ecgi

Challenges of the market for initial coin offerings

Pablo de Andrés
Universidad Autónoma de Madrid and ECGI

David Arroyo
Institute of Physical and Information Technologies

Ricardo Correia
Universidad Autónoma de Madrid

Alvaro Rezola
Universidad Autónoma de Madrid

This paper can be downloaded without charge from:
http://ssrn.com/abstract_id=3413117

https://ecgi.global/content/working-papers

european corporate governance institute

Challenges of the market for initial coin offerings

Pablo de Andrés
David Arroyo
Ricardo Correia
Alvaro Rezola

Abstract

This article analyzes the main problems and the solutions adopted in the market for Initial Coin Offerings (ICO), to anticipate the future of this market and determine implications for issuers, investors and regulators. ICOs represent an alternative and innovative financing solution that has experienced spectacular growth and notoriety in recent years. ICOs rely on Blockchain protocols and the ICO market is, therefore, characterized as decentralized, disintermediated and unregulated. Our results show that although the ICO market is innovative, it already displays many of the problems of traditional financial markets, and that these problems were at the genesis of the last financial crisis. Our analysis of the problems and solutions adopted shows a tension between what the Blockchain technology offers, and the problems associated with the financing of innovation. Considering the problems and solutions adopted, we no longer expect the ICO market to be characterized as disintermediated, unregulated or even decentralized in the near future. Furthermore, it is a real possibility that ICOs may end up being a progressor model eventually replaced by similar but more specialized financing models, some of which may already exist. With respect to the particular solutions of the ICO market, while some represent the realization of the potential of Blockchain, others such as forks have important Governance implications with the potential to create as many problems as the ones they address.

Pablo de Andrés
Professor of Finance
Universidad Autónoma de Madrid, Finance and Marketing Department
C/ Francisco Tomás y Valiente, 5
28049 Cantoblanco - Madrid, Spain
phone: +34 914 976 527
e-mail: p.andres@uam.es

David Arroyo
Researcher
Spanish National Research Council,
Institute of Physical and Information Technologies
Serrano 144
28006 Madrid, Spain
e-mail: david.arroyo@uam.es

Ricardo Correia*
Assistant Professor of Finance
Universidad Autónoma de Madrid, Finance and Marketing Department
C/ Francisco Tomás y Valiente, 5
28049 Cantoblanco - Madrid, Spain
phone: +34 914 975 469
e-mail: ricardo.correia@uam.es

Alvaro Rezola
Research Assistant
Universidad Autónoma de Madrid, Finance and Marketing Department
C/ Francisco Tomás y Valiente, 5
28049 Cantoblanco - Madrid, Spain
phone: +34 914 975 745
e-mail: alvaro.rezola@uam.es

*Corresponding Author

Review

Challenges of the market for initial coin offerings

Pablo de Andrés [a], David Arroyo [b], Ricardo Correia [c,*], Alvaro Rezola [c]

[a] *Universidad Autónoma de Madrid and ECGI, Finance and Marketing Department, C/ Francisco Tomás y Valiente, 5, 28049 Cantoblanco, Madrid, Spain*
[b] *Instituto de Tecnologías Físicas y de la Información, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain*
[c] *Universidad Autónoma de Madrid, Finance and Marketing Department, C/ Francisco Tomás y Valiente, 5, 28049 Cantoblanco, Madrid, Spain*

ARTICLE INFO

ABSTRACT

This article analyzes the main problems and the solutions adopted in the market for Initial Coin Offerings (ICO), to anticipate the future of this market and determine implications for issuers, investors and regulators. ICOs represent an alternative and innovative financing solution that has experienced spectacular growth and notoriety in recent years. ICOs rely on Blockchain protocols and the ICO market is, therefore, characterized as decentralized, disintermediated and unregulated. Our results show that although the ICO market is innovative, it already displays many of the problems of traditional financial markets, and that these problems were at the genesis of the last financial crisis. Our analysis of the problems and solutions adopted shows a tension between what the Blockchain technology offers, and the problems associated with the financing of innovation. Considering the problems and solutions adopted, we no longer expect the ICO market to be characterized as disintermediated, unregulated or even decentralized in the near future. Furthermore, it is a real possibility that ICOs may end up being a progressor model eventually replaced by similar but more specialized financing models, some of which may already exist. With respect to the particular solutions of the ICO market, while some represent the realization of the potential of Blockchain, others such as forks have important Governance implications with the potential to create as many problems as the ones they address.

1. Introduction

A financing alternative that has been gaining considerable importance is the Initial Coin Offerings (ICO), a means of financing early-stage digital innovations through the issuance of crypto-assets.[1] Being a digital, decentralized, disintermediated, global, and unregulated market, ICOs present novel challenges, but also some innovative solutions to these problems. The merits of Blockchain, the information protocol developed with Bitcoin and currently supporting most of the crypto-securities, has been extensively lauded, to the point that Blockchain is currently a household name. In turn, regulators have assumed a sandbox approach, hoping that this technology ends up realizing its full potential,[2] but inevitably problems arose raising questions about the future of ICOs.

With respect to Blockchain, academic research reflects the increasing acceptance of Bitcoin as an alternative asset, as so, it is not surprising that current academic interest focuses on the relation and dynamics of Bitcoin with other commodities such as gold (Klein, Thu, & Walther, 2018), other cryptocurrencies (Ji, Bouri, Lau, & Roubaud, 2019; Yi, Xu, & Wang, 2018) and traditional financial securities (Fang, Bouri, Gupta, & Roubaud, 2019). With respect to ICOs, existing literature has so far focused on the determinants of the success of an ICO (e.g., Adhami, Giudici, & Martinazzi, 2018; Flood & Robb, 2017; Huang, Meoli, & Vismara, 2020; Lee, Li, & Shin, 2021), regulatory aspects (e.g., Barsan, 2017; Kaal, 2018; Maume & Fromberger, 2019; Rodrigues, 2018; Teng, Griffin, & Koh, 2019), comparison with other methods to finance early-

---

[1] Crypto-assets is a term covering a new asset class of digital registries in Blockchain. Under that term, we find crypto-currencies, crypto-securities, and tokens. The focus of this article is on the role of digital assets as a type of financial security aimed at financing businesses, that is, crypto-securities. We will not focus directly on pure crypto-currencies such as Bitcoin but, given the perceived similarities between these crypto-currencies and tokens, we will refer to them when relevant. Furthermore, our arguments and analyses refer to public permissionless blockchains, that is, anyone can read/submit to the Blockchain and anyone can participate in the transaction verification process. For a more detailed explanation of the types of Blockchains, see Peters and Panayi (2015).

[2] In many situations, the positive externalities of the technology are taken for granted and the associated technological risks are disregarded (Baldwin, 2018; Collomb, De Filippi, & Sok, 2018).

stage innovations (e.g., Catalini & Gans, 2019; Kaal & Dell'Erba, 2017; Lipusch, 2018), Corporate Governance issues (Daluwathumullagamage & Sims, 2020; Giudici & Adhami, 2019; Gurrea-Martínez & Remolina, 2020; Yermack, 2017), ICO financial performance (Zhang, Aerts, Lu, & Pan, 2019; Howell, Niessner, & Yermack, 2020; Momtaz, 2020a; Fisch & Momtaz, 2020; Lyandres, Palazzo, & Rabetti, 2020; Momtaz, 2021; Benedetti and Kostovetsky, 2021) and agency conflicts and signaling effects (Chen, 2019; Fisch, 2019; Momtaz, 2020b).

Since the height of the ICO market in 2018, several developments such as the first YoY decrease in 2019 and the arrival of new breed of ICO offspring raise important questions about the future of the ICO market. Although Blockchain applications for alternative financing solutions are unlikely to disappear, it is unclear what form they will have in the near future. Will ICOs remain the dominant model and what characteristics will they have? Are ICOs likely to be replaced with more specialized models? What challenges lie ahead for Blockchain based financing models? These questions have all important applications for issuers, investors and regulators alike. Existing research focuses mainly on exploring the potential of this market, on the determinants of its success or on particular aspects. Our paper in turns focuses on the current problems afflicting the whole market and on the current solutions that address them. We show that the current problems that afflict the market are equally relevant in defining its future as are its current success stories and unrealized potential. Our results contribute to existing literature by showing that the market currently display similar problems to existing financing solutions, how the current evolution of the market is affecting the very core characteristics that have traditionally been used to define it and how a new generation of specialized offspring is emerging. All these aspects are naturally likely to influence the focus of all future research.

The structure of the article is as follows. Section 2 describes the Blockchain technology and the ICO process. Section 3 describes the current main problems identified in ICO markets. Section 4 critically analyzes the current responses of ICO markets to the problems identified in Section 3. Finally, Section 5 provides a discussion of the results and the main conclusions.

2. The Blockchain environment and the ICO market

Blockchain is a distributed ledger in which information is stored in blocks that contain a cryptographic hash of previous blocks ensuring the integrity of information and effectively creating a decentralized and disintermediated technological solution. Although Blockchain appears in 2008, as the supporting protocol for the cryptocurrency Bitcoin (Nakamoto, 2008), there were previous attempts at developing similar information protocols and similar cryptocurrencies not controlled by a central bank. If Blockchain and Bitcoin are not radical inventions, it is important to understand why they succeeded while previous attempts have failed. Additionally to being the supporting protocol for cryptocurrencies, Blockchain also allowed the development of related businesses and Blockchain represents the information protocol for a new financing solution, the Initial Coin Offerings that we describe in this section.

2.1. Distributed ledger technology and blockchain

Although commercially successful applications of distributed ledger technology (DLT) are recent, the birth of DLTs can be traced back several

decades[3]. DLT is a cryptographic information protocol developed in the late 1950s and early 1960s for defense purposes, with the objective of distributing data through various repositories so that an attack on any repository would not result in the corruption or total loss of data. Additionally to the DLT architecture, Blockchain incorporates several cryptographic developments such as Merkle Hash Trees (Merkle, 1979) and Proof-of-Work (Back, 2002; Dwork & Naor, 1993)[4]. With respect to previous protocols, Blockchain goes a step further in information security by running a parallel digital system without trusted third parties, administered by methods of distributed consensus.

A few initial projects did make commercial use of DLTs[5], but Bitcoin and Blockchain, represent its first successful economic application. The success of Bitcoin and Blockchain is explained by three different factors: an ingenious system of incentives, a favorable economic context and social acceptance. The last two factors have been clearly influenced by the recent financial crisis.

With respect to the system of incentives needed to develop the network required to run the DLT, the Bitcoin Blockchain presented the first practical solution to this problem (Narayanan & Clark, 2017), as it compensated participants, who are referred to as miners, in the network responsible for maintaining the system. In the process, miners earn a crypto-currency attached to the network and use it as a medium of payment in the digital system, thus encouraging the growth of the network, of the currency, of the information protocol and of the community[6].

In terms of the social and economic context, the global financial crisis of 2007–2009 had important economic and social repercussions. It led to a series of public bailouts of financial institutions (e.g., the US Troubled Asset Relief Program), the implementation of expansionary fiscal and monetary policies that significantly decreased interest rates (e.g., the quantitative easing programs and debt purchases by central banks), a significant increase in unemployment, and the enforcement of new regulations targeting financial markets (e.g., see Berkmen, Gelos, Rennhack, & Walsh, 2012; McCauley, McGuire, & von Peter, 2012).

Socially, the financial crisis and the governmental response to it, created the perfect breeding ground for a technology with the ability to eliminate financial intermediaries and for the emergence of a currency that evaded the control of any central bank. Furthermore, Blockchain fostered the creation of new businesses and provided an escape route from unemployment.

In terms of the economy, this period was marked by a sharp decrease in interest rates and in returns overall. However, this decreases in interest rates did not affect borrowers and investors the same way. Investors were struggling to obtain decent yields, but borrowers were facing credit rationing, regardless of the decrease in interest rates (Brunnermeier, 2009; Campello, Graham, & Harvey, 2010; Shleifer & Vishny, 2010)[7]. Directly and indirectly, these events have fostered the

---

[3] It is certainly fair to consider Blockchain as a novel contribution in the field of the distributed consensus and in the creation of Peer-To-Peer information systems. Nevertheless, its introduction as a core component of Bitcoin and the subsequent cryptoeconomics convey an astonishing example of how forgotten academic work can be properly updated and exploited in real practical scenarios (Narayanan & Clark, 2017).

[4] For a comprehensive description of the origins of Blockchain please see Sherman, Javani, Zhang, and Golaszewski (2019).

[5] For example, see Nick Szabo's Bit gold or Dai's B-Money (Dai, 1998).

[6] In fact, there is an interlocking interdependence in Bitcoin between the security of the information blocks, the health of the mining ecosystem, and the value of the currency (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016).

[7] Credit constraints cannot simply be considered as a restriction on the credit offered; an increase in the price of credit is also a constraint. Although central banks may reduce their discount rates, commercial banks are able to increase the credit spreads so much that the overall effect is an increase in the price of credit. Duchin, Oguzhan, and Sensoy (2010) highlight this aspect of the 2007–2009 financial crisis.

development of alternative financial markets (Glasius & Pleyers, 2013; Monjas-Barroso, 2012) such as cryptocurrencies and the Initial Coin Offerings. Not only cryptocurrencies represented alternative speculative investments but ICOs allowed investors to meet borrowers, bypassing traditional financial intermediaries. Borrowers can obtain financing at reasonable prices and investors can obtain reasonable yields in a context of very low interest rates. Furthermore, since this "new" market is digital, it is also global by nature (with no language, geographical, cultural, or legal barriers), allowing borrowers to access a broader base of potential investors, and investors to access a broader base of investment opportunities.

2.2. Initial coin offerings

An ICO is the acronym adopted for the first issuance of crypto-assets from a company. It initially comprehended early-stage innovative firms looking for financing. These firms are not commonly willing to dilute their ownership to outsiders in the form of mining and chose to issue a limited number of crypto-assets (e.g. tokens) with additional rights, similar to a hybrid security. Crypto-assets are contracts that provide the owner with certain rights formalized in code, referred to as smart contracts, and run on DLTs. First, a token is a currency in itself, which may acquire value through its use in commercial transactions or through its purchase for speculative gains. The token may also award rights to the acquisition of the goods and services offered by the firm (utility). Finally, the token can also be a financial security awarding rights that can be classified as debt or equity or even as a subscription right on a security that may be created in the future.

Both initial and seasoned offerings of crypto-assets fall under the umbrella of investment crowdfunding. The crowdfunding ICO model has been quite successful so far and has gone through three stages in what concerns the characteristics of the smart contract. The first stage is the altcoin[8] stage and ICOs issued mostly crypto currencies with partial modifications of the Bitcoin Blockchain. Currently the first stage is decreasing in importance and in what concerns currencies the focus now is mostly on stable coins. The second stage of ICOs came from companies building infrastructure services around the Blockchain ecosystem, attaching utility rights to the tokens issued. These rights range from governance and voting rights to identity or payment platforms. Among them, Ethereum stands as the most notable example by building a DLT capable of launching standardized smart contracts in a fairly easy manner. One of these contracts is the ERC20 (Vogelsteller & Buterin, 2017), capable of issuing new tokens. The emergence of *easy to develop smart contracts*[9] opened the door for the third and current stage, where the existing IT infrastructure and market legitimacy allows startups not directly involved with DLTs to consider issuing crypto-securities as an alternative to traditional securities issuance. Currently, the second and third stages are expected to run in parallel because there are many infrastructure services still needed to fulfill the second stage of ICOs and competition is likely to appear, even for existing services (e.g., Stellar and NEM look to compete with Ethereum's dominance as crowdfunding platforms).

In terms of figures, the ICO model has raised $90 million USD in 2016 from 29 ICOs, more than $6 billion USD in 2017 from 875 ICOs, and a yearly market high of more than $7.5 billion USD in 2018 from a total of 1253 offerings[10]. In 2019, the market showed its first YoY decrease in terms of volumes and offerings have raised $370 million USD from 109 operations.

A potential explanation for the decrease in the number and volume of ICOs following 2018 was the arrival of new models of public issues of crypto assets either addressing some of the ICO problems or as a form of issuance specialization. These new models such as Security Token Offerings (STOs) and Initial Exchange Offerings (IEOs) ensure regulatory compliance and indirectly signal issue quality, both these models focus essentially on security tokens.[11] A different model is a Token Generation Event (TGE),[12] this model focusses mainly on utility tokens and therefore is designed to avoid regulatory scrutiny (Hussey, 2019).

2.3. Current ICO process: The unsustainable status quo of the ICO market

The current situation in the market for ICOs, where serious value-creating ventures compete for funding with opportunistic or even illegal ventures, is not sustainable in the long run and is commonly described as the wild west of financial markets (e.g., see Robinson, 2018).

The current process followed for an ICO is presented in Fig. 1.

An ICO starts (1) when an entrepreneur feels they have reached a point in the development of a product or service that allows potential investors to recognize its merits and potential (Ibba, Pinna, Baralla, & Marchesi, 2018). The first marketing stage (2) is to announce the plans to perform a token issue in the near future, detailing the project, its nature and objectives, the nature of the tokens issued and the underlying Blockchain. A white paper is usually published at this stage, detailing the project, its merits, and future developments in their Roadmap. A web page may accompany the white paper and this web page often represents the only tangible part of the whole project. Traditionally, ICOs relied on the Blockchain community and therefore, it is not unusual for an important part of the promotion efforts to take place on social media platforms (Rhue, 2018). The most commonly used are Telegram, Twitter, Facebook, Reddit, Slack, and Bitcoin Talk[13]. More recently, crowdfunding websites such as Gitcoin have also become popular.

Following the first disclosure of information and marketing efforts, a smart contract is deployed in a Blockchain (overwhelmingly Ethereum, Haffke & Fromberger, 2020) representing the cap table (3). Marketing efforts at this stage target community leaders or influential players to participate in a private placement before the public offering, also called pre-ICO (4). These investors benefit from discounted prices in exchange for participating in publicity and in marketing efforts during the offering.

The pricing of an ICO is usually defined on a single crypto-currency[14] to avoid regulation and it usually follows one of two patterns: it is either set by the issuer or it is determined through a Dutch auction system. Occasionally, for quality and sizable projects, niche advisors have appeared that offer services similar to traditional investment banks, including classic IPO advisory services such as bookbuilding, as well as advice with the technical parts of the process (e.g. smart contract auditing and cap table allocation during the offering). At this stage, the marketing efforts intensify, and the price is usually published both in

---

[8] See Hermann, Trimborn, Ong, and Lee (2018) for an historical analysis of altcoins, their properties, and evolution.

[9] The trade-off between functionality and security is a major concern in any information technology (Cranor & Garfinkel, 2005). In the case of smart contracts, the creation of new items is not a difficult task, but in many instances, the resulting products pose critical security problems (Nikolic et al., 2018).

[10] Source: ICO data https://www.icodata.io/.

[11] Naturally this model relies on centralized Exchanges, but 2019 also saw the arrival of a similar issuance model in Decentralized Exchanges, the Initial DEX offering (IDO). IDOs differ from IEOs, because it is not an exchange that backs the issue, but a launchpad platform (see Georgiev, 2021).

[12] For a detailed analysis of differences between ICOs, IEOs, STOs and Private Issues and IPOs see PWC (2019).

[13] The first social media platforms described are generalist (e.g., Reddit, Slack), and others are specialist platforms. The importance of these communication channels is not negligible; Benedetti and Kostovetsky (2021) measure the link between financial returns of an ICO and the intensity of Twitter posts and find it to be significant.

[14] There are also ICOs issued in USDs or other fiat currencies, although they are uncommon. When ICOs are priced in cryptocurrencies, potential investors need to operate with cryptocurrencies wallets.
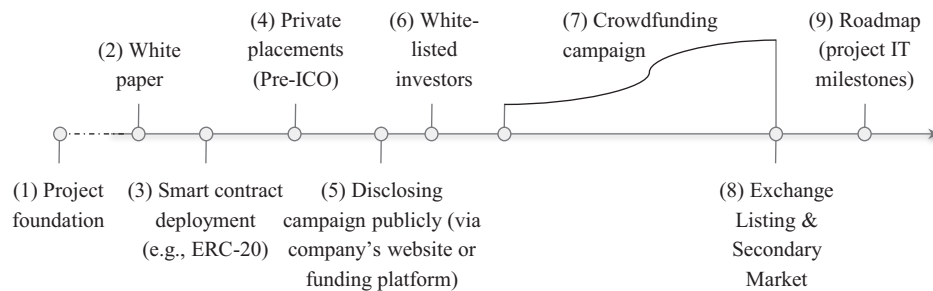
Fig. 1. ICO process.

exchanges and the company's website (5). To attract more interest, companies offer early participants a place in the offering white-list (6). Becoming a white-listed investor in a campaign ensures priority allotment and this is especially appealing in oversubscribed ICOs, as hot offerings push the technical limits of public Blockchains and may congest the network so much that some participants are unable to execute their orders until after the listing. During the campaign period (7), potential investors place their orders and are allotted the corresponding tokens, similarly to any subscription period of a public offer. Good campaigns usually last a few days, but bad campaigns may last substantially longer (campaigns last 40 days on average according to Howell et al., 2020). A successful campaign usually ends with the listing of the tokens (8). The listing may take place in Centralized Crypto Exchanges (CEX) or Decentralized Crypto Exchanges (DEX).[15] Although there is no conclusive data on first time token listings in DEX vs CEX, the importance of DEX is still marginal. Nonetheless, DEX is growing in importance, and it currently represents around 10% of the volumes of trade of CEX (see Aspris, Foley, Svec, & Wang, 2021). CEX are more user friendly, present high liquidity, allow easy conversion of crypto currencies to fiat currencies and are still more reputable than DEX. However, CEX imply more complex procedures lo list (e.g. KYC and AML), retain control of the users assets (custodial services) and, given their size, CEX are especially prone to hackers attacks. Currently, most ICOs can only access DEX and this partially explains the growth in the importance of DEX, nonetheless, according to Aspris et al. (2021) when ICOs are able to simultaneously trade in DEX and CEX, the trading volumes of the ICO in the CEX usually multiply by a factor of 70.

The issuance process of a successful ICO does not necessarily finish when the tokens trade in a secondary market. The issuer may still not have full access to the proceeds from the issue and it is important to ensure that investors are satisfied to create demand for future issues. With respect to access to the proceeds, the smart contract may have linked the access to the funds raised to the accomplishment of measurable business milestones detailed in the Roadmap (9) and the issuer now needs to achieve them. Furthermore, the need to provide liquidity may require the services of market makers and this is applicable also for tokens listed in DEX (Angeris, Evans, & Chitra, 2020). One other common strategy used to engage trading, is to perform Airdrops. An Airdrop is a marketing strategy to distribute free tokens to holders of tokens or coins of a specific Blockchain (usually Ethereum). Through this giveaway, buzz is created, potentially attracting the attention of more investors. It is important to point out that it is a costly strategy and that it should be properly optimized (Fröwis & Böhme, 2019).

This process of setting up an ICO presents several problems. First, it is simple enough that anybody with minimum technological literacy is able to issue tokens, even if there is little to show in terms of the development of a value-creating product or service. Second, although it uses Blockchain technology, it also relies on traditional internet protocols such as a webpage[16] and social networks,[17] which are considerably less secure and prone to hacker attacks. Third, the lack of standards, third party verification, and lack of a paper trail that is able to support legal liability, create serious problems of information asymmetries[18]. Finally, the lack of a proper custodian and the practice of issuers of obtaining immediate and uncontrolled access to the funds creates a strong incentive to deceive investors.

2.4. ICOs vs IPOs

Initial Coin offerings and Initial Public Offerings (IPOs) are often presented as competing financing channels of innovation, however as we will see, most of the similarities begin and end with the acronyms.

As Table 1 presents, the differences between ICOs and IPOs are manyfold. Starting with the type of securities issued, IPOs are limited to equity or debt, while in ICOs usually the token represents a complex security. With respect to the legal requirements and the disclosure of information, ICOs have little requirements and in most cases the disclosure of information is voluntary both in terms of financial information but also technical information. Even though issuers have the possibility to evade regulations, Huang et al. (2020) show that issuers tend to choose countries with ICO friendly regulations. IPOs in turn need to present a prospectus that includes, additionally to financial

---

[15] Although trading in DEX is decentralized, this secondary market depends on terms set in the smart contract, therefore even though being decentralized, almost all of the ICOS trading on DEX rely on the use of the Ethereum Blockchain, something that goes against the decentralization objectives.

[16] See the case of CoinDash discussed in Section 3.3 in which hackers attacked the website supporting the ICO.

[17] Indeed, the systemic risk of Blockchains can be interpreted as lower than that of many centralized platforms. However, the risk in terms of endpoint-security is far worse for Blockchains (Narayanan & Clark, 2017). First, users are responsible for managing their private keys in order to have access to their assets. This is not a minor concern since it involves dealing with cryptographic solutions that have not been properly understood by average end users (Eskandari, Clark, Barrera, & Stobert, 2018; Krombholz, Judmayer, Gusenbauer, & Weippl, 2016). Second, public Blockchains store information in an open and transparent way. Furthermore, all the information in a Blockchain is immutable, which means that internal integrity is preserved. Nonetheless, external integrity is not guaranteed by Blockchain, and thus, it is possible that the transaction log of an ICO does not contain the related company's financial records. That is, it is possible to have an inconsistency between information recorded in Blockchain and business rules (Rhue, 2018).

[18] Although Open Social Networks could pave the way for scams, they can also be leveraged to overcome information asymmetries (Lee et al., 2021). We can say that the ICOs ecosystem is somehow bootstrapped, since a sort of circular dependence exists between the integrity of the information allocated in the Blockchain and the external information in whitepapers and in social networks to earn potential investors' trust. It should be noted that the issuer defines the scope and quality of all the information provided during the whole funding process, even when advisors participate, information is not audited by a third party, is not required to follow any standards, and most of it is unverifiable.

Table 1
Analysis of initial coin offerings and initial public offerings.

	Securities	Legal requirements[a]	Information disclosure	Development stage	Investor access	Risk
ICO	Equity, debt, hybrids	Depend on market where issue is performed.	Most cases voluntary, unaudited	Early stage	Easy, may be limited by technological constraints.	Very high
IPO	Equity, debt (NCDs)	Registration, compliance with exchange listing and regulatory requirements, due diligence, KYC and AML.	Prospectus detailing financial details, risks and all relevant audited information for the security sale.	Firm is well established in the market, has an audited history of financial statements.	Limited, in attractive IPOs demand usually exceeds offer.	Moderate

[a] This table does not include Corporate Law since in the case of formal business structures (e.g. firm, corporation, etc.) there is no difference between issuing through an ICO or IPO. In the case of insolvency or eventual liquidation for instance, the rights of the investors in the ICO or the IPO would be similarly protected, and their level of priority would be defined by the nature of their claims. Nonetheless, entrepreneurs that choose to issue through an ICO are able to do so even without setting up a formal business structure in which case investors are completely unprotected in legal terms, following with the case of insolvency, in this situation any insolvency rights depend entirely on the terms of the smart contract.

information and valuations supporting the price, all information able to influence the IPO such as potential risks, managerial information including compensation, nature of the relation with underwriters, exchange where securities will list, lock up or waiting periods, etc. With respect to Know Your Client (KYC), Anti Money Laundering (AML) compliance and the due diligence process, these are all an integral part of an IPO, however the same is not clear in the case of ICOs, because an ICO issuer still has the ability to completely avoid regulation (according to Zetzsche, Buckley, Arner, & Föhr, 2019 less then a third of the ICOs in their sample specified the applicable issuing laws) and even when regulation is put forward to address some of these aspects it does so in an incomplete manner (for the case of the 5th EU AML Directive see Haffke, Fromberger, & Zimmermann, 2020).

With respect to the development stage, IPOs usually represent the end of a process in which following the involvement of private investors the business is mature enough to go through a public offer. ICOs in turn, are usually very early stage investments in most cases financing little more than ideas or projects (according to Haffke & Fromberger, 2020, less than half of the ICOs performed in 2019 claimed to have a product in the market before the ICO). Contrary to an IPO, with an ICO, many entrepreneurs are able realize their first important capital gains before actually producing anything or actually taking a product to the market.

With respect to access by investors, apart from Blockchain constraints, there are little limitations in investing in an ICO, while access to IPOs is sometimes limited by the scarcity of the securities issued and by the actions of gatekeepers such as investment banks and brokers.

An IPO is a costly and lengthy process where many administrative and legal hurdles need to be overcome and that usually involves many agents such as the firm, investment banks, lawyers, auditors, analysts and exchanges. An ICO is fast process when compared to an IPO, there are less requirements to meet and the whole process can be done almost without intermediaries. In terms of costs, an ICO may appear cheap when compared with an IPO, however the true costs of an ICO are not clear since there may be significant costs whenever the tokens are pre-sold, listed in a centralized crypto exchange and when airdrops are performed.

Naturally, all these differences have risk implications and the slow and lengthy requirements of an IPO aim at securing investor protection, something absent from an ICO process. As so, not surprisingly, ICOs are very high-risk investments when compared with IPOs. In their analysis of the performance of ICOs and IPOs issued in 2019, Haffke and Fromberger (2020) show a six-month percentage of 90% of total or big losses for ICOs while the same figure was only 23% for the case of IPOs.

3. Main problems of the Initial Coin Offerings market

The ICO market performs the basic functions of traditional financial markets, which is the logical place in which agents in need of funding meet agents in search of investment opportunities. As such, the ICO market, to a greater extent presents problems similar to those of

traditional financial markets. From the point of view of economics, the problems we discuss in this article translate into an inefficient allocation of resources resulting from important asymmetries of information between issuers and investors. From the point of view of ethics, they reflect a lack of proper standards, lack of transparency in the selling process, a consequential lack of proper accountability, and pure deceit and fraud of non-qualified investors.

3.1. Blockchain and the tragedy of the commons

The current situation can be best described as a Tragedy of the Commons (TOC) failure in which the whole market may suffer from the actions of a few opportunistic agents[19] (Matsumura, 2017). Consider the case of the existing conflict between honest Blockchain technology developers and opportunists that are simply trying to make a quick buck through fraud or the simple overexploitation of the technology by offering useless services and products.[20]

TOC failure is not exclusive to ICOs and has already described traditional financial intermediaries (e.g., see Schwarcz, 2011). Following the 2007–2009 financial crisis, unlike other industries that experienced similar crises in terms of magnitude (e.g., the nuclear power industry and the Three Mile Island US accident and the chemical industry with the Bhopal accident in India), the financial services industry failed to perceive itself as a community bound by a common fate (Omarova, 2011). Although the ICO market and particularly Blockchain developers present a higher sense of community (e.g., see Reijers, O'Brolcháin, & Haynes, 2016) and there are initiatives being proposed to address the TOC failure (Matsumura, 2017); many agents still do not perceive the existence of a common fate for the whole Blockchain community. Another aspect that is more severe in the case of the ICOs is the threat in the case that TOC failure persists. While traditional financial intermediaries fear limitations on their access to specific financing sources, the removal of public safety nets, or the imposition of mandatory contributions to a common systemic risk fund (see Omarova, 2011; Schwarcz, 2011), the threat to the ICO market may involve a complete ban of token issuance or trading. Financial regulators, faced with the continuing inefficiencies of ICO market agents, may decide to ban token issuance and trading or substantially curtail the token market (e.g., see the cases of South Korea and China).

---

[19] We have to take into account that by agents we mean either human or artificial agents. In fact, ICOs are built upon the so-called Infosphere (as opposed to the Biosphere) and thus the implications of the TOC should be properly adapted (Greco & Floridi, 2004).
[20] The morally questionable actions of the opportunistic agents are detailed in the following subsections.

3.2. Scams, deceit, manipulation, and copycat projects

Fraud in ICOs is one of the greatest challenges and threats to the Blockchain community and this is widely recognized by regulators and market agents. Recently, Securities and Exchanges Commission (SEC) chairman Jay Clayton expressed his disbelief at the levels of fraud being committed in the ICO market, implying that further regulatory action may be required to protect investors (Baker, 2018). Two leading members of the Blockchain community, Joseph Lubin, co-founder of Ethereum, and Brad Garlinghouse, CEO of Ripple, have acknowledged that many ICOs are fraudulent and that further regulatory action is expected (see Choudhury, 2017).

Some characteristics of permissionless Blockchain make it especially tempting to agents that aim to commit scams, fraud, or offer irrelevant services of no value:

1. Pseudoanonimity in the most popular Blockchains (i.e., Bitcoin and Ethereum): although all information is public, it cannot be traced back to any particular agent.
2. The nature of the entrepreneurs: since Blockchain is a new market, it will expectedly attract fraudsters and scammers (see Baker, 2018). However, even honest entrepreneurs are essentially creative agents that have the natural ability to justify their behaviors, which oftentimes leads them to display unethical behaviors (e.g., see Gino & Ariely, 2012).

In the case of pure crypto-currencies and particularly Bitcoin, its use in illegal activities such as the sale of illegal drugs was synonymous with the site the Silk Road, however some figures indicate that the prevalence of criminal transactions was relatively smaller than in the case of other means of payment (see Brito, 2013). The issuance of ICOs does not have such a dishonorable reputation but, as we will see, the prevalence of fraud is quite significant.

With ICOs, a particularly fraudulent use of smart contracts involves promoting Ponzi schemes under the disguise of high yield investment programs or simply, social games (Bartoletti, Carta, Cimoli, & Saia, 2020). However, as in the case of Bitcoin, the weight of these criminal transactions is still relatively insignificant even though it already triggered the issuance of regulator warnings (SEC, 2013). Although Bartoletti et al. (2020) classify 10% of the smart contracts of their sample as Ponzi schemes, these account for only 0.05% of the transactions recorded on the Ethereum Blockchain. The relatively small impact of these schemes is mostly explained by their failure to attract users and by the poor programming skills of the fraudsters, often producing codes with severe bugs or programming so poor that the Ponzi scheme contracts are themselves highly vulnerable to hacking. An exception in terms of the volumes lost in a Ponzi scheme is the recent case of Modern Tech (see Biggs, 2018; Ngo, 2018) in which the fraudsters performed an exit scam after raising approximately $660 million via Ponzi contracts.

Such exit scams are quite common also in the ICO world (e.g., see Biggs, 2018; Kean, 2018). In an exit scam, entrepreneurs claim that the tokens issued are to finance real business operations, however, once the funds are raised, the entrepreneurs disappear with the funds and no real business venture is actually pursued.

The use of pre-sales[21] to promote ICOs creates the perfect ground for flipping and for pump and dump schemes. While promoters advertise pre-sales to qualified investors as a quality signal, the actual terms and prices of the pre-sale are rarely made public. The pre-sale usually takes place with heavy discounts on the issuance price and few restrictions on the subsequent trading of the tokens.[22] This preferential treatment of a group of investors usually translates into flipping, by which pre-sale investors buy tokens with a heavy discount and then sell them at market values. While flipping may be morally questionable[23] it is not illegal and does imply market manipulation, however, the similar practice of a pump and dump is illegal. In a pump and dump scheme, investors buy the asset and release information aimed at increasing prices (pump) and later sell the asset at its inflated price (dump). The unregulated nature of the Blockchain market allows these market manipulation practices to thrive and it is easy to find agents that offer "pump" services on social networks (Gordon, 2017) and even pump "communities" that coordinate to implement these schemes (Williams-Grut, 2017).

Pump and dump schemes are not the only examples of market manipulation in the ICO market. Although manipulation is usually hard to prove and relies on the availability of considerable funds, the same does not occur in a market with low liquidity, in which assets are highly concentrated and decentralized trading is still common. Griffin and Shams (2020) analyze trading activities between Tether[24] and Bitcoin on the Bitfinex exchange and conclude that such trading activities are responsible for price increases in Bitcoin. The authors conclude that half of the increases in Bitcoin during 2017 were a result of the trading activities of Bitfinex using Tether. Another case of Bitcoin manipulation concerns the Mt. Gox exchange. Gandal, Hamrick, Moore, and Oberman (2018) analyzed Bitcoin transactions in the Mt. Gox exchange during the period of April 2011 to November 2013 and identified price manipulation. After identifying suspicious bot trades, some of which were actually operated by Mt. Gox itself, Gandal et al. (2018) conclude that these trades were able to justify the spectacular growth in the price of Bitcoin observed during this period. In 80% of the days on which suspicious trading occurred, the price of Bitcoin increased and always by a higher amount when compared to periods in which there was no suspicious trading. Although price manipulation by Mt. Gox was probably a way to hide a theft of Bitcoins as a result of a hacker attack, these examples show how manipulation is a real threat in crypto-asset markets.

Misrepresentation of the assets, the professional background of the founders, and the amounts raised are also currently significant problems in ICOs. Two notorious cases of general misrepresentation are Recoin and DRC World, for which criminal charges have already been brought by the SEC (SEC, 2017). In both cases, neither firm had the assets they claimed nor was there a professional team of experts to develop the business. Furthermore, it was proven that in both cases, the amounts raised with the ICOs fell way short of the amounts advertised by the ICO promoter.

There are many examples of useless services and simple copycats. In many cases of useless services, there is naturally also a problem of misrepresentation to attract unsuspecting investors.[25] Copycats were particularly rampant in Chinese promotions and this is even put forward by J. Lubin as the main reason for the Chinese ban of ICOs (see Choudhury, 2017).

---

[21] According to insiders, the vast majority of ICOs have pre-sales; Zetzsche et al. (2019) identify pre-sales in more than 50% of their sampled ICOs and Kharif (2017) puts this figure at approximately 80%.

[22] According to Zetzsche et al. (2019), most of the pre-sale terms identified in their sample of ICOs do not include lock-up periods.

[23] J. R. Willett, one of the fathers of the ICO concept, argues against pre-sales due to the unfairness that this practice may generate between qualified and retail investors (e.g., see Kharif, 2017).

[24] Tether is a crypto currency reportedly pegged to the USD. The relationships between Bitfinex and Tether have been a common topic of discussion on crypto forums with some sources claiming the same investors own the exchange and the crypto currency (see Leising, 2018).

[25] In the case of ATB Blockchain, a Blockchain promoted as the fastest on the market, the entrepreneurs misrepresented not only the technical abilities of the Blockchain (essentially a useless innovation according to Verified ICOs) but also their family backgrounds (see Class Action N0. 17–10,001 of the Southern District of New York).

3.3. Hacking attacks: Exposing the security giant with feet of clay

Blockchain technology prides itself on its technological security, supported by cryptography and a decentralized ledger. It is currently widely assumed that it is impossible to hack the Blockchain protocol (Jia & Zhang, 2017). In Kaminsky (2013), Dan Kaminsky, a famous computer engineer and hacker, discusses his inability to hack the Bitcoin protocol after several attempts. However safe the base protocol is, the level of security is not homogeneous across global Blockchain networks, since applications built on the protocol such as wallets and exchanges may present vulnerabilities and affect the whole Blockchain network (Jia & Zhang, 2017).[26] Although Blockchain technology ensures that information cannot be changed and manipulated, because the registries are essentially digital, decentralized, and anonymous, if a theft occurs by a hacker, it is impossible to cancel the transaction.[27]

Recent events have highlighted that some of the strengths of Blockchain can also be seen as weaknesses because hackers have been able to exploit several of its vulnerabilities. In fact, although the Blockchain core protocols are secure, the overall ecosystem possesses some vulnerabilities caused by poor security practices and end-user and Blockchain-based software (Jia & Zhang, 2017). Some attacks exploited the vulnerabilities of Blockchain wallets and exchanges, while others have taken advantage of vulnerabilities in other protocols that support websites and social media platforms; both mediums are an integral part of launching ICOs.

Given the volume of crypto-assets traded and stored, some entities are more prone to attacks by hackers. Crypto-asset exchanges, trading platforms, wallets, and funds are especially enticing to hackers due to the potentially high gains a single successful attack may generate.

Hacking attacks on exchanges are the most significant by volume, with the most notorious cases being those of Coincheck and Mt. Gox in Japan, Youbit in South Korea, NiceHash in Slovenia and Binance in the Cayman Islands. The case of Binance became notorious because it is the most reputable crypto exchange where apart from the theft of cryptocurrency the hackers were able to gain control of several private client accounts (Kharpal, 2019). It is important to highlight how these attacks take place in territories that traditionally have had a soft regulatory approach to crypto-assets and Blockchain technology. This implicitly indicates that a "harder" regulatory approach may be the desirable way to curtail such vulnerabilities. It is also worth noting how the South Korean approach to crypto-asset trading changed; partially influenced by the hacking attacks and the misuse of crypto-assets. Following an initial ban on anonymous trading of crypto-assets, Korea required a registration of all crypto exchanges and a trading prohibition to all Crypto Exchange Employees (Im, 2021).

The attack on CoinDash, a platform for trading Ether, is possibly the most infamous attack on a trading platform and is also a perfect example of the off-chain vulnerabilities posed by the reliance of the ICO process on other less safe protocols, such as the ones used by webpages. Coin-Dash was performing an ICO to raise funds and supported the white paper with a website detailing the Ethereum wallet address to transfer the funds to. Contrary to previous cases of attacks on exchanges, hackers did not take advantage of vulnerabilities in the Blockchain code; instead, they exploited the weakness of the off-chain services by attacking the website supporting the ICO and changing the wallet address.

In terms of funds, the DAO is the most representative case, and it is a perfect example of vulnerabilities at different levels. It is a decentralized fund to invest in projects selected by a set of curators and subject to voting by holders of DAO tokens. The funded projects would then return the funds based on preset payment terms subject to default risk. The hacking attack targeted the funds raised by the ICO by exploiting a vulnerability of the smart contract. While the DAO worked on fixing this bug, it was targeted by a hacker who was able to transfer one third of the funds raised by the DAO ICO to a subsidiary account. In terms of governance mechanisms, the case also highlights an important failure of highly decentralized organizations that rely on a democratic process of decision-making. By having a highly fragmented "ownership"[28] structure, there were more than 11,000 token holders at the time of the attack and it was not possible to obtain an agreement in time to divide the funds raised by the ICO into several accounts.[29] Following several proposals, it was decided to implement a hard fork that would "re-write the history" eliminating the hacking attack and the funds were returned to the DAO.

In terms of wallets, the attack on Parity is noteworthy for various reasons. First, Parity is one of the most trusted Ethereum wallets in the market and was founded by Gavin Wood, one of the co-founders of Ethereum. Second, the hackers targeted funds stored in multisig wallets, a theoretically safer solution than single-signature wallets in which a single key provides access to the funds. Finally, the attack on Parity is illustrative of a particular response of the Blockchain community to a hacker attack. By exploiting a vulnerability in the implementation of a Blockchain end-user view, hackers were able to steal approximately $32 M from multisig Parity wallets before they were stopped. In this case, the hackers were prevented from stealing the remaining $85 M stored in the wallets by a group of white hackers called the White Hat Group.[30] Once alerted to the attack, this group stole the remaining $85 M stored in the multisig Parity wallets by exploiting the same Blockchain vulnerability and returned the funds to their original owners once the wallet vulnerabilities were patched.

Hacking attacks are incredibly damaging to Blockchain technology, because they hurt the protocol where it hurts most, namely, by questioning the so-called security of the technology, an imperative when dealing with digital assets. Hackers were able to expose vulnerabilities at all levels, attacking the code of accomplished programmers, attacking what are theoretically the most secure solutions offered, attacking major intermediaries that allocate significant investments to security issues, and highlighting major flaws in the current process of issuing ICOs. Hacking attacks also attract the attention of regulators, increasing the risk of a regulatory response and a reprisal against the firms that are

---

[26] Regarding this, we must recall that the security of a system is defined by its weakest point (Schneire, 2011). Blockchain functionality encompasses end-user views, software applications, and off- and on-chain services that take advantage of the tamper-resistant nature of core protocols as the consensus mechanism and the P2P network. Nevertheless, a security breach in any of these external elements exposes the vulnerability of the whole network.

[27] Although thefts can be easily followed in the Blockchain and funds can be traced to the personal account of the hacker, there is no easy solution to return the funds to its rightful owners. De-anonymization can only be performed by properly leveraging transaction graph analysis (Meiklejohn et al., 2013), and analyzing off-chain security vulnerability problems (e.g. Goldfeder, Kalodner, Reisman, & Narayanan, 2018) and monitoring exchange activity. In fact, companies such as The Blockchain Intelligence Group (BIG), Blockseer, or Chainanalysis are able to trace suspicious patterns in Bitcoin and deanonymize (when possible) the related users.

[28] Ownership is not the most correct term because DAO token holders are not equity holders in a strict sense; although they have voting rights, there is no actual ownership of The DAO itself.

[29] Another vulnerability of the DAO case was the use of a single account to store all the ether raised via the ICO, although in this case the justification given was that the funds raised exceeded all expectations.

[30] See Section 4.3 where white hackers are defined and their current role in ICO markets is analyzed and discussed.

victims of hacking attacks.[31]

By contrast, the analysis of the hacking attacks on the Blockchain environment also show us that the Blockchain community has a common interest in addressing the problem and, as discussed in Section 4.6, uses a vast portfolio of innovative solutions to address the problem.

3.4. Complacency of market participants

The subject of complacency is at the heart of the TOC failure. We can discuss complacency on two different levels: that of honest business enterprises and, most importantly, that of investors. In the first case, honest business enterprises have been complacent with their dishonest competitors for financing. Given current market conditions in which traditional investments such as equity (Vlastelica, 2018), sovereign debt (Ismailidou, 2016), or even junk debt (Platt, 2018) offer very low or even negative yields, investors are driven to crypto-assets in their search for profitability. In this context, through signaling, honest business enterprises are finding it easy to obtain financing at reasonable costs and this explains their complacency.

The case of investor complacency is harder to explain. Through screening,[32] qualified investors have been able to select value-creating ICOs and generate reasonable returns while ignoring opportunist ventures. In the case of retail investors, the lack of yield drives them to crypto-assets; however, the lack of information provided in most ICOs makes it hard to explain how rational investors could make such investment choices. In their analysis of a sample of over 1000 ICOs, Zetzsche et al. (2019) found that:

- More than half of the ICOs do not provide personal or background information on the project promotor;
- In most of the ICOs, the name on the white paper differs from that of the ICO issuer;
- Roughly two thirds of the ICOs do not provide any information on the applicable law.

In normal circumstances, all these aspects would alarm a rational investor; however, in the same sample of ICOs, the authors find that few ICOs have failed to meet the minimum subscription level set, meaning that investors are completely disregarding the lack of important information to support any investment decision. According to EY (2017) the growth in ICO investments is driven mostly by the Fear or Missing Out (FOMO) rather than by a rational valuation of the business opportunity and, according to Colagrossi (2018), this FOMO is even expanding into traditional financial firms.

The existence of opportunistic issuers has not been perceived as a serious problem; however, their existence will seriously affect the position of investors and honest business enterprises in several ways. First, there is the threat of regulating or even banning the ICO market. Second, funding channeled to opportunistic ventures may eventually affect access to funding of value-creating projects, since investment capital is limited. Finally, losses in opportunistic ventures will reflect on the image of the ICO market, inevitably leading to an increase in the funding costs for all issuers.

3.5. The complexity of securities

The complexity of securities makes it hard to assess their fair value, generating inefficient pricing and asset bubbles and makes it difficult to discern fraud. During the 2007–2009 financial crisis, the focus was on the complexity of subordinated debt, preferred shares, and securitized assets. In the current ICO market, we observe that crypto-assets represent a manifold increase in complexity when compared to these securities. A crypto-asset is a sort of hybrid asset comprising rights of different types and is also a sort of bundling of different value sources. One particularly troubling aspect is this bundling of different rights (cryptocurrency, security, and utility).[33] It is well recognized in the economic literature that bundling represents a strategy to lure consumers or investors into buying useless assets, thereby creating a camouflaged Ponzi Scheme (Basu, 2010; Rubinstein & Spiegler, 2008). In the best-case scenario absent fraud, bundling makes it very hard to properly assess the economic value of the crypto-assets and may lead to mispricing or even bubble formations.

A further problem with most ICOs relates to the early development stage of the business venture. Even in the case of utility tokens—that is, tokens that are associated with products and services and that are not purchased with an aim to obtain a financial return—we observe an unexpected complexity in the tokens initially issued with the aim of financing the business. The impossibility of issuing functioning utility tokens leads to an initial issue of tokens that represent a derivative that can be swapped at a later date for a functioning utility token (e.g., for the SAFT project, see Batiz-Benet, Clayburgh, & Santori, 2017). Apart from raising several regulatory issues (the utility is not subject to financial regulation, but the derivative is), the derivative nature of these tokens leads to difficulties in valuation. If it is reasonable to assume that a consumer can assign a fair price to a product or service; it is less likely that the same consumer is able to fairly price a derivative of the same product or service.

In terms of the security component of tokens, we observe is that in most cases they are closer to a debt contract than to equity. Therefore, high-risk ventures are, in fact, being financed by debt of sorts, fostering a very high risk of adverse selection and the nature and complexity of the tokens is actually the source of these problems.

3.6. Inflated asset prices

In the 2007–2009 financial crisis, we observed a bubble in the real estate market driven by easy access to credit resulting from bank use of securitizations. The use of mortgage-backed securities and collateralized debt obligations fueled the real estate bubble, which in turn created a mispricing of the asset-backed securities themselves (Jarrow, 2011; Segoviano, Jones, Lindner, & Blankenheim, 2013). Currently, we observe a state of overheating and a general recognition that cryptocurrencies markets (Monaghan, 2018; Quinlan & Cheng, 2018) and ICO markets (Zetzsche et al., 2019) are possibly displaying a bubble formation driven from a purely speculative assessment of these assets. The fact that most ICOs are issued in cryptocurrencies (Zetzsche et al., 2019) makes it harder to properly assess the fairness of the issuance prices given the volatility of the cryptocurrencies themselves. Paradoxically, investors that are driven to alternative financial markets by the high prices of traditional financial securities are possibly creating a bubble by investing in assets that are probably more overvalued than the traditional financial securities they initially avoided.

---

[31] The responses of the Financial Services Agency of Japan (FSA) and the SEC to the hacking attacks on Coincheck and the DAO, are illustrative of this point. Once alerted, financial authorities in Japan launched an investigation into security gaps in all its crypto-asset exchanges and demanded that Coincheck improve its business practices and announced that the FSA would monitor its response to the theft (Uranaka & Wilson, 2018). In the case of the DAO, the SEC launched an investigation into the legality of the DAO organization and its ability to offer securities and, although it decided not to bring charges, the SEC found the DAO to be in violation of existing regulation on securities offerings.

[32] Signaling and screening are mechanisms initially discussed by Spence (1973) that aim to mitigate an adverse selection problem created by information asymmetries. In simple terms, honest business enterprises are able to credibly signal their quality to the market through signaling and qualified investors are able to perform a proper due diligence process on the upcoming ICOs through screening.

[33] Bundling practices are quite common in digital markets, as shown in Kwon, Anandalingam, and Ungar (2005).

3.7. Lax financial regulation

The 2007–2009 financial crisis emerged after a period of deregulation when, in 1999, President Clinton passed the Gramm-Leach-Bliley Act into law that repealed the Glass-Steagall Act, which, among other things, imposed a separation between investment and commercial banking. The current development of the market for ICOs moves parallel to a new wave of regulation in the financial markets (e.g., MIFID II, the Dodd-Frank Act, among others). However, it is safe to say that ICO markets are these days mostly unscathed by this regulatory fervor and can still be unregulated. Without taking any ideological side on the regulate / do not regulate discussion, we feel that unregulated markets create the perfect environment that attracts all economic agents aimed at committing fraud and deceit. It is indisputable that the two greatest financial crises the world has experienced (the 1929 crash and the financial crisis of 2007–2009) occurred exactly at the time of non-existent or lax regulations. In this sense, the current regulatory state of the ICO markets must generate legitimate concerns regarding the potential for another financial crisis, albeit one of more modest impact, because it is not yet clear if the ICO market is systemically relevant.

3.8. Perverse compensation systems

The nature of compensation is important in financial markets in the sense that it may lead agents into taking actions that diverge from the optimal. Following the 2007–2009 financial crisis, much was written on bankers' compensation schemes and the risk-taking incentives they induced (see Bebchuk, Cohen, & Spamann, 2010; Rajan, 2008). Currently, we observe similar problems with the business ventures that try to obtain financing from ICOs. Three main problems are identifiable in this case:

1. Most ICO issuers are in such an early stage of their business ventures that they have no source of income other than the capital advanced by investors in the ICO. This advanced collection of funds reduces the incentives to develop the business further and may actually lead to early abandonment (Valenzuela, 2017).
2. It is common practice to have the proceeds from the ICO transferred to the private wallet of the issuer; this situation makes it unclear if the issuer actually wants funds to finance a business venture or simply obtain a direct personal gain from the ICO (see Matsumura, 2017).
3. There is no proper disclosure of information regarding the compensation of key staff both within and outside of the organization issuing the tokens. This fact makes it hard for investors to assess the reasonability of the amounts raised and its real application, which may lead to suspicions of misdealing and misappropriation of funds (see Tezos ICO, Bart, 2017).

3.9. Importance of the ICO market problems

The problems identified in this section are relevant for various reasons. First, the future of Blockchain technology and specifically the market for the issuance and trading of tokens may depend on how effectively market agents are able to address these problems. As the problems multiply and the ICO market grows exponentially, regulators are showing less willingness to allow market agents to address these problems (e.g., see the cases of South Korea and China). Second, given the current size and growth of the ICO market, these problems are more likely to affect the whole economy. Recent examples from the Fintech world show us how fast a business can change from too-small-to-care to too-big-to-fail (e.g., see Xie & Yap, 2017 and the case of the Chinese money market fund Yu'e Bao).[34] Finally, the fact that most of the problems observed in the ICO market are the same problems that occurred at the beginning of the 2007–2009 financial crisis is particularly worrying. Schwarcz (2011) points out that a TOC failure, complacency of market participants, complexity of markets and securities, and conflicts of interest[35] were the critical market failures that culminated in the financial crisis. Blinder (2013) puts forward a series of weaknesses that were at the core of the crisis, including inflated asset prices, complexity of financial securities, lax financial regulation, and perverse compensation systems.

The next section analyzes the current solutions that have been proposed to address the problems identified in this section.

4. Addressing the problems of the ICO market

4.1. Self-regulation

The ICO industry has been particularly active in identifying the main problems that are currently afflicting the ICO market and proposing solutions through self-regulatory initiatives. These initiatives are often triggered by crises and the fact that the ICO industry is making such self-regulatory efforts is indicative of the importance of these problems. Most of the current efforts are devoted to the development and adoption of codes of conduct (e.g., see Crypto Valley, 2018; Matsumura, 2017), however, the effectiveness of these efforts is uncertain (Lagace, 2007). First, there is little empirical evidence that the adoption of industry-led self-regulation and codes of conduct lead to actual improvements. Second, these initiatives are often greeted as marketing tools that aim at deterring critics and governmental regulatory initiatives. Finally, the existence of a multitude of codes of conduct may create more problems than the ones they try to address since the coexistence of multiple standards may confuse stakeholders and generate cost inefficiencies.

Recently, we have witnessed a positive development that addresses most of the failures of previously discussed industry-led codes of conduct, because for any self-regulatory initiative to be successful it is important that it involves a significant number of agents and independent third parties.[36] The most recent self-regulatory initiative was able to join different market agents such as the Waves Platform, the ICO Governance Foundation, Ethereum, and Deloitte representing the independent third party (see Sundararajan, 2017). The self-regulatory body that is being created will develop reporting, regulatory, fiscal, accounting, KYC, and business due diligence standards for ICOs. The involvement of many parties harmonizes the codes of conduct and allows cost efficiency when internalizing the negative externalities generated by opportunistic agents and hackers.[37]

As with the Internet, Blockchain is evolving towards a set of

---

[34] Zetzsche et al. (2019) attribute the initial development of the progression from too-small-to-care to too-big-to-fail to Douglas W. Arner and Jànos Barberis in Regulating FinTech Innovation: A Balancing Act Seminar, Asian Institute of International Financial Law (Apr. 1, 2015).

[35] Several of the problems we have analyzed can easily be framed in the context of conflicts of interest between different market agents. Consider the case of the pre-sales and flipping and pump-and-dump schemes. The former case is clearly a conflict between qualified and retail investors and the latter a conflict between agents that manipulate the markets and retail investors. Compensation schemes can also easily be framed as a conflict of interests.

[36] Lagace (2007) argues that third party verification represents a crucial element to assess self-regulatory initiatives and the adoption of codes of conduct

[37] Internalizing negative externalities is always a costly process. Consider the case of banking systemic risk and the proposals to create a systemic self-funded bank fund (see Omarova, 2011; Schwarcz, 2011). These initiatives can only be cost-efficient through the involvement of a significant number of agents.

applications that configure broader and more complex scenarios. The tension between their technological underpinnings and practical demands determines the conflicting nature of ICOs, and requires a proper Blockchain standard (Hardjono, Lipton, & Pentland, 2018). The International Standards Organization (ISO) is currently developing a set of standards for Blockchain and other DLTs through their ISO/TC 307 technical committee. The standards will address different aspects such as security and privacy, identity, governance, and interoperability of the different DLTs and of the smart contracts that are used to support an ICO. Although the standards are still under development and little is known apart from its objectives, its comprehensive nature will address most of the problems we have discussed in Section 3. The involvement of the ISO organization is very welcome because contrary to self-regulatory initiatives, independent certifications have shown to have a positive impact in terms of performance. According to Toffel (2006), firms that adopt certification standards are better in terms of the standard-measured performance than those that do not adopt them.[38]

The development of self-regulatory initiatives and the creation of certification standards are much needed in the current ICO markets. However, these initiatives should not be perceived as a panacea,[39] and given the current dynamics of ICO markets, it may even be too soon to start imposing standards. In Lagace (2007), Prof. Toffel raises the question of whether standardizations reduce workers' skills due to routinization of tacit knowledge and skills. The question is particularly important in the Blockchain environment that is characterized as being highly innovative. In this context, there is always the risk that adoption of standards too early may stifle innovation.

4.2. Problems become business opportunities

The current state of ICOs is lacking a serious due diligence process before and during the issuance stage. Given the lack of fundamental information to support a rational investment decision, some agents have stepped in to provide an external and independent assessment of the financial performance of the firms obtaining financing. Hartmann, Wang, and Lunesu (2018) identify 28 websites that evaluate upcoming and ongoing ICOs. The founders of these websites are basically setting up for-profit businesses that mitigate the effects of the information asymmetries between issuers and retail investors.

However important these efforts may be in mitigating the effects of information asymmetries, they still fall short of the level of professionalism of traditional financial markets in terms of the financial analysis performed. Hartmann et al.'s (2018) analysis of the aforementioned 28 websites reveals great heterogeneity in the evaluation process and not all the sites examined are transparent regarding aspects of the evaluation process. This process also reveals considerable differences in terms of ICO items analyzed and the evaluation process itself, with some sites relying on an internal team of analysts while others rely on crowd-based evaluations. The outcome of the evaluation processes also differs considerably with some sites providing a qualitative analysis of the evaluation process in the form of a report and others providing a score or rating classification. Hartmann et al. (2018) highlight important aspects of ICOs that are not covered by current evaluations such as the technical information regarding the projects underlying the ICOs, the Blockchains used, the software depository, and the quality of smart contracts.

This type of independent evaluators is crucial for the functioning of financial markets not only in terms of reducing the problems of information asymmetries but also in terms of changing the behavior of poorly rated firms. In an analysis of the behavior of firms being rated, Chatterji and Toffel (2010) demonstrate that firms that were poorly rated subsequently showed an improvement in performance that surpassed a control group of unrated and highly rated firms.

As such, this area is expected to develop further and it not unreasonable to anticipate that more firms and evaluation methods will appear and that some traditional ratings firms may move into the Blockchain ecosystem as the importance of ICOs increases.

4.3. White hacking

A hacker is defined by the Internet Users' Guide as "A person that delights in having an intimate understanding of the workings of a system, computers, and computer networks in particular." Notice that this definition does not mention the moral nature of the hacker. The most notorious hackers have become those that have performed illegal actions or outright theft. Less advertised is the fact that hackers have in the past been known to right some wrongs and they are usually referred to as white hackers.[40] White hackers are currently being employed as software auditors and testers. Through their knowledge of how to break and disrupt systems, they are able to test and incorporate improvements in Blockchains and smart contracts (see Suberg, 2017). The altcoin Dash is currently employing white hackers to hack its Blockchain and expose its vulnerabilities. With the incentive of a "Bug Bounty," several invited hackers will identify and fix security flaws. A similar arrangement was made between the SmartOne legal services marketplace and the White Hat crypto-asset hacker system to ensure security for the marketplace of the token LEGAL (The Merkle, 2017).

The actions of white hackers have become notorious in the Blockchain ecosystem and in some cases, they have acted without any "Bug Bounties" incentive. In the case of the hacking attack on Parity, discussed in Section 3.3, white hackers mitigated a hacking theft by exploiting the same vulnerability used to steal the funds.

While the importance of white hackers is unquestionable in prevention, through the testing, auditing, and development process of Blockchains and smart contracts, their use to mitigate thefts or fraud is more questionable. Regardless of how notorious their actions have become, it is not reasonable to rely on white hackers to address criminal hacking attacks. First, although their actions have become notorious, they represent little more than anecdotes and in most hacking attacks, white hackers did nothing to stop them. Second, and regardless of their good intentions, white hackers can expose themselves to criminal charges by exploiting the same vulnerabilities that criminal hackers have exploited to commit their crimes. Finally, some of the apparently selfless actions of white hackers may be considered little more than gimmicks aimed at promoting their name and services as system testers and auditors.

4.4. Transparency

Open source is at the very heart of Blockchain inception and evolution. Although there are some proposals whose source code is not publicly accessible (e.g., Enigma, nChain, SETL), it is highly likely that most of them will eventually follow a path similar to that of Corda, which is currently an open-source project that started out as a proprietary project. Open source emerged in response to the proprietary codes developed by large software firms, mainly to address the limitations of the proprietary model. The infancy of the open-source model can be traced back several decades; however the "commercial" model is more recent

---

[38] The empirical analysis performed in Toffel (2006) focused on the environmental certification ISO 14000.

[39] These initiatives address many of the problems that we have previously discussed; however, other problems of a more technical nature (e.g. vulnerability to hacking attacks) are only marginally affected by these harmonization efforts.

[40] White and ethical hacking are the results of academic research, as they occur with the security evaluation of smart contracts (Nikolic et al., 2018). In fact, since Blockchain is far from being considered a mature technology; its improvement in terms of security and efficiency calls for an intensive collaboration between academic and IT professionals in general.

and is linked with the emergence of "free" software. Business enterprises rejected "free" software; however, open source does not have the negative business connotations of free software.[41] By creating a collaborative model in terms of code development, the open-source model is able to develop better and more resilient software.[42] Open-source development encompasses the means to expand itself and self-perpetuate through particular copyright agreements. Open-source code uses Free and Open-Source Software (FOSS) licenses. The most popular FOSS license is the MIT License, through which all developers that use and develop FOSS software are obliged to release their developments, even if they are commercial, under the same non-proprietary license agreement.[43] The source code is kept in software repositories; these represent hosting facilities that store and keep track of changes in the code developments, promote discussion, record bugs, and provide documentation of the stored software (e.g., SourceForge, GitHub, BitBucket, GitLab, etc.).

Crowdsourcing is another key component in open-source development (Mao, Capra, Harman, & Jia, 2017), with platforms such as Stack Overflow especially relevant to the life cycle of open-source development (Vasilescu, Filkov, & Serebrenik, 2013). However, with respect to security aspects, it is necessary to emphasize that overconfidence regarding open access forums can lead to vulnerable systems (Fischer et al., 2017). This being the case, there is a desire to educate open-source developers in secure programming techniques and encourage the responsible use of copy and paste (i.e., the widely accepted code reuse) methodologies. As a further backup, the open-source community also provides for the automatic evaluation of the security of source code (Acar et al., 2017). The initiative by GitHub of including security alerts in the platform is of major relevance (see Santos, 2018).

Raymond (1999) discusses the advantages of open-source development. An important aspect is the involvement of many highly motivated programmers: First, they develop software for their own use, something that does not always happen when the software is developed to meet a request or an order. Second, there is always a programmer willing to pick up the work left by a less motivated or unavailable programmer. Finally, code developed in collaboration is not only optimally written but is also constantly being re-written, thereby eliminating redundancies, the duplication of R&D efforts, inefficiencies, and potential bugs.

Open source has several implications for Blockchain (Valkenburgh, 2017) and it is at the core of the decentralized Blockchain model since it is developed and improved by many programmers. It reduces the technical entry barriers for potential Blockchain developers since it allows them to access, learn from, and even use existing code (i.e. new enterprises develop their own Blockchain by forking an existing Blockchain). Furthermore, the open-source model gives much more transparency to Blockchain developments by making all kinds of information and data public and easily accessible. Commercially, this serves to engage clients and users, since it provides a channel to receive comments and to conduct corresponding software customization and improvements, contributing to perfecting both the technology and the end user experience.

This level of transparency of the Blockchain, the smart contracts, and of the very development of the business enterprise has strong implications for ICOs. First, access to the code of the smart contract ensures that the firm has no incentive to lie, exaggerate, or deceive in its white paper or in other forms of communication and access to the source code increases the probability of ICO success (Adhami et al., 2018). The use of open source therefore reduces the issue of scams and deceits.[44] On the other hand, this level of transparency can increase the number of hacking attacks, because hackers also have access to the smart contract code and are therefore able to identify any bugs or vulnerabilities more easily.[45] Second, the possibility to observe and assess the level of business development makes it easier to anticipate an exit scam and mitigate the effect of perverse compensation schemes. Perverse compensation schemes and the engagement in high-risk ventures can be mitigated by linking the access to funding to the accomplishment of specific and measurable business development milestones. However, this level of disclosure may also be accompanied by a loss of competitive advantages and encourage copycat projects.

4.5. Forks

In Blockchain, project forks can be divided into soft and hard forks; soft forks are usually associated with protocol upgrades and two versions of the Blockchain usually run in parallel, whereas hard forks imply a modification of the consensus rules (Antonopoulos, 2017). Soft forks are not intended to create two competing Blockchains since only one is expected to survive as users adopt the updated protocol. Hard forks on the other hand create two Blockchains and may create significant problems for users, exchanges, and wallets. Throughout the history of Blockchain there have been several planned hard forks (e.g., the implementation of Segregated Witnesses in the Bitcoin protocol in 2017). However, contentious hard forks represent one of the most critical controversies in the Blockchain community. The lack of consensus usually extends beyond the hard fork implementation and the two teams of developers are in many cases unwilling to work together to solve the problems for users, exchanges, and wallets through a clean split, forcing users and exchanges to run splitter contracts individually and in some cases result in the duplication of crypto currencies. Moreover, in the past, these disputes led to a schism in the Ethereum community after being applied to solve the DAO hack, or the split into Bitcoin and Bitcoin cash after increasing the block size in 2017.

The case of the DAO is an example of the use of a hard fork to address a hacker theft. Through the implementation of a hard fork departing from a block prior to the theft, history can be re-written in a way that the theft is not recorded in the new branch of the Blockchain. Verge is another famous case of the use of a hard fork to address a 51% attack (see Sedgwick, 2018). Verge's attack case and solution is quite interesting in the sense that Verge developers used a hard fork following the attack to prevent the attacker from, among other things, being able to rewrite Verge's history.[46]

Although forks appear to be a simple technological solution for almost any problem that may arise in the Blockchain environment, the reality is that they raise as many problems as the ones they try to address. The hard fork is therefore akin to a nuclear solution in the Blockchain protocol and its application after the DAO hack was the first case where the goal of the hard fork was not technical but regulatory (De Filippi & Wright, 2018).

A non-technical hard fork means that, in a chain of blocks, history

---

[41] Linux, one of the paradigms of open source, is widely adopted in business environments. In this regard, the incorporation of Microsoft into the Linux Foundation is highly significant, and even more relevant is its acquisition of GitHub.

[42] See Sijbrandij (2018) for a description of the historical developments of open source since its inception to its commercial application.

[43] This is the reason why many of these licenses are referred to as viral or copyleft software licenses.

[44] Bartoletti et al. (2020) identify Ponzi schemes in Ethereum through the analysis of the code in smart contracts.

[45] In the case of the hacking attack on The DAO (see Section 3.3), the hacker was able to transfer part of the funds raised with the ICO by exploiting a vulnerability in the code of the smart contract that would most likely go undetected if the code was not open for consultation.

[46] In a 51% attack, an agent is able to control more than 50% of the network's mining hashrate, which under a Proof or Work system would allow this agent to monopolize all future block mining, implement double spending, block transactions, and even change historical blocks.

can be rewritten if token holders "democratically" approve the decision. This possibility to rewrite history has no close parallel in traditional financial markets and it in fact contradicts two defining features of Blockchain: rewriting the history of transactions, and introducing human intervention (Yermack, 2017). Traditional governance mechanisms allow agents to change the future of organizations and financial markets. Blockchain governance and the option to implement forks may not only change the future of organizations and markets in the Blockchain environment but also their past.[47] The ethical and governance implications of this are tremendous and therefore the Blockchains methods of consensus are a crucial element to always take into account.

4.6. Other solutions and technological developments

Some particular problems of ICO markets have also particular solutions and, in some cases, they even trigger technological developments.

In the case of the hacking attack on CoinDash, in which a hacker replaced the wallet address of CoinDash with their own in the webpage supporting the ICO, the solution implemented was to distribute tokens to all the investors affected (Zhao, 2017). This solution was implemented because the ERC-20 token standard used does not enable token revocation. Naturally, the stolen tokens are still valid, and this particular solution will never be optimal since it implies a value dilution effect for all token holders.[48] New token standards such as the ERC-777[49] include several functionalities that mitigate this type of hacking attack. Specifically, hook functionalities enable the possibility of further controlling tokens. The ERC-777 also proposes the creation of a new type of actor for tokens management, the operator. The standard defines a set of default operators, which are installed for all holders of tokens. The operators can be used to conduct gas deduction and, consequently, to reduce the complexity of sending transactions. Moreover, the token holder can revoke authorization from operators, therefore preventing an attack such as the one CoinDash suffered. Another possibility of diminishing the impact of stolen or unspent tokens comes from the implementation of vesting functionalities as done by OpenZeppelin.[50]

The identification of fake tokens, malicious smart contracts, and simple copycats is a complex task since the source code of smart contracts is rarely made available.[51] However, programmers were able to address this problem by decompiling the bytecode that is stored in the Blockchain, and to subsequently perform an exhaustive analysis to detect either malicious code patterns or the emission of copycat tokens. In this regard, static and dynamic tools for the analysis of the bytecode in the Blockchain are being developed to identity possible attacks and fraudulent ICOs (Nikolic, Kolluri, Sergey, Saxena, & Hobor, 2018).

5. Conclusions and discussion

Blockchain represents an information protocol characterized by being a digital, decentralized and disintermediated solution. These characteristics are part of its attraction with the potential to reduce costs while increasing the speed of transactions and providing previously unimaginable levels of transparency. Of the many uses of Blockchain, ICOs are one of most recognized applications. As so, the ICO market assumed the characteristics of Blockchain, additionally to the fact that it was also an unregulated market, making it a market different to what existed in terms of financing solutions. Regardless of these differences, our analysis shows that the ICO market already displays most of the problems of traditional financial markets. It is particularly worrying that many of these problems are exactly those that existed at the genesis of the 2007–2009 financial crisis. In this sense, our analysis shows problems and solutions that are shared with traditional financial markets but also problems and solutions particular to the ICO markets. This section draws conclusions and implications from both sets of problems/ solutions.

As the ICO market evolved, clear tensions arose between what the technology offered and what the nature of the financial transactions demanded. Financing markets are characterized by asymmetries of information between the borrower and the investor, and these are enhanced with innovative products, non-accredited investor participation and complex securities. Our analysis leads us to conclude that the ICO market will likely not be characterized as decentralized, disintermediated or unregulated in the near future.

With respect to decentralization, we observed that although issuers are able to DIY[52] the issuance and trading process of a token, they overwhelmingly choose to use the Blockchain and the ERC smart contracts of Ethereum. Similar evidence exists with respect to trading with most tokens being listed in centralized crypto exchanges. This centralization process has important repercussions for the establishment of standards and for the distribution of market power. Although there are still ongoing efforts to define ICO standards (e.g. ISO Technical Committee and several ICO market associations) competition has already set de facto standards for Blockchain and smart contracts. Given the nature of the Ethereum Foundation we do not expect the emergence of market power problems, nonetheless, such centralization does raise important concerns in digital markets prone to hacking attacks in which code vulnerabilities are constantly being exploited.

With respect to disintermediation, although made technologically redundant, the problems we analyze show that intermediaries can mitigate many of the asymmetrical information problems and most of the intermediation we observe is endogenously promoted by market participants. Most notably we have technical and financial Blockchain ratings firms seizing the opportunity to profit from mitigating asymmetries of information. Other examples of intermediation are the proposal to create operator agents under the ERC-777 Ethereum standard, ICO auditors as discussed in Collao and Winship (2019), ICO advisors and even market makers. The very fact that issuers are overwhelmingly choosing to issue under the Ethereum Blockchain and listing in centralized crypto exchanges also makes these agents important intermediaries in the ICO markets.

With respect to regulation, more and more governments and international institutions are leaving the sandbox approach and are moving in to regulate crypto assets (Butterfill & du Cros, 2021; Guida, 2021; Ma, 2021). This move is a response to some of the problems we analyzed, it is evidence that the self-regulatory efforts are falling short of what is required, but it is also an acceptance of these markets and a recognition of their current importance. ICO regulation will always be a great challenge given the digital and global nature of this market whereby regulatory arbitrage and innovation stifling will always be major concerns (Pasanisi, 2018). Nonetheless, the gains from a harmonized global regulation of ICOs are manyfold:

---

[47] According to Siegel (2016), when a fork is implemented, as in the case of the Ethereum fork implemented by the Ethereum Foundation to address the DAO hacking attack, the Foundation becomes simultaneously a judge and jury, something that was clearly not intended when the Ethereum Blockchain was developed.

[48] The hacking attack on CoinDash had further developments with the hacker returning 30,000 of the initially 43,000 stolen ether tokens (De, 2018). There is no real justification and only speculation as to why the hacker partially returned the funds, which, measured in fiat currency, were actually worth more than the initial amount stolen (Osborne, 2018).

[49] For details of the ERC-777 standard, see https://github.com/ethereum/EIPs /blob/master/EIPS/eip-777.md.

[50] The complete description of the OpenZeppelin vesting functionality can be found at https://github.com/OpenZeppelin/token-vesting-ui

[51] According to Zhou et al. (2018), around 77.6% of smart contracts are not properly associated with the corresponding source code.

[52] In Adhami et al. (2018) analysis of ICOs around 12% of their sample was fully decentralized with no formal business being set up.

1. Corporate fraud, hacking attacks and market manipulation will have a clear framework for prosecution and will in expectation be less common.
2. Market volatility will be reduced by eliminating regulatory uncertainty.
3. Tax avoidance and tax arbitrage will be curtailed.
4. End of the ongoing cat and mouse game between regulators and market participants that has been leading to an increase in the complexity of securities (e.g. hybrids and derivatives) and of issuance models (e.g. Token Generation Events), many times simply to evade regulation.

Given recent advances in the harmonization of corporate tax rates of multinationals (Thomas, 2021) and the regulatory upgrade of China following its 2021 May's crackdown on mining and trading activities (Ma, 2021), we feel the timing may be right for achieving similar global regulatory advances with respect to crypto markets.

This paper focuses on anticipating the extent to which the problems and solutions of the ICO market will shape its future. In this respect we identify some clear trends. First, with respect to regulation and intermediation, all evidence points to a no going back case in both cases, however with centralization the future is not so clear. Centralize vs decentralize ICOs is one of the important current discussions, since both alternatives present strong positive aspects. As mentioned previously, centralization raises important security concerns and the short history of ICOs has showed us that the threat of hacking attacks should never be overlooked. Decentralization on the other hand, potentially increases security, but makes it harder to implement standards and enforce effective investor protection. Since both aspects are crucial for the development of the ICO markets all future developments need to be properly monitored and assessed. Second, the dynamic nature of crypto markets raises the possibility that ICOs may end up just being the precursor of alternative crypto financing solutions. The arrival of alternative solutions such as STOs, IEOs, IDOs or TGEs, might conduce to a process of specialization that may end up draining out the ICO markets.

With respect particular solutions to the ICO market such as Forks and new Smart Contract Standards, they have to potential to solve problems but also to create new ones. New smart contract standards are the natural way forward for this technology and they represent innovative technical solutions to classic economic problems (e.g. mitigate perverse compensation schemes, prevent some types of fraudulent ventures or morally reprehensive actions such as flipping, facilitate regulatory compliance, streamline insolvencies, etc.). In this sense, as Yermack (2017) points out, Blockchain technology has the potential to significantly improve Corporate Governance through an impressive level of transparency and its ability to constrain the actions of agents based on contingent events. On the other hand, the possibility to enforce hard forks raises important Governance issues since it allows re-writing the past of an organization. It remains to be seen if Blockchain will meet its Corporate Governance expectations while addressing the problems raised by Blockchain Governance itself.

Our results have clear implications for investors, issuers and regulators. First, investors need to conduct thorough due diligence because of the risks they face when investing in an ICO. Additionally to increased business risk associated with tech startups, they face fraud risk, important cybersecurity issues and even legal risks. Second, issuers need to take legal and cybersecurity issues very seriously. Even when using well established and reputable solutions for Blockchains, smart contracts or crypto exchanges, issuers should secure the services of software auditors and testers to ensure protection from hacking attacks. Under the current volatile legal landscape, the global issuance of complex securities may very easily lead to a violation of securities issuance laws, therefore it is important to secure legal advice in what concerns the choice of issuance model and to guarantee regulatory compliance. Finally, the biggest current challenges fall on the backs of regulators. It is clear that the sandbox approach and simply putting out warnings (e.g. SEC, 2013) and

recommendations is no longer working. Zetzsche et al., 2019 even argues that by advertising the unregulated nature of ICO market, warnings may end up having the perverse effect to attract undesirable promoters. The current problems of ICO markets require legislation that acknowledges the economic and technical idiosyncrasies of a global digital market. Failure to do so, will prolong the current state of impunity of fraudsters and hackers, keep volatility high, promote increased complexity of securities and issuance models and foster regulatory and tax arbitrage with the consequential loss of competitive advantages of countries with stricter regulatory approaches.

Our analysis is essentially of a qualitative nature, but a quantitative analysis of these problems detailing their incidence level and importance is an ongoing research process. Future research will also focus on the on-going centralize/decentralize debate and on the ongoing evolution of issuance models and securities design. In this sense, we expect that future technical developments regarding Blockchain and academic research will move in tandem.

References

Acar, Y., Stransky, C., Wermke, D., Weir, C., Mazurek, M. L., & Fahl, S. (2017). Developers need support, too: A survey of security advice for software developers. In *Proceedings - 2017 IEEE cybersecurity development conference, SecDev 2017* (pp. 22–26).

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

Angeris, G., Evans, A., & Chitra, T. (2020). When does the tail wag the dog?. In *Curvature and market making*. Retrieved from https://arxiv.org/abs/2012.08040.

Antonopoulos, A. M. (2017). *Mastering bitcoin: Programming the open blockchain* (2nd ed.). Sebastopol, US: O'Reilly Media.

Aspris, A., Foley, S., Svec, J., & Wang, L. (2021). Decentralized exchanges: The "wild west" of cryptocurrency trading. *International Review of Financial Analysis, 77*, 101845.

Back, A. (2002). Hashcash: A denial of service counter-measure. Retrieved from http://www.hashcash.org/papers/hashcash.pdf.

Baker, N. (2018). Widespread fraud in ICOs and penny stocks shocked SEC's jay clayton. In *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-04-10/widespread-fraud-in-icos-and-penny-stocks-shocked-sec-s-clayton.

Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications, 4*. https://doi.org/10.1038/nprot.2017.031

Barsan, I. (2017). Legal challenges of initial coin offerings. *Revue Trimestrielle de Droit Financier, 3*, 54–65.

Bart, K. (2017). Record ICO's Swiss ties raise eyebrows. Retrieved from https://www.finews.com/news/english-news/28253-tezos-ico-swiss-foundation-dls-kathleen-arthur-breitman.

Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. (2020). Dissecting Ponzi schemes on Ethereum: Identification, analysis and impact. *Future Generation Computer Systems, 102*, 259–277.

Basu, K. (2010). A marketing scheme for making money off innocent people: A user's manual. *Economics Letters, 107*, 122–124.

Batiz-Benet, J., Clayburgh, J., & Santori, M. (2017). The SAFT project: Toward a compliant token sale framework. Retrieved from https://www.cooley.com/-/media/cooley/pdf/reprints/saft-project-whitepaper.ashx.

Bebchuk, L. A., Cohen, A., & Spamann, H. (2010). The wages of failure: Executive compensation at bear Stearns and Lehman 2000–2008. *Yale Journal on Regulation, 27*, 257–282.

Benedetti, H., & Kostovetsky, L. (2021). Digital tulips? Returns to investors in initial coin offerings. *Journal of Corporate Finance, 66*, 101786.

Berkmen, S., Gelos, G., Rennhack, R., & Walsh, J. (2012). The global financial crisis: Explaining cross-country differences in the output impact. *Journal of International Money and Finance, 31*, 42–59.

Biggs, J. (2018). Exit scammers run off with $660 million in ICO earnings. Retrieved from https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/.

Blinder, A. (2013). *After the music stopped: The financial crisis, the response, and the work ahead*. New York, US: Penguin Press.

Brito, J. (2013). Beyond silk road: Potential risks, threats, and promises of virtual currencies. In *Testimony to the senate committee on homeland security and governmental affairs, November 18*.

Brunnermeier, M. (2009). Deciphering the liquidity and credit crunch 2007-2008. *Journal of Economic Perspectives, 23*, 77–100.

Butterfill, J., & du Cros, N. (2021). The state of crypto regulation - June 2021. Retrieved from https://coinshares.com/insights/crypto-regulation-june-2021.

Campello, M., Graham, J., & Harvey, C. (2010). The real effects of financial constraints: Evidence from a financial crisis. *Journal of Financial Economics, 97*, 470–487.

Catalini, C., & Gans, J. (2019). Initial coin offerings and the value of crypto tokens. In *NBER working paper series - working paper 24418*.

Chatterji, A., & Toffel, M. (2010). How firms respond to being rated. *Strategic Management Journal, 31*, 917–945.

Chen, K. (2019). Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals. *Electronic Commerce Research and Applications, 36*, 100858.

Choudhury, R. (2017). *Many ICOs are fraudulent, say men behind two top bitcoin rivals.* CNBC. Retrieved from https://www.cnbc.com/2017/11/17/many-icos-are-fraud-according-to-ethereum-co-founder-and-ripple-ceo.html.

Colagrossi, M. (2018). Banks' fear of crypto turns to FOMO. Retrieved from https://cryptobriefing.com/banks-fear-crypto-turns-fomo/.

Collao, V., & Winship, V. (2019). The new ICO intermediaries. *Italian Law Journal, 5*, 731–755.

Collomb, A., De Filippi, P., & Sok, K. (2018). From IPOs to ICOs: The impact of blockchain. Retrieved from https://ssrn.com/abstract=3185347.

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: Designing secure systems that people can use.* Sebastopol, US: O'Reilly Media.

Crypto Valley. (2018). Mission and policy framework. Retrieved from https://cryptovalley.swiss/codeofconduct/.

Dai, W. (1998). B-Money. Retrieved from http://www.weidai.com/bmoney.txt.

Daluwathumullagamage, D., & Sims, A. (2020). Blockchain-enabled corporate governance and regulation. *International Journal of Financial Studies, 8*, 36.

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code.* Cambridge, US: Harvard University Press.

De, N. (2018). Hacker returns $26 million in ether months after ICO theft. Retrieved from https://www.coindesk.com/hacker-returns-26-million-ether-months-ico-theft/.

Duchin, R., Oguzhan, O., & Sensoy, B. (2010). Costly external finance, corporate investment, and the subprime mortgage credit crisis. *Journal of Financial Economics, 97*, 418–435.

Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In *, 92. Advances in cryptology: Proceedings of crypto* (pp. 139–147).

Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). *A first look at the usability of bitcoin key management.* Retrieved from doi: https://doi.org/10.14722/usec.2015.23015.

EY. (2017). EY research: initial coin offerings (ICOs). Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-research-initial-coin-offerings-icos.pdf.

Fang, L., Bouri, E., Gupta, R., & Roubaud, D. (2019). Does global economic uncertainty matter for the volatility and hedging effectiveness of bitcoin? *International Review of Financial Analysis, 61*, 29–36.

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

Fisch, C., & Momtaz, P. (2020). Institutional investors and post-ICO performance: An empirical analysis of investor returns in initial coin offerings (ICOs). *Journal of Corporate Finance, 64*, 101679.

Fischer, F., Böttinger, K., Xiao, H., Stransky, C., Acar, Y., Backes, M., & Fahl, S. (2017). Stack overflow considered harmful? The impact of copy & paste on android application security. *IEEE Symposium on Security and Privacy (SP), 2017*, 121–136.

Flood, J., & Robb, L. (2017). Trust, anarcho-capitalism, blockchain and initial coin offerings. In *Griffith University Law School Research Paper No. 17-23*.

Fröwis, M., & Böhme, R. (2019). The operational cost of Ethereum airdrops. In C. Pérez-Solà, G. Navarro-Arribas, A. Biryukov, & J. Garcia-Alfaro (Eds.), *Data privacy management, cryptocurrencies and Blockchain technology* (pp. 255–270). Berlin, Germany: Springer.

Gandal, N., Hamrick, J., Moore, J., & Oberman, T. (2018). Price manipulation in the bitcoin ecosystem. *Journal of Monetary Economics, 95*, 86–96.

Georgiev, G. (2021). What is an initial DEX offering (IDO)? How is it different than ICO & IEO?. Retrieved from https://cryptopotato.com/what-is-an-initial-dex-offering-ido-how-is-it-different-than-ico-ieo/.

Gino, F., & Ariely, D. (2012). The dark side of creativity: Original thinkers can be more dishonest. *Journal of Personality and Social Psychology, 102*, 445–459.

Giudici, G., & Adhami, S. (2019). The impact of governance signals on ICO fundraising success. *Journal of Industrial and Business Economics, 46*, 283–312.

Glasius, M., & Pleyers, G. (2013). The global moment of 2011: Democracy, social justice and dignity. *Development and Change, 44*, 547–567.

Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *Proceedings on Privacy Enhancing Technologies, 4*, 179–199.

Gordon, S. (2017). Anatomy of an ICO pump and dump. Retrieved from https://medium.com/@ProgRockRec/anatomy-of-an-ico-pump-and-dump-325c735d5f19.

Greco, G. M., & Floridi, L. (2004). The tragedy of the digital commons. *Ethics and Information Technology, 6*, 73–81.

Griffin, J., & Shams, A. (2020). Is bitcoin really un-tethered? *The Journal of Finance, 75*, 1913–1964.

Guida, V. (2021). Washington wakes up to crypto influence amid infrastructure fight. Retrieved from https://www.politico.com/news/2021/08/09/cryptocurrency-influence-washington-infrastructure-fight-502792.

Gurrea-Martínez, A., & Remolina, N. (2020). Corporate governance challenges in initial coin offerings. In *Singapore Management University School of law research paper 19/2020*.

Haffke, L., & Fromberger, M. (2020). ICO market report 2019/2020. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770793.

Haffke, L., Fromberger, M., & Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML directive (EU) and how to address them. *Journal of Banking Regulation, 21*, 125–138.

Hardjono, T., Lipton, A., & Pentland, A. (2018). Towards a design philosophy for interoperable blockchain systems. Retrieved from http://arxiv.org/abs/1805.05934.

Hartmann, F., Wang, X., & Lunesu, I. (2018). Evaluation of initial cryptoasset offerings: The state of the practice. In *2018 international workshop on blockchain oriented software engineering (IWBOSE)* (pp. 33–39).

Hermann, E., Trimborn, S., Ong, B., & Lee, T. (2018). The cross-section of crypto-currencies as financial assets: An overview. *Handbook of Blockchain, Digital Finance, and Inclusion, 1*, 145–173.

Howell, S., Niessner, M., & Yermack, D. (2020). Initial coin offerings: Financing growth with cryptocurrency token sales. *Review of Financial Studies, 33*, 3925–3974.

Huang, W., Meoli, M., & Vismara, S. (2020). The geography of initial coin offerings. *Small Business Economics, 55*, 77–102.

Hussey, M. (2019). What are token generation events (TGEs)?. Retrieved from https://decrypt.co/resources/token-generation-events-what-are-they-guide.

Ibba, S., Pinna, A., Baralla, G., & Marchesi, M. (2018). ICOs overview: Should investors choose an ICO developed with the lean startup methodology? *XP 2018: Agile Processes in Software Engineering and Extreme Programming*, 293–308.

Im, F. (2021). South Korea looks to ban crypto exchange employees from trading on their own platforms. Retrieved from https://www.coindesk.com/south-korea-looks-to-ban-crypto-exchange-employees-from-trading-on-their-own-platforms.

Ismailidou, E. (2016). Treasury yields plunge to all-time lows on 'insatiable' demand for safety. Retrieved from https://www.marketwatch.com/story/treasury-yields-tumble-to-record-lows-as-brexit-fears-resurface-2016-07-05.

Jarrow, R. (2011). The role of ABS, CDS and CDOs in the credit crisis and the economy. In A. Lo Blinder, & R. Solow (Eds.), *Rethinking the financial crisis* (pp. 210–234). New York, US: Russell Sage Foundation.

Ji, Q., Bouri, E., Lau, C., & Roubaud, D. (2019). Dynamic connectedness and integration in cryptocurrency markets. *International Review of Financial Analysis, 63*, 257–272.

Jia, K., & Zhang, F. (2017). Between liberalization and prohibition. In M. Campbell-Verduyn (Ed.), *Bitcoin and beyond* (pp. 88–108). London, UK: Routledge.

Kaal, W. (2018). Initial coin offerings: The top 25 jurisdictions and their comparative regulatory responses. In *Stanford journal of Blockchain law & policy*. Retrieved from https://stanford-jblp.pubpub.org/pub/ico-comparative-reg.

Kaal, W., & Dell'Erba, M. (2017). Initial coin offerings: Emerging practices, risk factors, and red flags. In *U of St. Thomas (Minnesota) legal studies research paper no. 17-18*.

Kaminsky, D. (2013). I tried hacking bitcoin and I failed. In *Business Insider*. Retrieved from https://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4?IR=T.

Kean, B. (2018). Don't believe the hype. In *Five largest ICO "exit scams": Expert take*. Retrieved from https://cointelegraph.com/news/dont-believe-the-hype-the-five-largest-ico-exit-scams-expert-take.

Kharif, O. (2017). *Hedge Funds Flip ICOs*. Bloomberg: Leaving Other Investors Holding the Bag. Retrieved from https://www.bloomberg.com/news/articles/2017-10-03/hedge-funds-flip-icos-leaving-other-investors-holding-the-bag.

Kharpal, A. (2019). Hackers steal over $40 million worth of bitcoin from one of the world's largest cryptocurrency exchanges. Retrieved from https://www.cnbc.com/2019/05/08/binance-bitcoin-hack-over-40-million-of-cryptocurrency-stolen.html.

Klein, T., Thu, H., & Walther, T. (2018). Bitcoin is not the new gold – A comparison of volatility, correlation, and portfolio performance. *International Review of Financial Analysis, 59*, 105–116.

Krombholz, K., Judmayer, A., Gusenbauer, M., & Weippl, E. (2016). The other side of the coin: User experiences with bitcoin security and privacy. In *FC 2016: Financial cryptography and data security* (pp. 555–580).

Kwon, R., Anandalingam, G., & Ungar, L. (2005). Iterative combinatorial auctions with bidder-determined combinations. *Management Science, 51*, 407–418.

Lagace, M. (2007). Industry self-regulation: What's working a and what's not?. In *Harvard business school*. Retrieved from https://hbswk.hbs.edu/item/industry-self-regulation-whats-working-and-whats-not.

Lee, J., Li, T., & Shin, D. (2021). The wisdom of crowds in FinTech: Evidence from initial coin offerings. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195877.

Leising, M. (2018). U.S. regulators subpoena crypto exchange bitfinex, tether. In *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc.

Lipusch, N. (2018). Initial coin offerings - A paradigm shift in funding disruptive innovation. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148181.

Lyandres, E., Palazzo, B., & Rabetti, D. (2020). ICO success and post-ICO performance. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377448.

Ma, W. (2021). China's cryptocurrency regulations will propel similar regulations globally. In *International financial law review*. Retrieved from https://www.iflr.com/article/b1sw6s2wlhg3fd/chinas-cryptocurrency-regulations-will-propel-similar-regulations-globally.

Mao, K., Capra, L., Harman, M., & Jia, Y. (2017). A survey of the use of crowdsourcing in software engineering. *Journal of Systems and Software, 126*, 57–84.

Matsumura, M. (2017). *ICO governance: A protocol-based self-regulation of token sales in decentralized capital markets. ICO Governance Foundation White paper*.

Maume, P., & Fromberger, M. (2019). Regulation of initial coin offerings: Reconciling US and EU securities Laws. *Chicago Journal of International Law, 19*, 548–585.

McCauley, R., McGuire, P., & von Peter, G. (2012). After the global financial crisis: From international to multinational banking? *Journal of Economics and Business, 64*, 7–23.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In *, 6. Proceedings of the internet measurement conference* (pp. 127–140).

Merkle, R. C. (1979). *Secrecy, authentication, and public-key systems [unpublished doctoral dissertation]*. Stanford University.

Momtaz, P. (2020a). Initial coin offerings. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3166709.

Momtaz, P. (2020b). Entrepreneurial finance and moral Hazard: Evidence from token offerings. *Journal of Business Venturing, 106001*.

Momtaz, P. (2021). The pricing and performance of cryptocurrency. *The European Journal of Finance, 27*, 367–380.

Monaghan, A. (2018). Bitcoin biggest bubble in history, says economist who predicted 2008 crash. In *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/feb/02/bitcoin-biggest-bubble-in-history-says-economist-who-predicted-2008-crash.

Monjas-Barroso, M. (2012). Alternativas de Financiación a través de Internet en Periodos de Racionamiento de Crédito: ¿Desintermidiación o Reintermidiación? *Boletin de Estudios Economicos, 67*, 247–266.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. New Jersey, US: Princeton University Press.

Narayanan, A., & Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM, 60*, 36–45.

Ngo, D. (2018). Exit scam: Vietnamese cryptocurrency company goes dark after allegedly duping investors of US$660M in ICOs. Retrieved from https://coinjournal.net/exit-scam-vietnamese-cryptocurrency-company-goes-dark-after-allegedly-duping-investors-of-us660m/.

Nikolic, I., Kolluri, A., Sergey, I., Saxena, P., & Hobor, A. (2018). *Finding the greedy, prodigal, and suicidal contracts at scale*. Retrieved from doi: arXiv:1802.06038v1.

Omarova, S. (2011). Wall street as community of fate: Toward financial industry self-regulation. *University of Pennsylvania Law Review, 159*, 411–492.

Osborne, C. (2018). Hacker returns 20,000 ETH stolen during CoinDash ICO. Retrieved from https://www.zdnet.com/article/hacker-returns-20000-eth-stolen-during-coindash-ico/.

Pasanisi, J. (2018). Head to head: Should there be global harmonisation of ICO Regluation. In *International financial law review*. Retrieved from https://www.iflr.com/article/b1lp1vpl2dw7wc/head-to-head-should-there-be-global-harmonisation-of-ico-regulation.

Peters, G. W., & Panayi, E. (2015). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2692487.

Platt, E. (2018). *US junk bond premiums slide to 2014 low*. Financial Times. Retrieved from https://www.ft.com/content/a9b3d584-d613-3a68-9900-faa2e0855c7c.

PWC. (2019). 5th ICO / STO report: A strategic perspective. Retrieved from https://www.pwc.ch/en/publications/2019/ch-PwC-Strategy%26-ICO-Report-Summer-2019.pdf.

Quinlan, B., & Cheng, H. (2018). Fool's gold?. In *Unearthing the world of cryptocurrencies*. Retrieved from https://www.quinlanandassociates.com/wp-content/uploads/2018/01/Quinlan-Associates-Fools-Gold-Sample-Pages.pdf.

Rajan, R. (2008). *Bankers' pay is deeply flawed*. Financial Times. Retrieved from https://www.ft.com/content/18895dea-be06-11dc-8bc9-0000779fd2ac.

Raymond, E. (1999). *The cathedral and the bazaar*. Sebastopol, California: O'Reilly Media.

Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in blockchain technologies & social contract theories. *Ledger, 1*, 134–151.

Rhue, L. (2018). Trust is all you need: An empirical exploration of initial coin offerings (ICOs) and ICO reputation scores. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3179723.

Robinson, R. (2018). The new digital wild west: Regulating the explosion of initial coin offerings. *Tennessee Law Review, 85*, 897–960.

Rodrigues, U. (2018). Semi-public offerings?. In *Pushing the boundaries of securities law*. *University of Georgia School of Law Legal Studies Research Paper No. 2018–30*.

Rubinstein, A., & Spiegler, R. (2008). Money pumps in the market. *Journal of the European Economic Association, 6*, 237–253.

Santos, M. (2018). How security alerts are keeping your code safer [Blog post]. Retrieved from https://blog.github.com/2018-03-21-security-alerting-a-first-look-at-community-responses/.

Schneire, B. (2011). *Secrets and lies: Digital security in a networked world*. Indianapolis, US: John Wiley & Sons.

Schwarcz, S. (2011). Financial industry self-regulation: Aspiration and reality. *University of Pennsylvania Law Review, 159*, 293–302.

SEC. (2013). Investor Alert: Ponzi schemes Using virtual Currencies. Retrieved from https://www.sec.gov/files/ia_virtualcurrencies.pdf.

SEC. (2017). *SEC Complaint: REcoin Group Foundation, LLC, DRC World Inc. a/k/a Diamond Reserve Club, and Maksim Zaslavskiy. U.S. Securities and Exchange Commission*.

Sedgwick, K. (2018). Verge is forced to fork after suffering a 51% attack. Retrieved from https://news.bitcoin.com/verge-is-forced-to-fork-after-suffering-a-51-attack/.

Segoviano, M., Jones, B., Lindner, P., & Blankenheim, J. (2013). *Securitization: Lessons learned and the road ahead. IMF working paper - WP/13/255*.

Sherman, A., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of blockchain technologies. *IEEE Security and Privacy, 17*, 72–77.

Shleifer, A., & Vishny, R. (2010). Unstable banking. *Journal of Financial Economics, 97*, 306–318.

Siegel, D. (2016). Understanding the DAO attack [Blog post]. Retrieved from https://www.coindesk.com/understanding-dao-hack-journalists.

Sijbrandij, S. (2018). How open source became the default business model for software. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/16/how-open-source-became-the-default-business-model-for-software/#7c4d0c184e72.

Spence, A. (1973). Job market signaling. *Quarterly Journal of Economics, 87*, 355–374.

Suberg, W. (2017). Dash employs white hat hackers to hack its own blockchain. Retrieved from https://cointelegraph.com/news/dash-employs-white-hat-hackers-to-hack-its-own-blockchain.

Sundararajan, S. (2017). New self-regulatory body aims to develop ICO standards. Retrieved from https://www.coindesk.com/new-self-regulatory-body-aims-to-develop-ico-standards.

Teng, F., Griffin, P., & Koh, A. (2019). Picking flowers in an ICO garden. *Research Collection School of Computing and Information Systems*, 3–19. Retrieved from https://ink.library.smu.edu.sg/sis_research/5900.

The Merkle. (2017). White hat hackers, smart contract & blockchain experts team up with smartone in anticipation of LEGAL token launch. Retrieved from https://themerkle.com/white-hat-hackers-smart-contract-blockchain-experts-team-up-with-smartone-in-anticipation-of-legal-token-launch/.

Thomas, L. (2021). 130 countries back global minimum corporate tax of 15%. Retrieved from https://www.reuters.com/business/countries-backs-global-minimum-corporate-tax-least-15-2021-07-01/.

Toffel, M. (2006). Resolving information asymmetries in markets: The role of certified management programs. *Harvard Business School working paper no. 07-023*.

Uranaka, T., & Wilson, T. (2018). Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft. In *Taiga Reuters*. Retrieved from https://www.reuters.com/article/us-japan-cryptocurrency/japan-raps-coincheck-orders-broader-checks-after-530-million-cryptocurrency-theft-idUSKBN1FI06S.

Valenzuela, J. (2017). How dash solves the "ICO Problem". Retrieved from https://www.dashforcenews.com/dash-solves-ico-problem/.

Valkenburgh, P. V. (2017). What is "open source" and why is it important for cryptocurrency and open blockchain projects?. Retrieved from https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects.

Vasilescu, B., Filkov, V., & Serebrenik, A. (2013). Stack overflow and GitHub: Associations between software development and crowdsourced knowledge. In *2013 IEEE international conference on social computing (SocialCom)* (pp. 188–195).

Vlastelica, R. (2018). This 1 chart shows the U.S. stock market is the most expensive in the world. Retrieved from https://www.marketwatch.com/story/this-1-chart-shows-the-us-stock-market-is-the-most-expensive-in-the-world-2017-12-28.

Vogelsteller, F., & Buterin, V. (2017). ERC-20 token standard. Retrieved from https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-tokenstandard.

Williams-Grut, O. (2017). WALKTHROUGH: How traders 'pump and dump' cryptocurrencies. Retrieved from http://uk.businessinsider.com/how-traders-pump-and-dump-cryptocurrencies-2017-11/#telegram-is-the-app-of-choice-for-cryptocurrency-traders-here-is-a-message-sent-to-advertise-the-pumpking-community-telegram-channel-1.

Xie, Y., & Yap, C.-W. (2017). Meet the Earth's largest money-market fund. In *Wall street journal*. Retrieved from https://www.wsj.com/articles/how-an-alibaba-spinoff-created-the-worlds-largest-money-market-fund-1505295000.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*, 7–31.

Yi, S., Xu, Z., & Wang, G.-J. (2018). Volatility connectedness in the cryptocurrency market: Is bitcoin a dominant cryptocurrency? *International Review of Financial Analysis, 60*, 98–114.

Zetzsche, D., Buckley, R. P., Arner, D. W., & Föhr, L. (2019). The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators. *Harvard International Law Journal, 60*, 267–315.

Zhang, S., Aerts, W., Lu, L., & Pan, H. (2019). Readability of token whitepaper and ICO first-day return. *Economics Letters, 180*, 58–61.

Zhao, W. (2017). CoinDash ICO hacker nets additional ether as theft tops $10 Million. Retrieved from https://www.coindesk.com/coindash-ico-hacker-nets-additional-ether-theft-tops-10-million/.

Zhou, Y., Kumar, D., Bakshi, S., Mason, J., Miller, A., & Bailey, M. (2018). Erays: Reverse engineering Ethereum's opaque smart contracts. In *Proceedings of the 27th USENIX security symposium* (pp. 1371–1385).

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities.*

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

www.ecgi.global

european corporate governance institute

ECGI Working Paper Series in Law