ecgi

# Regulatory and Market Challenges of Initial Coin Offerings

Law Working Paper N° 461 /2019
July 2019

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

ECGI Working Paper Series in Law

# Regulatory and Market Challenges of Initial Coin Offerings

Working Paper N° 461/2019

July 2019

Pablo de Andrés
David Arroyo
Ricardo Correia
Alvaro Rezola

The authors thank the Regional Government of Madrid and European Social Fund (Grant number ref.: EARLYFIN, S2015/HUM-3353) for their financial support for this research.

## Abstract

This article analyzes the main problems and the solutions adopted in the market for Initial Coin Offerings (ICO), an alternative financing solution that has experienced spectacular growth and notoriety in recent years. This market relies on the use of Blockchain protocols and is, therefore, characterized as disintermediated, decentralized and unregulated. The problems we identify in this article, their severity, and the solutions currently being adopted to address them, lead us to conclude that it is unlikely that either of these characteristics will survive in the near future. Our results also indicate that the concerns expressed by regulators and other market agents regarding ICO markets are well founded. We find it particularly disturbing that such a new, revolutionary market already displays many of the problems of traditional financial markets, and that these problems were exactly the ones that occurred at the genesis of the last financial crisis.

Keywords: Blockchain, initial coin offerings, regulation, cryptoassets and cryptoeconomy, trust modeling: fairness and accountability, decentralization and disintermediation risks, entrepreneurial finance, investment crowdfunding

JEL Classifications: K22, G32, O16, L26

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

# Regulatory and Market Challenges of Initial Coin Offerings

Pablo de Andrés
Universidad Autónoma de Madrid and ECGI
Finance and Marketing Department
C/ Francisco Tomás y Valiente, 5
28049 Cantoblanco – Madrid (Spain)

David Arroyo
Instituto de Tecnologías Físicas y de la Información
Consejo Superior de Investigaciones Científicas,
Serrano 144,
28006 Madrid, Spain

Ricardo Correia
Universidad Autónoma de Madrid
Finance and Marketing Department
C/ Francisco Tomás y Valiente, 5
28049 Cantoblanco – Madrid (Spain)

Alvaro Rezola
Universidad Autónoma de Madrid
Finance and Marketing Department
C/ Francisco Tomás y Valiente, 5
28049 Cantoblanco – Madrid (Spain)

**Abstract:**

This article analyzes the main problems and the solutions adopted in the market for Initial Coin Offerings (ICO), an alternative financing solution that has experienced spectacular growth and notoriety in recent years. This market relies on the use of Blockchain protocols and is, therefore, characterized as disintermediated, decentralized and unregulated. The problems we identify in this article, their severity, and the solutions currently being adopted to address them, lead us to conclude that it is unlikely that either of these characteristics will survive in the near future. Our results also indicate that the concerns expressed by regulators and other market agents regarding ICO markets are well founded. We find it particularly disturbing that such a new, revolutionary market already displays many of the problems of traditional financial markets, and that these problems were exactly the ones that occurred at the genesis of the last financial crisis.

**Keywords:** Blockchain, Initial Coin Offerings, Regulation.

**Acknowledgements:** The authors thank the Regional Government of Madrid and European Social Fund (Grant number ref.: EARLYFIN, S2015/HUM-3353) for their financial support for this research.

## 1. Introduction

The global financial crisis of 2007–2009 had important repercussions for the economy. 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 et al., 2012; McCauley, 2012). Directly and indirectly, these events have fostered the development of alternative financial markets (Monjas-Barroso, 2012; Glasius and Pleyers, 2013) based on the adoption of new technologies (e.g., Blockchain, etc.), and these markets are characterized by disintermediation and deregulation.

The emergence of alternative financing in this context can be explained by the fact that, although interest rates decreased following the crisis, lenders were rationing credit (Brunnermeier, 2009; Shleifer and Vishny, 2010; Campello et al., 2010)[1]. This was the primary driver of the development of alternative financing channels. However, other factors have also fostered the growth of crowdsourced financing solutions and Blockchain technology itself. Following the public outcry caused by the bailout of financial institutions, people developed a general distrust of existing financial institutions and have become very receptive to alternatives (see Glasius and Pleyers, 2013, for a thorough analysis of the motivations and aims of the Occupy movements). These alternative financing solutions allow investors to meet lenders, bypassing traditional financial intermediaries. Lenders can obtain financing at reasonable prices and investors can obtain reasonable yields in a context of very low interest rates. Furthermore, since these “new” markets are digital, they are also global by nature (with no language, geographical, cultural, or legal barriers), allowing borrowers to

access a broader base of potential investors, and at the same time, allowing investors to access a broader base of investment opportunities.

A financing alternative that has been gaining considerable importance[2] is the Initial Coin Offerings (ICO) market, a means of financing early-stage digital innovations through the issuance of crypto-assets[3]. Being a digital, decentralized, disintermediated, global, and unregulated market, ICOs present novel challenges, but also some innovative solutions to these problems. This article analyzes the main problems currently afflicting the ICO market and the solutions that have been put forward to address these. It highlights the similarities between some of the problems currently facing ICO markets and those that occurred at the beginning of the 2007–2009 financial crisis[4]. It also highlights the specific and "new" problems of the ICO market and their associated solutions. Given the ongoing process of self-regulation by ICO market agents and the still uncertain regulatory environment that will govern ICO markets in the near future, the results of our article should be of interest to ICO market agents and financial regulators alike.

In terms of regulation, on one hand, the financial regulations passed following the crisis are contrary to the spirit of these new deregulated markets by increasing the protection of small investors (e.g., Markets in Financial Instruments Directive II in the EU). On the other hand, President Obama signed the 2012 JOBS Act, which modifies the Securities Act of 1933 by lowering issuance requirements and costs and opening the door to these new markets. These apparently contradictory approaches are possibly explained because these alternative emerging markets generate welfare gains: they provide potential solutions for credit rationing, unemployment, lack of yield in investment opportunities, democratize the access to profitable investment opportunities and are, therefore, more or less well-received by governments. It is however possible that underlying the current *laissez faire* approach of many governments, the

positive externalities of the technological development are being taken for granted while the associated technological risks are being disregarded (Harmsen et al., 2018; Collomb et al., 2018).

This article belongs to the stream of literature that analyzes the phenomena of ICOs. To date, academic efforts have covered the determinants of the success of an ICO (e.g., Adhami et al., 2018; Flood and Robb, 2017), sociological aspects (e.g., Vardi, 2018; Atzori and Ulieru, 2017), financing early-stage innovations (e.g., Kaal and Dell'Erba, 2017; Lipusch, 2018), risks involved in investing in ICOs (Chohan, 2017) and the ethics of Bitcoin (e.g. Pasztor, 2018) and computing science (e.g. Vardi, 2019).

In terms of regulation, most of the research overwhelmingly focuses on analyzing the current regulatory approaches being followed on a national level to deal with the emergence of ICOs (Barsan, 2017, Hornuf and Schwienbacher, 2017, Gurrea-Martínez and León, 2018, Kaal, 2018, Enria, 2018). The interest on ICO regulation coincides and possibly even triggers, a renewed interest in two other regulatory topics namely, global regulatory solutions (Bennett and Raab, 2018, Hacker and Thomale, 2019 and Marian, 2019) and self-regulation in financial markets (Matsumura, 2017, Batiz-Benet et al., 2017, Keidar and Blemus, 2018).

Even though ICOs are regulated in several countries, there is a clear intention by Blockchain entrepreneurs to circumvent regulation through various means (Rodrigues, 2018) making the bulk of the ICO market to date still an unregulated market. This paper shows the importance and severity of the problems currently afflicting the ICO market that are in a great extent due to this regulatory vacuum (e.g. scams, deceit, manipulation, copycat projects, complexity of securities, etc.). It performs an analysis of the current problems that afflict the ICO markets, considering a regulatory perspective and assessing the following issues:

- If the concerns raised by ICO market agents, policymakers and researchers concerning the unregulated nature of the ICO markets are justified;
- How the ICO market addresses its problems and how effective these actions are in deterring further regulation;
- The extent to which these problems are likely to shape the future of ICO markets.

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 conclusions.

## 2. The Blockchain environment and the ICO market

The current regulatory context of the ICO markets was shaped by the 2007-2009 financial crisis. The 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, amongst others) aimed at the protection of small investors[5]. However, it is safe to say that ICO markets are these days mostly unscathed by this regulatory fervor and are still mostly unregulated. 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. In this section we critically analyze the phenomena ICO markets from the emergence of Blockchain to the actual ICO process.

### 2.1 The emergence of Blockchain

Although the aftermath of the financial crisis of 2007–2009 witnessed the emergence of commercial applications of distributed ledger technology (DLT), namely Blockchain, the birth of DLTs can be traced back several decades[6]. A distributed ledger is a cryptographic information protocol developed in the late 1950s and early 1960s[7] 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. A few initial projects did make commercial use of distributed ledger technology[8], but Bitcoin, using its distributed ledger Blockchain, represents the first successful economic application of the technology, allowing the recording of data in an open, distributed, certifiable, and immutable way.

With respect to existing protocols, distributed ledgers go a step further in information security by running a parallel digital system without trusted third parties, administered by methods of distributed consensus. In order to build the necessary network that will support the information system, an incentive must exist to absorb the associated IT costs. The Bitcoin Blockchain was the first practical solution to this problem (Narayanan and 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 information protocol and the community[9]. Once a crypto-currency (e.g., Bitcoin, Ether) is generally accepted, other entities capable of building services for that community are also incentivized to work in return for these crypto-currencies.

Early-stage innovative firms that look for financing in these markets may not be willing to dilute their ownership to outsiders in the form of mining and choose to issue a limited number of crypto-assets with additional rights, similar to a hybrid security. First, a token is a crypto-asset 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.

### 2.2 Initial coin offerings

An ICO or Initial Coin Offering is the term adopted for the first issuance of crypto-assets from a company. A crypto-asset is a contract that provides the owner with certain rights formalized in code, referred to as smart contracts, and run on DLTs. 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, having raised $99 million USD in 2016 from 46 ICOs, more than $6.5 billion USD in 2017 from 456 ICOs, and more than $21.5 billion USD in 2018 from a total of 1082 offerings[10].

In its infancy, the model has seen three representative stages of ICOs based on the relative weight of the characteristic attached to the smart contract. The first ICO stage is the altcoin stage[11], in which the Bitcoin success triggered the issuance of mostly currency-like crypto-currencies with partial modifications of the Bitcoin Blockchain. This is the case with LTC (Litecoin) and BCH (Bitcoin Cash), with a focus on the speed of transaction, or DASH and XMR (Monero), with a focus on privacy. These crypto-assets are merely cryptocurrencies, as their sole logic and use is as a means of payment. Looking at the evolution of the market capitalization of altcoins and other crypto-assets, it is safe to say that the hype surrounding

this first stage is past us. In 2013, Bitcoin accounted for 95% of the total market capitalization. Today, the four most representative crypto-currencies (Bitcoin, Bitcoin Cash, Litecoin, and Ripple) account for less than 50% of the market. The second wave 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 and Buterin, 2017), capable of issuing new tokens. The emergence of *easy to develop smart contracts*[12] 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. The evolution of the weights of infrastructure ICOs highlights the emergence of this third stage. The weight of infrastructure ICOs reduced from 46% in 2016 to 34% in 2017. 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).

### 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 or a token crowd sale starts 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 et al., 2018). The first stage is to

announce the plans to perform a token issue in the near future, detailing the project, its nature, and objectives. A white paper is usually published at this stage, detailing the project, its merits, and future developments. 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

bpromotion efforts to take place on social media platforms (Rhue, 2018). The most commonly used are Telegram, Twitter, Facebook, Reddit, Slack, and Bitcoin Talk[13]. The issuer announces the incoming ICO or creates a thread in these platforms and triggers a discussion on the value and attractiveness of the ICO. The pricing 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.

It should be noted that the issuer defines the scope and quality of all the information provided. This information is not audited by a third party, is not required to follow any standards, and most of it is unverifiable.

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[15] and social networks,[16] 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[17]. 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.

## 3. Main problems of the Initial Coin Offerings market

The ICO market performs the basic functions of traditional financial markets, which is to be the logical place where 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 in traditional financial markets. However, the idiosyncrasies of the ICO market differentiate it from traditional financial markets, namely, it is a fast-growing emerging market for digital innovators and currently, still a mostly unregulated market.

From the point of view of economics, the problems we discuss in this article translate into an inefficient allocation of resources. From the point of view of unregulated markets, 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[18] (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[19].

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 et al., 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 ICO market 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 take action and ban token issues and trading to address the negative externalities of the TOC failure (e.g., see the cases of China and South Korea) or at least substantially curtail the token market.

**3.2 Scams, deceit, manipulation, and copycat projects:**

Nowadays, 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. The first is that there is pseudoanonimity in the most popular Blockchains (i.e., Bitcoin and Ethereum), meaning that all information is public but cannot be traced back to any particular agent. The second aspect

relates to 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 and 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, although 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 (e.g., see Bartoletti et al. 2017). However, as in the case of Bitcoin, the weight of these criminal transactions is still relatively insignificant. Although Bartoletti et al. (2017) classify approximately 10% of the smart contracts recorded in 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 Ngo, 2018; Biggs, 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 operations that

aim at delivering real products or services; however, once the funds are raised, the entrepreneurs disappear with the funds and no real business venture is actually pursued.

The use of social media to promote ICOs and information asymmetries between the promoters and potential investors in ICO pre-sales[20] creates the perfect ground for flipping and for pump and dump schemes. While promoters advertise the pre-sales to qualified investors as a quality signal, the actual terms and prices of the pre-sale are made public in very few cases. The pre-sale usually takes place with heavy discounts on the issue price and few restrictions on the subsequent trading of the tokens[21]. 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 ethically questionable[22] 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), profiting on the difference. The unregulated nature of the Blockchain market allows these market manipulation practices to thrive. In the Blockchain community it is easy to find agents that offer "pump" services on social networks (Gordon, 2017) and even pump "communities" (Williams-Grut, 2017) that coordinate to implement these schemes.

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 the main rule. Griffin and Shams (2018) analyze trading activities between Tether[23] 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 et al. (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[24]. 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).

### 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 and 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 and Zhang, 2017)[25]. Although Blockchain technology insures 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[26].

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 et al., 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, and NiceHash in Slovenia. 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 as also the misuse of crypto-assets, and following an initial ban on anonymous trading of crypto-assets, Korea is now considering banning all trading (see Reuters, 2018b).

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. CoinDash 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"[27] 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[28]. 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 $32M from multisig Parity wallets before they were stopped. In this case, the hackers were prevented from stealing the remaining $85M stored in the wallets by a group of white hackers called the White Hat Group[29]. Once alerted to the attack, this group stole the remaining $85M 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 victims of hacking attacks[30].

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[31], 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 450 ICOs, Zetzsche et al. (2018) found that:

- Almost half of the ICOs do not provide personal or background information on the project promotor;
- In one third of the ICOs, the name on the white paper differs from that of the ICO issuer;
- More than 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 less than 1.5% 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 properly determine their fair value and may generate 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)[32]. It is well recognized in the economic literature that in many cases, this sort of bundling represents a strategy to lure consumers or investors into buying useless assets, thereby creating a camouflaged Ponzi Scheme (Rubinstein and Spiegler, 2008; Basu, 2010). 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 et al., 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 the token 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.

Finally, the security design of the tokens is a crucial aspect that regulators need to address since their complexity is, in most cases, not the answer to a market failure (e.g. optionality features in debt contracts to mitigate agency conflicts) but a means to avoid regulation (Rodrigues, 2018).

### 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 interaction between the

investments and the financing functions prior to the crisis was remarkably strong. 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, 2012; Segoviano et al., 2013). Currently, we observe a state of overheating and a general recognition that cryptocurrencies markets (The Guardian, 2018; Quinlan and Cheng, 2018) and ICO markets (Zetzsche et al., 2018) 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., 2018) 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.

### 3.7 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 Rajan, 2008; Bebchuk et al., 2010). Currently, we observe similar problems with the business ventures that try to obtain financing from ICOs. Three main problems are identifiable in this case. First, 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). Second, 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). Finally, 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, Finews, 2017).

### 3.8 Importance of the ICO market problems

In sum, 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 Japan). 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 and Yap, 2017 and the case of the Chinese money market fund Yu'e Bao). 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[33] 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 Matsumura, 2017; Crypto Valley, 2018), 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[34]. 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, know your client, 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[35].

As with the Internet, Blockchain is evolving towards a set of 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 et al., 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[36].

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,[37] 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 et al. (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[38]. 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 insure security for the marketplace of the token LEGAL (see 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.

White hacking represents a particular solution for digital markets to the problems of hackers' thefts and criminal actions. While the importance of white hackers is unquestionable in terms of prevention through the testing, auditing, and development process of Blockchains and smart contracts, their use to address thefts 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 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[39]. By creating a collaborative model in terms of code development, the open source model is able to develop better and more resilient software[40]. 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[41]. 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 et al., 2017), with platforms such as Stack Overflow especially relevant to the life cycle of open source development (Vasilescu et al., 2013). However, taking into account 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 GitHub Blog, 2018).

Raymond (1999) discusses the advantages of open source development. An important aspect is the involvement of a large number of 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 a large number of 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 as a means 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 development of the Blockchain, smart contracts, and, in the case of digital services, in the very development of the business enterprise has a strong effect on the aspects of the ICO markets. 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 since the analysis of the terms of the smart contract would reveal the deceit. The use of open source therefore reduces the issue of scams and deceits[42]. On the other hand, this level of transparency also comes at a cost as, in this case, it 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[43]. Second, access to the code developed for the services the firm intends to offer addresses several problems such as scams and perverse compensation schemes. In terms of scams, the possibility to observe and assess the level of business development makes it easier to anticipate an exit scam. The negative

effects of perverse compensation schemes (e.g. engagement in high risk ventures) can be mitigated by linking the access to the funds raised through the ICO to the accomplishment of specific and measurable milestones. Access to an open source repository, where all the developments are recorded, allows a set of rules to be set up in a smart contract that conditions the access to further funding to the actual achievement of a set of measurable objectives. 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, pp. 256–260). 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 Bitcoin protocol in 2017). However, contentious hard forks represent one of the most critical controversies in the Blockchain community. The lack of consensus in the protocol changes underlying a contentious hard fork 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. Moreover, in the past, these disputes led to 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. Further differences are that soft forks and planned hard forks are usually born out of developers' consensus to apply a protocol update and do not

usually create a significant disturbance to the Blockchain (although planned hard forks make all nodes upgrade the software). On the other hand, contentious hard forks may raise several issues such as forcing users and exchanges to run splitter contracts individually and, in some cases, result in the duplication of crypto-currencies.

Forks can also be used to address some of the problems we have previously discussed. Consider the case of a hacker theft of crypto-currency. 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. The case of the DAO is an example of the use of a hard fork to re-write history. This was the solution implemented to solve the problem of the hacker theft of one third of the funds raised via the DAO ICO. Another famous case of such use of a hard fork is that of the altcoin Verge in which a hard fork was used 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, amongst other things, being able to rewrite Verge's history[44].

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 and Wright, 2018).

A non-technical hard fork means that, in a chain of blocks, history 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[45]. The ethical and governance implications of this are tremendous and this is why 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 used standard (ERC-20) 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[46]. New token standards such as the ERC-777[47] 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 is done in OpenZeppelin[48] and as is common in traditional financial contracts such as executive stock options.

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[49]. 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 et al., 2018).

## 5. Conclusions

Our analysis of the problems that currently affect ICO markets shows that the concerns raised by policymakers and researchers are well justified. Currently, serious entrepreneurs and Blockchain developers coexist with and share the market with agents that aim at, manipulate, committing fraud, deceit investors or simply steal through hacking attacks. Furthermore, although the ICO market is hailed as a "new" and revolutionary market, it 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 what concerns the efforts of ICO market agents to mitigate its problems we observe two complementary approaches. On one hand, there is a technological approach through the development of technical solutions in the design of smart contracts, in improving transparency and enhancing the protection of the IT systems overall. On the other hand, there is an effort to develop self-regulation and standards that addresses most of the problems of the lack of transparency and of proper accountability in the whole ICO process. Unfortunately, the recent news of ongoing hacking attacks (see the recent case of Binance in Barret, 2019), Ponzi-schemes (see Argyle Coin LLC Diamond-Backed Crypto in Smith, 2019) and exit scams (see startups RepuX and JoyToken in Boddy, 2019) amongst other criminal enterprises

in the ICO markets, seriously questions the effectiveness of the efforts adopted by the ICO market agents. Given this scenario, it is very unlikely that regulators do not feel pressured to take further actions to put an end to these occurrences.

The ICO market is characterized as a disintermediated, decentralized, global, and unregulated market; however, given the problems and solutions we have identified, it is unlikely that it will remain so in the near future. Although Blockchain technically eliminates the need for independent third parties, it is expected and desired that more independent third parties are involved to address the problem of information asymmetries between issuers and retail investors. Although Blockchain is still envisioned as the cornerstone of disintermediation and transparency, the complexity of the technology is a major obstacle to fulfill both properties simultaneously. All the transactions are publicly available, and anyone can access the data, however, the size of the Blockchain and the underpinnings of the data model and protocols are not easy to understand. The lack of standard software libraries eventually leads to querying platforms such as Etherscan, which recentralizes Blockchain. This leads us to the important question of the implementation of standards. Standards have the potential to mitigate many of the problems we have addressed, and valid initiatives are already being developed (e.g., ISO technical committee TC 307); however, the adoption of these common and necessary standards, although greatly improving transparency, will naturally be against the principle of disintermediation.

In terms of regulation and the global nature of the ICO market, the results of our analysis have several implications for policymakers and regulators. We expect regulation to intervene at the core of the ICO concept, the nature of the crypto-assets themselves. It is interesting to observe that the current complexity of tokens resulted in many cases from a desire to evade financial market regulation, however, the problems that this increased complexity created ended up

attracting further the attention of the regulators. The much-needed regulatory solutions for the problems currently faced in the ICO markets are one of the great current challenges for financial regulators. However, the decentralized, highly technical, dynamic, and global nature of this market poses serious challenges to this task, which will most likely need to include self-regulatory entities that are as dynamic as the market itself and able to act globally. Notwithstanding these challenges, we feel the time for regulators to act is now. Firstly, there is enough evidence that the ICO market agents have been unable to address their problems. Secondly, the dramatic reduction in the amounts issued through ICOs in 2019[50] eliminate the fear of stifling innovation. Finally, given this dramatic reduction in ICOs the very attitude of the market agents towards regulation may have changed significantly and its unexpected that some may even welcome a stricter regulatory approach.

Given all the above, we predict that in the near future, although the Blockchain protocol may still be characterized as disintermediated, decentralized, and unregulated, the same will not be true for the ICO markets.

## 6. 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). https://doi.org/10.1109/SecDev.2017.17

Adhami, S., Giudici, G., & Martinazzi, S. 2018. *Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings*. Journal of Business and Economics 100, 64-75.

Antonopoulos, A. M. 2017. *Mastering Bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc."

Atzori, M., & Ulieru, M. 2017. *Architecting the eSociety on Blockchain: A Provocation to Human Nature*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2999715

Baker, N. 2018. *Widespread Fraud in ICOs and Penny Stocks Shocked SEC's Jay Clayton*. https://www.bloomberg.com, accessed 16th of April 2018. url: https://www.bloomberg.com/news/articles/2018-04-10/widespread-fraud-in-icos-and-penny-stocks-shocked-sec-s-clayton

Barrett, B. 2019. Hack Brief: Hackers Stole $40 Million from Binance Cryptocurrency Exchange. https://www.wired.com, accessed 24th of May 2019. url: https://www.wired.com/story/hack-binance-cryptocurrency-exchange/

Barsan, I. 2017. *Legal Challenges of Initial Coin Offerings*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064397

Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. 2017. *Dissecting Ponzi schemes on Ethereum: identification, analysis and impact*. Università di Cagliari working paper.

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*. Protocol Labs White Paper.

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.

Benedett, H., & Kostovetsky, L. 2018. *Digital tulips? Returns to investors in Initial Coin Offerings*. Available at SSRN: https://ssrn.com/abstract=3182169

Bennett, C. & C. Raab 2018. Revisiting the governance of privacy: Contemporary policy instruments in global perspective. Regulation & Governance, 1-18.

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*. https://techcrunch.com, accessed 16th of April 2018. url: 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: Penguin Press.

Boddy, M. 2019. Blockchain Sister Startups Allegedly Pull $8 Million Exit Scam. https://cointelegraph.com, accessed 24th of May 2019. url: https://cointelegraph.com/news/blockchain-sister-startups-allegedly-pull-8-million-exit-scam

Brito, J. 2013. *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*. 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.

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.

Chatterji, A., & Toffel, M. 2010. *How Firms Respond to Being Rated*. Strategic Management Journal 31, 917–945.

Chohan, U. 2017. Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. Discussion Paper Series: Notes on the 21st Century.

Choudhury, R. 2017. *Many ICOs are fraudulent, say men behind two top bitcoin rivals*. https://www.cnbc.com, accessed 16th of April 2018. url: 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*. https://cryptobriefing.com, accessed 16th of May 2018. url: https://cryptobriefing.com/banks-fear-crypto-turns-fomo/

Collomb, A., Filippi, P. De, & Sok, K. 2018. *From IPOs to ICOs: The Impact of Blockchain*. Available at SSRN: https://ssrn.com/abstract=3185347

Cranor, L. F., & Garfinkel, S. 2005. *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc.

Crypto Valley. 2018. *Mission and Policy Framework*. https://cryptovalley.swiss/, accessed 3rd of July 2018. url: https://cryptovalley.swiss/codeofconduct/

De Filippi, P. D. F., & Wright, A. 2018. *Blockchain and the Law: The Rule of Code*. Harvard University Press.

De, N. 2018. *Hacker Returns $26 Million in Ether Months After ICO Theft*. https://www.coindesk.com, accessed 24th of June 2018. url: 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.

Enria, A. 2018. Designing a Regulatory and Supervisory Roadmap for FinTech. Speech by Andrea Enria - Chairperson of the European Banking Authority (EBA). Copenhagen Business School.

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

EY. 2017. *EY research: initial coin offerings (ICOs)*. EYGM Limited.

Finews. 2017. *Record ICO's Swiss Ties Raise Eyebrows*. finews.com, Thursday, 3 August 2017, Katharina Bart reports. https://www.finews.com/news/english-news/28253-tezos-ico-swiss-foundation-dls-kathleen-arthur-breitman

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*. In *Security and Privacy (SP), 2017 IEEE Symposium on* (pp. 121–136)

Flood, J., & Robb, L. 2017. *Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings*. Griffith University Law School Research Paper No. 17-23

Gandal, N., Hamrick, J., Moore, J., & Oberman, T. 2018. *Price Manipulation in the Bitcoin Ecosystem*. Journal of Monetary Economics (forthcoming).

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.

GitHub Blog. 2018. *How security alerts are keeping your code safer*. https://blog.github.com/, accessed 23rd of September 2018. url: https://blog.github.com/2018-03-21-security-alerting-a-first-look-at-community-responses/

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*, *2018*(4), 179-199.

Gordon, S. 2017. *Anatomy of an ICO Pump and Dump*. https://medium.com, accessed 17th of April 2018. url: 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. 2018. *Is Bitcoin Really Un-Tethered?* Working paper - Available at SSRN: https://ssrn.com/abstract= H.

Gurrea-Martínez, A. & N. León 2018. The Law and Finance of Initial Coin Offerings. Ibero-American Institute for Law and Finance, Working Paper Series 4/2018.

Hacker, P. & C. Thomale 2018. Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. Financial Law Review, 645-696.

Hardjono, T., Lipton, A., & Pentland, A. 2018. *Towards a Design Philosophy for Interoperable Blockchain Systems*. 1–27. Retrieved from http://arxiv.org/abs/1805.05934

Harmsen, S., Wall, M. A., Huang, R., & Kircher, M. F. 2018. *In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism*. Palgrave Communications, 4(14), 2055–1045. https://doi.org/10.1038/nprot.2017.031

Hartmann, F., Wang, X., & Lunesu, I. 2018. *Evaluation of Initial Cryptoasset Offerings: the State of the Practice*. 1st Int. Workshop on Blockchain Oriented Software Engineering, IWBOSE 2018, Campobasso, Italy.

Hermann, E., Trimborn, S., Ong, B., & Lee, T. 2016. *The Cross-Section of Crypto-Currencies as Financial Assets: An Overview*. SFB 649 Discussion Paper 2016-038.

Hornuf, L. & A. Schwienbacher 2017. Should securities regulation promote equity crowdfunding? Small Business Economics 49, 579–593.

Horten, M. 2016. *The closing of the net*. John Wiley & Sons.

Ibba S., Pinna A., Baralla G., & Marchesi M. 2018. *ICOs Overview: Should Investors Choose an ICO Developed with the Lean Startup Methodology?* In: Garbajosa J., Wang X., Aguiar A. (eds) Agile Processes in Software Engineering and Extreme Programming. XP 2018. Lecture Notes in Business Information Processing, vol 314. Springer, Cham.

Ismailidou, E. 2016. *Treasury yields plunge to all-time lows on 'insatiable' demand for safety*. https://www.marketwatch.com, accessed 17th of April 2018. url: https://www.marketwatch.com/story/treasury-yields-tumble-to-record-lows-as-brexit-fears-resurface-2016-07-05

Jarrow, R. 2012. *The Role of ABS, CDS and CDOs in the Credit Crisis and the Economy*. Rethinking the Financial Crisis, eds., Blinder, A. Lo, and R. Solow, Russell Sage Foundation.

Jia, K. & Zhang, F. 2017. *Between liberalization and prohibition*. In *Bitcoin and Beyond* (pp. 88–108). Routledge. https://doi.org/10.4324/9781315211909-5

Kaal, W. and Dell'Erba, M. 2017. *Initial Coin Offerings: Emerging Practices, Risk Factors, and Red Flags*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067615

Kaal, WA. 2018. *Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3117224

Kaminsky, D. 2013. *I Tried Hacking Bitcoin And I Failed*. https://www.businessinsider.com/, accessed 23rd of September 2018. url: https://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4?IR=T

Kean, B. 2018. *Don't Believe the Hype. Five Largest ICO "Exit Scams": Expert Take*. https://cointelegraph.com, accessed 16th of April 2018. url: https://cointelegraph.com/news/dont-believe-the-hype-the-five-largest-ico-exit-scams-expert-take

Keidar, R. and S. Blemus 2018. Cryptocurrencies and Market Abuse Risks: It's Time for Self-Regulation, Lexology (forthcoming).

Kharif, O. 2017. *Hedge Funds Flip ICOs, Leaving Other Investors Holding the Bag*. https://www.bloomberg.com, accessed 17th of April 2018. url: https://www.bloomberg.com/news/articles/2017-10-03/hedge-funds-flip-icos-leaving-other-investors-holding-the-bag

Krombholz, K., Judmayer, A., Gusenbauer, M., & Weippl, E. 2016. *The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy*. Financial Cryptography and Data Security, Lecture Notes in Computer Science. Retrieved from https://www.sba-research.org/wp-content/uploads/publications/TheOtherSideOfTheCoin_FC16preConf.pdf

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?* Harvard Business School, https://hbswk.hbs.edu/, accessed 4th of May 2018. url: https://hbswk.hbs.edu/item/industry-self-regulation-whats-working-and-whats-not

Lee, J., Li, T., & Shin, D. 2018. *The Wisdom of Crowds and Information Cascades in FinTech: Evidence from Initial Coin Offerings*. Available at SSRN: https://ssrn.com/abstract=3195877.

Leising, M. 2018. *U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether*. https://www.bloomberg.com, accessed 14th of June 2018. url: 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*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148181

Lynch, D., & Lundquist, L. 1996. *Digital money: the new era of internet commerce*. Toronto: John Willey and Sons.

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.

Marian, O. 2019. Blockchain Havens and the Need for Their Internationally-Coordinated Regulation. University of California, Irvine - School of Law. Legal Studies Research Paper Series No. 2019-14.

Matsumura, M. 2017. *ICO Governance: a Protocol-Based Self-Regulation of Token Sales in Decentralized Capital Markets*. ICO Governance Foundation White paper.

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*. Proceedings of the Internet Measurement Conference - IMC '13, (6), 127–140. https://doi.org/10.1145/2504730.2504747.

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

Narayanan, A., & Clark, J. 2017. *Bitcoin's academic pedigree*. Communications of the ACM, 60(12), 36–45.

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, New Jersey: US.

Ngo, D. 2018. *Exit Scam: Vietnamese Cryptocurrency Company Goes Dark After Allegedly Duping Investors Of US$660M In ICOs*. https://coinjournal.net, accessed 17th of April 2018. url: 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*. https://doi.org/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*. https://www.zdnet.com/, accessed 24th of June 2018. url: https://www.zdnet.com/article/hacker-returns-20000-eth-stolen-during-coindash-ico/

Pasztor, J. 2018. *Bitcoin Investing - An Ethical and Regulatory Quandary*. Journal of Financial Service Professionals 72, 30-33.

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*. ArXiv Preprint ArXiv:1511.05740, 1–33. https://doi.org/10.2139/ssrn.2692487

Platt, E. 2018. *US junk bond premiums slide to 2014 low*. Financial Times, accessed 17th of April 2018. url: https://www.ft.com/content/a9b3d584-d613-3a68-9900-faa2e0855c7c

Quinlan, B., & Cheng, H. 2013. *Fool's Gold? Unearthing the world of cryptocurrencies*. Quinlan and Associates Report.

Rajan, R. 2008. *Bankers' pay is deeply flawed*. Financial Times, 9th January 2008.

Raymond, E. 1999. *The Cathedral and the Bazaar*. O'Reilly Media, Sebastopol, California.

Reijers, W., O'Brolcháin, F., & Haynes, P. 2016. *Governance in Blockchain Technologies & Social Contract Theories*. Ledger 1, 134-151.

Reuters 2018a. *Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft*. Taiga Uranaka and Thomas Wilson report. https://www.reuters.com/article/us-japan-cryptocurrency/japan-raps-coincheck-orders-broader-checks-after-530-million-cryptocurrency-theft-idUSKBN1FI06S

Reuters 2018b. *South Korea plans to ban cryptocurrency trading, rattles market*. Cynthia Kim and Dahee Kim report. https://www.reuters.com/article/us-southkorea-bitcoin/south-korea-plans-to-ban-cryptocurrency-trading-rattles-market-idUSKBN1F002B

Rhue, L. 2018. *Trust is All You Need: An Empirical Exploration of Initial Coin Offerings (ICOs) and ICO Reputation Scores*. Available at SSRN: 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*. University of Denver Sturm College of Law, Legal Research Paper Series, Working Paper No. 18-01.

Rodrigues, U. 2018. *Semi-Public Offerings? Pushing the Boundaries of Securities Law*. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3242205

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

Schneier, B. 2011. *Secrets and lies: digital security in a networked world*. John Wiley & Sons

Schwarcz, S. 2011. *Financial Industry Self-Regulation: Aspiration and Reality*. University of Pennsylvania Law Review 159, 293-302.

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*. https://news.bitcoin.com/, accessed 4th of May 2018. url: 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.

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

Siegel, D. 2016. *Understanding the DAO Attack*. Coindesk blog.

Sijbrandij, S. 2018. *How Open Source Became the Default Business Model for Software*. https://www.forbes.com, accessed 23rd of September 2018. url: https://www.forbes.com/sites/forbestechcouncil/2018/07/16/how-open-source-became-the-default-business-model-for-software/#7c4d0c184e72

Smith, R. 2019. SEC Reels in $30 Million Alleged Diamond-Backed Crypto Scam. https://www.ccn.com, accessed 24th of May 2019. url: https://www.ccn.com/sec-30-million-crypto-scam

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*. https://cointelegraph.com, accessed 27th of April 2018. url: 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*. https://www.coindesk.com, accessed 3rd of July 2018. url: https://www.coindesk.com/new-self-regulatory-body-aims-to-develop-ico-standards/

The Guardian. 2018. *Bitcoin biggest bubble in history, says economist who predicted 2008 crash*. www.theguardian.com, Friday 2 February 2018, Angela Monaghan reports. https://www.theguardian.com/technology/2018/feb/02/bitcoin-biggest-bubble-in-history-says-economist-who-predicted-2008-crash

The Merkle. 2017. *White Hat Hackers, Smart Contract & Blockchain Experts Team Up with SmartOne in Anticipation of LEGAL Token Launch*. https://themerkle.com, accessed 27th of April 2018. url: https://themerkle.com/white-hat-hackers-smart-contract-blockchain-experts-team-up-with-smartone-in-anticipation-of-legal-token-launch/

Toffel, M. 2006. *Resolving Information Asymmetries in Markets: The Role of Certified Management Programs*. Harvard Business School Working Paper No. 07-023.

Valenzuela, J. 2017. *How Dash Solves the "ICO Problem"*. https://www.Dashforcenews.com, accessed 16th of April 2018. url: 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?* https://coincenter.org url.: https://coincenter.org/entry/what-is-open-source-and-why-is-it-important-for-cryptocurrency-and-open-blockchain-projects

Vardi, M. 2018. *How the hippies destroyed the internet*. Communications of the ACM 61, 9.

Vardi, M. 2019. *Are we having an ethical crisis in computing?* Communications of the ACM 62, 7.

Vasilescu, B., Filkov, V., & Serebrenik, A. 2013. *Stack Overflow and GitHub: Associations Between Software Development and Crowdsourced Knowledge*. 2013 IEEE International Conference on Social Computing (SocialCom), 188-195.

Vlastelica, R. 2018. *This 1 chart shows the U.S. stock market is the most expensive in the world*. https://www.marketwatch.com, accessed 17th of April 2018. url: 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*. https//github.com/ethereum/EIPs/blob/master/EIPS/eip-20-tokenstandard

Williams-Grut, O. 2017. *WALKTHROUGH: How traders 'pump and dump' cryptocurrencies*. http://uk.businessinsider.com, accessed 17th of April 2018. url: 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*. https://www.wsj.com, accessed 20th of April 2018. url: 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*(1), 7–31.

Zetzsche, D., Buckley, R.P., Arner, D.W., & Föhr, L. 2018. *The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators*. EBI Working Paper Series - 2018 – no. 18.

Zhao, W. 2017. *CoinDash ICO Hacker Nets Additional Ether as Theft Tops $10 Million*. https://www.coindesk.com, accessed 24th of June 2018. url: https://www.coindesk.com/coindash-ico-hacker-nets-additional-ether-theft-tops-10-million/

Zhou, Y., Kumar, D., Bakshi, S., Mason, J., Miller, A. and Bailey, M. 2018. *Erays: Reverse Engineering Ethereum's Opaque Smart Contracts*. Proceedings of the 27th USENIX Security Symposium. Baltimore, MD, USA.

## 7. Endnotes

[1] 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 et al. (2010) highlight this aspect of the 2007-2009 financial crisis.

[2] According to ICOdata.io, the growth rate in the number of ICOs and in the amounts raised has been nothing short of spectacular since 2014. The average arithmetic growth rate in the last 4 years has been 1,069.3% in the number of ICOs and 2,136.6% in the amount raised.

[3] 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).

[4]The current state of ICO markets also presents some of the worrying dynamics of the Dot-Com bubble of 2000.

[5] As mentioned previously, on a different spirit, President Obama signed the 2012 JOBS Act and opened the door to new markets such as ICOs.

[6] 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 and Clark, 2017).

[7] See Lynch and Lundquist (1996).

[8] For example, see Nick Szabo's Bit gold.

[9] 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, et al., 2016).

[10] Source: Coinschedule, Cryptocyrrency ICO Stats https://www.coinschedule.com/.

[11] See Hermann et al. (2016) for an historical analysis of altcoins, their properties, and evolution.

[12] The trade-off between functionality and security is a major concern in any information technology (Cranor and 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).

[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; Benedett and Kostovetsky (2018) 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.
[15] See the case of CoinDash discussed in section 3.3 in which hackers attacked the website supporting the ICO.
[16] 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 and 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 et al., 2018; Krombholz et al., 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).
[17] Although Open Social Networks could pave the way for scams, they can also be leveraged to overcome information asymmetries (Lee et al., 2018). 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.
[18] 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 and Floridi, 2004).
[19] The morally questionable actions of the opportunistic agents are detailed in the following subsections.
[20] According to insiders, the vast majority of ICOs have pre-sales; Zetzsche et al. (2018) identify pre-sales in 70% of their sampled ICOs and Kharif (2017) puts this figure at approximately 80%.
[21] According to Zetzsche et al. (2018), most of the pre-sale terms identified in their sample of ICOs do not include lock-up periods.
[22] 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).
[23] 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).
[24] 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. 17-10001 of the Southern District of New York).
[25] Regarding this, we must recall that the security of a system is defined by its weakest point (Schneier, 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.
[26] 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, et al., 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.
[27] 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.
[28] 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.
[29] See section 4.3 where white hackers are defined and their current role in ICO markets is analyzed and discussed.
[30] 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 (Reuters, 2018a). 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.
[31] 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.

[32] Bundling practices are quite common in digital markets, as shown in Kwon et al. (2005).
[33] 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.
[34] Lagace (2007) argues that third party verification represents a crucial element to assess self-regulatory initiatives and the adoption of codes of conduct
[35] 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.
[36] The empirical analysis performed in Toffel (2006) focused on the environmental certification ISO 14000.
[37] 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.
[38] 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.
[39] 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.
[40] See Sijbrandij (2018) for a description of the historical developments of open source since its inception to its commercial application.
[41] This is the reason why many of these licenses are referred to as viral or copyleft software licenses.
[42] Bartoletti et al. (2017) identify Ponzi schemes in Ethereum through the analysis of the code in smart contracts.
[43] 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.
[44] 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.
[45] 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.
[46] 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).
[47] For details of the ERC-777 standard, see https://github.com/ethereum/EIPs/blob/master/EIPS/eip-777.md.
[48] The complete description of the OpenZeppelin vesting functionality can be found at https://github.com/OpenZeppelin/token-vesting-ui
[49] According to Zhou et al. (2018), around 77.6% of smart contracts are not properly associated with corresponding source code.
[50] According to https://www.icodata.io/, and regarding ICOs issued until May, we observe a reduction of 94.5% in the volumes of financing obtained in 2019 relative to the same period in 2018.

## 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

ECGI Working Paper Series in Law



www.ecgi.global/content/working-papers

**Electronic Access to the Working Paper Series**

The full set of ECGI working papers can be accessed through the Institute's Web-site (www.ecgi.global/content/working-papers) or SSRN:

| | |
|---|---|
| **Finance Paper Series** | http://www.ssrn.com/link/ECGI-Fin.html |
| **Law Paper Series** | http://www.ssrn.com/link/ECGI-Law.html |

www.ecgi.global/content/working-papers