

**Dr. Aurelio Gurrea-Martínez**, JSM (Stanford), MSc (Oxford)  
Singapore Management University - School of Law  
55 Armenian Street  
Singapore 179943

**Australian Government**  
Department of the Treasury  
Financial System Division  
Langton Crescent  
Parkes Act 2600  
Canberra, Australia

13 March 2019

To the Australian Department of the Treasury,

On January 2019, the Australian Department of the Treasury issued a consultation paper on Initial Coin Offerings inviting interested parties to submit comments.

The document attached to this letter seeks to provide comments to the proposed regulatory framework of Initial Coin Offerings in Australia. Since most of these comments, included as Annex 1, are based on a recent work on Initial Coin Offerings co-authored with my colleague Nydia Remolina, I also include our paper as Annex 2.

I hope these comments can be helpful to improve the regulatory framework of Initial Coin Offerings in Australia.

With best wishes,



Dr. Aurelio Gurrea-Martínez  
SMU School of Law  
Email: [aureliogm@smu.edu.sg](mailto:aureliogm@smu.edu.sg)

## **Annex 1**

### **Proposal to enhance the regulatory framework of Initial Coin Offerings in Australia**

## 1. Classification of tokens

The consultation paper on ICOs (CP-ICO) issued by the Australian Department of the Treasury distinguishes three types of tokens: (i) *currency tokens*, for those digital assets conferring rights to another digital currency; (ii) *asset, equity or investment tokens*, for those digital assets conferring rights to a promised future cash flow linked to an underlying business or investment; and (iii) *utility or access tokens* to those digital assets conferring rights to have access to a product or service provided by the issuer usually at some future point in time. Likewise, the CP-ICO mentions that any type of token can be classified as a 'security', emphasizing that "*a token may be a financial product even if it is described by another name, such as a utility token*".<sup>1</sup>

In my opinion, this classification proposed by the Australian Department of the Treasury is definitely more appropriate and accurate than those proposed in other jurisdictions. For example, in the guidance on cryptoassets recently issued by the Financial Conduct Authority,<sup>2</sup> the UK regulator distinguishes between payment tokens, security tokens, and utility tokens. In my view this classification is misleading, since it mixes up the *function* of a token with its *legal nature*. From a legal (securities regulation) perspective, tokens can only be classified as a *security* or not. For this reason, in my response to the guidance on cryptoassets proposed in the United Kingdom,<sup>3</sup> I have suggested that the FCA should abandon this classification. Instead, I proposed to classify tokens depending on various factors, including function (e.g., utility tokens, asset tokens, and payment tokens), legal nature (e.g., security tokens and non-security tokens) and nature from an accounting/finance perspective (equity tokens or debt tokens). Therefore, a token could be classified as security (or not) *regardless of its function* (e.g., utility token, payment token or asset token) and its accounting and finance nature (e.g., equity or liabilities/debt).

Thus, the classification proposed by the Australian Department of the Treasury represents a significant improvement from the regulatory framework of Initial Coin Offerings proposed in other countries. Still, some improvements can be made.

First, the CP-ICO uses several expressions to refer to the same tokens. For example, it uses the expression 'asset token', 'equity token' and 'investment tokens' as synonyms. And while the use of various expressions can be useful to clarify what the regulator means by each term, I think the use of these particular expressions can be misleading. For instance, the expression 'investment tokens' can be confused with *investment products* and, if so, with security tokens, when –as explained above– an asset token (functional classification) can be a security token (legal classification) or not. Likewise, the term 'equity token' to refer to 'asset tokens' can also be misleading because some actors may believe that the asset token should be registered as equity from an accounting/finance perspective while that is not necessarily the case – it will depend on the particular features of the token. As a result, the Treasury should either abandon these misleading expressions using to clarify the type of tokens they are referring to or explain these terms a bit more in order to avoid any misunderstanding.

---

<sup>1</sup> See the Australian Government, *Initial Coin Offerings*, Issues Paper, January 2019, p. 4.

<sup>2</sup> See Financial Conduct Authority, *Guidance on Cryptoassets*, Consultation Paper 19/3, January 2019 (available at <https://www.fca.org.uk/publication/consultation/cp19-03.pdf>).

<sup>3</sup> This response is available at <http://www.derechoyfinanzas.org/comments-to-the-guidance-on-crypto-assets-issued-by-the-financial-conduct-authority/>

Second, the Treasury may also consider the possibility of classifying tokens from a functional, legal and finance perspective, as it is proposed in the paper attached as Annex 2. Under this model, tokens would be categorized depending on three criteria:

- From a **legal perspective**, tokens would be classified as *security tokens* or *non-security tokens*. This classification will depend on whether the token, based on its features and distribution, meets the definition of security existing in Australia.
- From a **functional perspective**, tokens could be classified as *utility tokens*, *payment tokens* and *asset tokens*, following the classification of the Swiss Financial Market Supervisory Authority (FINMA), that my co-author and I find particularly useful for the classification of tokens from a functional perspective.
- From a **finance perspective**, tokens would be classified as *equity tokens* or *debt tokens*, depending on the rights conferred to the purchasers of tokens (“tokenholders”). If a tokenholder is entitled to a fixed return or to a given set of products or services, my co-author and I propose to classify these tokenholders as debtholders. By contrast, if the tokenholder is entitled to variable returns depending on the issuer’s future performance, the tokenholder should be classified as an equityholder, even if these equityholders should be distinguished from the shareholders if the issuer is a corporation.<sup>4</sup>

## **2. Consumer and investor protection, market integrity and the stability of the financial system**

The regulatory framework of Initial Coin Offerings proposed by the Treasury can also be improved in other aspects mainly related to consumer and investor protection, market integrity, and the potential impact that ICOs on financial stability and market trust. To enhance these aspects, I propose the implementation of four policy recommendations: (i) issuers of any type of tokens should be required to submit a simple, standardized *electronic form* to the securities regulator (or any other public authority) providing some basic information about the ICO; (ii) *commercial banks and pension funds* should not be allowed to engage in pre-sales of tokens; (iii) several strategies should be implemented to promote *education and awareness* about the risks associated with ICOs; and (iv) various measures to protect the purchasers of *non-security tokens* should be implemented.

### **2.1. Submission of electronic form for any issuance of tokens**

Under the regulatory approach proposed by Treasury, and also existing in most countries around the world, regulators cannot easily have control over the ICO market. Indeed, since they only have the opportunity to know about those (security) tokens registered with the regulator, they do not have an entire view of the ICO market. Therefore, this lack of control may lead to several problems, including higher risk of scams, as well as lack of compliance with securities regulation even in cases of security tokens.

---

<sup>4</sup> For more details, see Gurrea-Martínez & Remolina (2018), included as Annex 2.

To solve this problem, my co-author and I propose that *any* issuance of tokens, no matter whether they are security or non-security tokens, should be *disclosed* to the regulator. The way to do so may consist of requiring issuers to submit a simple, harmonized *electronic form* to the securities regulator or any other public authority. This electronic form should contain some basic information of the issuer and the ICO, including the promoter's location, description of the token, blockchain governance, qualifications of the technical team, and risk factors.<sup>5</sup> Likewise, other information potentially relevant for investors and consumers should be including, such as the identity of the promoters and their legal advisors, the accounting and finance aspects of the ICO, and any legal or contractual provisions available to protect tokenholders. By submitting this harmonized, electronic form, not only it will be easier to monitor any issuance of tokens, but it will also be easier for investors and analysts to compare ICOs. Therefore, this comparability could serve as an additional tool to protect tokenholders, while it can also facilitate the analysis and investigation of ICOs. As a result, it will incentivize promoters to behave in a more honest and diligent manner, since the regulator will be in a better position to identify, enforce and sanction scams, as well as those ICOs failing to comply with securities regulation.

## **2.2. Bans on commercial banks and pension funds**

The purchase of tokens associated with products or projects that have not been developed yet, usually referred to as 'pre-sale of tokens', are particularly risky. In addition to the risk of scams existing in the ICO industry (according to some empirical studies, more than 80% of ICOs are scams<sup>6</sup>), some of these projects will never be developed for reasons unrelated to fraud. As I result, I think commercial banks and pension funds should not be allowed to participate in a pre-sale of tokens. And they should not be so for two primary reasons. First, these institutions invest savings and retiring pays of many debtholders unable to adjust the conditions of their 'loans'. Therefore, their clients are not usually able to adjust this risk. Second, unlike it happens with other institutions (e.g., hedge funds or even venture capital funds), investing resources in highly risky activities is not part of the business model of a commercial bank and, though a lesser extent, of a pension fund. Therefore, they should rather focus on their primary business. Finally, even if more capital requirements are imposed to compensate for the higher risk, the potential losses associated with these institutions may create several externalities for society, including lack of confidence and systemic risk.

## **2.3. Financial education and awareness**

The CP-ICO does not seem to put enough emphasis on the implementation of activities to make investors and consumers aware of the risks associated with the purchase of tokens. Several factors make the purchase of tokens particularly risky, including the high probability of scams, the lack of effective devices to protect tokenholders (especially non-security tokenholders), the larger asymmetries of information between

---

<sup>5</sup> These requirements are suggested in Chris Brummer, *What should be in an ICO white paper?* (2018) (available at <https://cointelegraph.com/news/what-should-be-in-an-ico-white-paper-expert-take>) and Chris Brummer, Trevor Kiviat, and Jai R. Massari, *What Should Be Disclosed in an Initial Coin Offering?* (2018) (available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3293311](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3293311)).

<sup>6</sup> According to some studies, more than 80% of the ICOs conducted in 2017 were scams. See <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams>

promoters and tokenholders, and the high risk of irrational behavior that seem to exist in the crypto market. For this reason, the regulator should spend more resources in educating and warning retail investors and consumers about the risks associated with the purchase of tokens. For that purpose, initiatives like the *Howey Coin* conducted by the U.S. Securities and Exchange Commission, as well as an active use of social media with information and warnings to investors, could be a first step to achieve this goal.

#### **2.4. Protection of non-security tokenholders**

Finally, the CP-ICO does not seem to provide an adequate protection to non-security tokenholders, that is, the purchasers of non-security tokens. While security tokenholders are protected by securities laws, non-security tokenholders have been left basically without any legal protection – only the white paper, whose enforceability is not even clear. Therefore, in addition to the protecting non-security tokenholders through the *electronic form*, I think other legal devices should be implemented. First, regulators may impose *cooling off* periods. Thus, non-security tokenholders will be able to return the token within a given period of time without bearing any cost. This measure not only will protect non-security tokenholders *ex post*, but it will also encourage many issuers to think twice what they are going to sell and how. Second, policy-makers may also decide to *regulate products*. Through this mechanism, the regulator may think about the possibility of prohibiting certain ICOs with terms or tokens particularly obscure. Third, regulators may also decide to impose *conduct obligations* on the issuer. Namely, they may require issuers to take into account the interest of tokenholders prohibiting situations in which the issuer seeks to exploit non-security tokenholders' biases, mistakes, and lack of information. Finally, an additional tool to protect non-security tokenholders may consist of using *litigation rules*. For instance, the legislator may establish that any unclear provision established in the white paper should be interpreted in favor of non-security tokenholders. By doing that, not only non-security tokenholders will enjoy *ex post* a higher level of protection, but issuers will also have incentives to draft the white paper in a clearer manner.

\*\*\*

## Annex 2

### The Law and Finance of Initial Coin Offerings<sup>7</sup>

Aurelio Gurrea-Martínez<sup>8</sup>

Nydia Remolina<sup>9</sup>

---

<sup>7</sup> For helpful comments and discussions, we would like to thank Chris Brummer, Alfonso Delgado, Scott Hirst, Richard Squire, Felix Steffek, Ricardo Torres, Werner Bikkerk, Jenifer Varzaly, and the participants of various events held at the U.S. Securities and Exchange Commission, Harvard Law School, Cambridge University, ITAM, the Argentinian Securities Commission, Centro de Estudios Garrigues, Javeriana University, the Sao Paulo Stock Exchange (B3), and the International Organization of Securities Commissions (IOSCO), where we had the opportunity to present previous drafts of this paper. This work will be published by Oxford University Press in a book on crypto-assets edited by Professor Chris Brummer in collaboration with the International Monetary Fund (forthcoming, 2019). This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Emerging Area Research Project Funding Initiative.

<sup>8</sup> Aurelio Gurrea-Martínez is Assistant Professor of Law at Singapore Management University, where he teaches comparative corporate governance, securities and financial regulation, and comparative and international insolvency law. He is also a Fellow of the Program on International Financial System affiliated with Harvard Law School and Director of the Ibero-American Institute for Law and Finance. Email: [aureliogm@smu.edu.sg](mailto:aureliogm@smu.edu.sg)

<sup>9</sup> Nydia Remolina León is Legal Advisor for Innovation, Regulation and Digital Transformation at Grupo Bancolombia. Lecturer in Financial Regulation at Javeriana University and Research Associate at the Ibero-American Institute for Law and Finance. Email: [nremolina@derechoyfinanzas.org](mailto:nremolina@derechoyfinanzas.org).

## Summary

<b>I. Concept, Features and Structure of ICOs</b>	<b>10</b>
<b>1. Tokens</b>	<b>10</b>
1.1 <i>The concept and features of tokens</i>	11
2.1.1. Functional classification	11
2.1.2. Legal classification	12
1.2 <i>The pre-sale of tokens</i>	13
1.3 <i>The crowdsale and distribution of tokens to the public</i>	14
<b>2. The cryptocurrencies received in return</b>	<b>15</b>
<b>3. Blockchain: the technology behind Initial Coin Offerings</b>	<b>16</b>
<b>4. The White Paper</b>	<b>18</b>
<b>5. Differences between ICOs and other methods to raise capital</b>	<b>19</b>
<b>II. Regulatory approaches to deal with ICOs</b>	<b>21</b>
<b>1. Existing regulatory approaches</b>	<b>22</b>
1.1. <i>Contractual Approach</i>	22
1.2. <i>Bans</i>	23
1.3. <i>Security Token Registration</i>	24
1.4. <i>Comprehensive Token Registration</i>	27
<b>2. Toward a safe but efficient system to deal with ICOs</b>	<b>27</b>
<b>III. Accounting and finance aspects of ICOs</b>	<b>29</b>
<b>IV. Corporate governance issues</b>	<b>31</b>
<b>1. The concept and nature of tokenholders</b>	<b>31</b>
<b>2. Protecting tokenholders from the promoter's opportunism</b>	<b>33</b>
2.1. <i>Agency problems in a world of tokenholders</i>	33
2.2. <i>Legal strategies to protect tokenholders</i>	36
2.2.1. Protecting security tokenholders	36
2.2.2. Protecting non-security tokenholders	37
2.3. <i>Market devices to protect tokenholders</i>	38
<b>V. Anti-Money Laundering implications of ICOS</b>	<b>39</b>
<b>VI. New challenges for privacy law and data protection</b>	<b>41</b>
<b>VII. Insolvency</b>	<b>42</b>
<b>VIII. International challenges and cooperation in ICOs</b>	<b>44</b>
<b>IX. Future of capital markets, finance and corporate governance in a world of tokenized securities</b>	<b>45</b>
<b>X. Conclusion</b>	<b>48</b>

## Introduction

Initial Coin Offerings (“ICOs”) are becoming an important source of funding for companies,<sup>10</sup> especially startups. In 2017, ICOs raised around \$4 billion in the United States,<sup>11</sup> reaching more than \$21 billion in 2018<sup>12</sup> and surpassing venture capital as a fundraising mechanism.<sup>13</sup>

According to the Gartner hype cycle of new technologies,<sup>14</sup> blockchain technologies are *extremely hyped*.<sup>15</sup> Nevertheless, they still offer the potential for substantial change in technology development and delivery, disrupting how the economy, businesses and our society operate.

The growth of ICOs and accompanying instances of fraud have become increasingly obvious, attracting the attention of regulators. However, due to the distinctive features of the blockchain technologies of which they are based on, such regulation is extremely different from more common forms of regulation in other industries, and varies across jurisdictions. Unlike traditional investments like stocks and bonds, ICOs issue crypto-assets. Essentially, crypto-assets are digital representations of value utilizing blockchain technologies, where ledgers keep track of ownership using peer-to-peer networks of computers. This system is decentralized and as such eludes historical markets where central intermediaries (like broker dealers, exchanges, etc.) facilitate transactions.

In this paper we analyze the legal and financial aspects of ICOs, providing a set of recommendations to enhance the regulatory framework of this new source of finance. It is organized as follows. In Part I, we examine the concept, features and structure of an ICO. We note that because ICOs ultimately run on technology connecting buyers and sellers, or holders of a crypto-asset, they do not feature centralized intermediaries or gatekeepers in their transactions. They thus have no historical precedent and raise challenging questions for authorities tasked with overseeing crypto markets. In Part II, we analyze different regulatory approaches to deal with ICOs. We argue that none of the existing regulatory models provide an efficient and effective response to the challenges raised by ICOs. For this reason, we will propose a series of reforms to enhance the existing regulatory models. Part III deals with the accounting and financial issues of ICOs. It will emphasize that the classification of tokens as debt or equity may have several implications from a legal and financial perspective. In Part VI, we will

---

<sup>10</sup> In a world of ICOs, not all issuers of tokens are “companies”. For this reason, this paper will also use other words to refer to the issuers such as “founders”, “developers” or “issuers” themselves. Following this, all these expressions will be used as synonyms in this paper.

<sup>11</sup> Frank Chaparro, *ICO funding soars above \$4 billion as US regulators crack down*. BUSINESS INSIDER (2017), available at <http://www.businessinsider.com/ico-funding-soars-above-4-billion-as-us-regulators-crack-down-2017-12>

<sup>12</sup> See <https://www.coinschedule.com/stats.html?year=2018>. See also <https://www.economist.com/technology-quarterly/2018/09/01/initial-coin-offerings-have-become-big-business> and <https://www.ft.com/content/69abdb66-666c-11e8-b6eb-4acfcfb08c11>. The latter article also points out that *block.one*, a Cayman Islands-based company, raised more than 4 billion through a single ICO.

<sup>13</sup> Betsy Verecky, *Is a Cryptocurrency a Security? Depends*, MIT Management Sloan School (2018), available at [http://mitsloan.mit.edu/newsroom/articles/is-a-cryptocurrency-a-security-depends/?utm\\_source=mitsloanlinkedin&utm\\_medium=social&utm\\_campaign=gensler](http://mitsloan.mit.edu/newsroom/articles/is-a-cryptocurrency-a-security-depends/?utm_source=mitsloanlinkedin&utm_medium=social&utm_campaign=gensler).

<sup>14</sup> The hype cycle is a branded graphical presentation developed and used by the American research, advisory and information technology firm Gartner to represent the maturity, adoption, and social application of specific technologies. The hype cycle provides a graphical and conceptual presentation of the maturity of emerging technologies through five phases.

<sup>15</sup> See Mike Walker, *Hype Cycle for Emerging Technologies 2018*, GARTNER (2018), available at: <https://www.gartner.com/doc/3885468/hype-cycle-emerging-technologies->

focus on the corporate governance aspects of ICOs. Namely, it will be shown that the purchasers of tokens are highly exposed to the risk of opportunism of the ICO's promoter. As a result, a variety of legal and market devices will be proposed to minimize those agency problems existing between issuers and buyers of tokens. Part V analyzes how ICOs may raise issues related to money-laundering, and how regulators and policy-makers can deal with these problems. In Part VI, we provide an overview of the challenges of ICOs from the perspective of privacy law and data protection. Part VII examines how a situation of insolvency may affect the issuer and buyer of tokens, and how insolvency jurisdictions should deal with those issues arising in insolvency proceedings involving crypto-assets. In Part VIII, we discuss the jurisdictional issues arising in ICOs, and why regulators, policy-makers and international organizations such as the International Organization of Securities Commissions ("IOSCO") should work together to promote coordination in a variety of issues regarding ICOs. Part IX describes the future of capital markets and corporate governance in a world of tokenized securities. Part X concludes.

## I. Concept, Features and Structure of ICOs

An ICO is a new method to raise capital. This new method differs from existing fundraising mechanisms in four primary aspects. First, the person seeking to raise capital does not issue shares, bonds, or any other existing financial products. Instead, they will use crypto-assets, often referred to as tokens,<sup>16</sup> which entitle the owner to a variety of rights. Second, the issuer does not receive money, as it happens with an issuance of shares or bonds. Instead, it receives crypto-assets generally accepted by the public such as Bitcoin or Ether. Third, the issuance of tokens is not conducted through the traditional channel in which the regulator and other third parties, such as investment banks, need to intermediate. Instead, it is conducted through a new technology, blockchain, which is the technology used to create crypto-assets such as Bitcoin or Ether. Finally, unlike what occurs with many other issuances of shares, bonds or other type of securities, the issuance of tokens does not require the preparation and registration of a prospectus, unless those tokens are considered securities under a country's securities law. Indeed, in an issuance not involving securities, the issuer will just be required to prepare a simple document, which is not subject to any supervision or imposition of mandatory terms. This document is termed a "white paper". This white paper is the primary disclosure obligation of an ICO provided that the tokens issued by the promoter are not deemed as "securities" under the relevant country's securities law.

This section will provide a common understanding of these primary aspects of an ICO.

### 1. Tokens

ICOs are also known as token sales or coin sales.<sup>17</sup> Tokens are basically *digital assets* used in connection with decentralized services, applications, and communities known as token networks. In other words, tokens are digital assets that are recorded on a

---

<sup>16</sup> Crypto-assets, tokens, or digital assets are usually used as synonyms. For example, the Mexican Fintech law refers to these instruments as 'virtual assets'. In Singapore, the regulator uses the term 'digital token'. In Switzerland and the United States, the securities regulator uses the expression 'tokens'. In the United Kingdom, the regulator uses 'crypto-assets', which are then classified in different types of 'tokens'.

<sup>17</sup> International Organization of Securities Commissions. *IOSCO Board Communication on Concerns Related to Initial Coin Offerings*, Media Release (2018), available at: <https://www.iosco.org/news/pdf/IOSCONEWS485.pdf>

distributed ledger and can be transferred without an intermediary.<sup>18</sup> This means that the structuring of the issuance, the pricing of the offer and the distribution of these instruments do not involve the participation of any regulated entity like, for example, an investment bank. A common scenario is for tokens to be sold even before the token network is operational. In some of these cases, the tokens will be functional once the platform is developed.

### 1.1 The concept and features of tokens

There is no unified classification of tokens. Tokens may differ from one another, and different countries may even adopt different classifications to refer to similar tokens. In our opinion, it might be useful to classify tokens by two factors: (i) *functionality* of the token, which focuses on the function and economic substance of the token; and (ii) *legal nature* of the token, which is based on the particular features of the token (including its distribution), and the definition of “security” established in a particular jurisdiction.<sup>19</sup> In Part III, we will include a third classification based on the nature of the token from a financial perspective. This latter classification, which categorizes tokens as debt or equity instruments, will be particularly relevant from an accounting and financial perspective, as well as for a variety of legal issues (e.g., covenants, distribution of dividends or, especially in some civil law countries, directors’ duties and liability in situations in which the company’s net capital falls below a certain percentage of the legal capital).

#### 2.1.1. Functional classification

From the perspective of their functionality, this paper follows the classification of tokens proposed by the Swiss Financial Markets Supervisory Authority (“FINMA”). FINMA categorizes tokens into three types: (i) payment tokens; (ii) utility tokens; and (iii) asset tokens.<sup>20</sup> Likewise, they recognize that “hybrid” tokens can also exist. FINMA defines *payment tokens* as synonymous with cryptocurrencies.<sup>21</sup> Therefore, these tokens are only used to make payments generally with the issuer – for example, to purchase a future product or service in which the only accepted payment are these “cryptocurrencies” issued by the promoter. The ability of these tokens to serve as a payment method elsewhere will depend on the acceptance of these tokens by third parties.

The concept of *utility tokens* used by FINMA refers to those tokens that are intended to provide digital access to an application or service.<sup>22</sup> Therefore, many companies developing technological products may opt for the issuance of this type of tokens. From a financial and accounting perspective, these tokens seem to reflect the purchase of a future good or service provided by the issuer. Finally, FINMA defines *asset tokens* as

---

<sup>18</sup> Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016) (available at <http://extropy.io/publications/bluepaper.pdf>).

<sup>19</sup> Some authors and jurisdictions distinguish between ‘security tokens’ and ‘utility tokens’. For example, see the guidance of crypto-assets issued by the Financial Conduct Authority (available at <https://www.fca.org.uk/publication/consultation/cp19-03.pdf>). See also Finance Working Paper N° 564/2018, Sabrina T. Howell, Marina Niessner, and David Yermack, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, ECGI FINANCE WORKING PAPER N° 564/201 (available at [https://ecgi.global/sites/default/files/working\\_papers/documents/finalhowellniessneryermack.pdf](https://ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf)). In our opinion, this classification adopted by many authors and countries confuses the function of the token with its legal nature. Therefore, it should be abandoned. Otherwise, it can be misleading, since ‘utility tokens’ from a functional perspective can actually be considered ‘security tokens’ from a legal perspective and *vice-versa*.

<sup>20</sup> See <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>

<sup>21</sup> *Ibid.*

<sup>22</sup> *Ibid.*

those representing assets enabling token owners' participation in real underlying companies, or earnings streams, or an entitlement to dividends or interest payments.<sup>23</sup> In terms of their economic function, these tokens are analogous to equities, bonds or derivatives.<sup>24</sup>

### 2.1.2. Legal classification

The functional classification is very useful in understanding the features, nature and economic function of tokens. Likewise, it may provide some guidance about the *tentative* regulations applicable to the tokens. For example, as asset tokens are analogous to debt or equity, these tokens probably fall into the definition of "securities". Nevertheless, this intuitive relationship between the functional classification and the legal classification is just that: intuitive. Indeed, the fact that a token is an "asset token" from a functional perspective does not necessarily mean that, from a legal perspective, the same token is a *security token* – even though it will usually be so.

Perhaps more importantly, the fact that a token is classified as "payment token" or "utility token" from a functional perspective does not mean that these tokens cannot be considered as securities. The classification of a token as a "security token" or a "non-security token", which are legal classifications, will depend on how a particular country defines "securities".<sup>25</sup> In general, this judgment should be made after assessing a variety of factors, including the structure of the token, the functionality of the token, and the way the token was distributed. If, according to a particular legal system, a token is classified as a "security", these tokens will be classified as "security tokens" from a legal perspective, and the issuance of these tokens should comply with existing securities laws. In contrast, if a token does not meet the requirements existing in a particular country to be considered a "security", the token will be classified as a "non-security token" for the purpose of this paper. Therefore, the issuance will *not* have to comply with existing securities laws.

---

<sup>23</sup> Ibid.

<sup>24</sup> See <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>.

<sup>25</sup> For example, in the United States, securities are defined according to the "Howey test", which basically requires the existence of four elements: (i) an investment of money; (ii) the expectation of profits from that investment; (iii) the existence of a common enterprise; and (iv) the generation of profits derived from the efforts of a promoter or third party. For a detailed analysis of the "Howey Test", and more generally the concept of security in the United States, see John Coffee, Jr. and Hillary A. Sale, *SECURITIES REGULATION: CASES AND MATERIALS* (Foundation Press, 12<sup>th</sup> Edition, 2012), 246-327. This definition of security follows a functional approach and it is focused on the economic substance of the investment rather than its legal form. In countries in which the concept of security is defined following this functional approach, it will be easier that an investment is considered a "security". However, this is not always the case. In some countries, the concept of security is established in a more formalistic way. Namely, the legislator may establish the type of financial instruments that can be considered a security (e.g., shares, bonds, etc.), as it happens in Singapore. As a result, any financial instrument which is not specially mentioned in legislation would be excluded from the scope of securities regulation. Finally, other countries may follow an intermediate approach: to facilitate the identification of a security, they may establish a list of financial instruments that are always deemed a "security", but they also allow other financial instruments that may meet certain requirements to be considered "securities". This latter approach is followed, for example, in Spain (see article 2 of the 2015 Securities Market Act). The approach followed by a legal system to define "security" will have great implications in the context of ICOs. For instance, while countries with a flexible concept of securities, as it happens in the United States, will make easier to include a token within the scope of securities regulation, those countries defining securities by reference to a given list of financial instruments will unlikely allow a token to be classified as a security unless the legislation is amended to especially include tokens (or a particular type of tokens) as securities. For a useful analysis of a variety of tokens to see whether they meet the requirements to be considered "securities" under Singapore law, see Monetary Authority of Singapore, *A guide to digital token offerings* (2018), 10-19.

Sometimes, the features of the token will determine its legal nature. However, as shown by cases such as *Munchee*,<sup>26</sup> the distribution of the token may end up being the defining factor distinguishing a token from a security. Therefore, even though a functional classification of tokens can be useful for several purposes, the legal classification of the token will require a deeper analysis of the token as well as the circumstances surrounding the issuance.

In many situations, issuers will ask third parties (usually lawyers) to provide advice about the nature of the token.<sup>27</sup> In cases in which a formal *legal opinion* is issued, the issuer should enjoy a presumption of *good faith* when analyzing whether it made a mistake in the issuance of tokens – for instance, not complying with securities regulations when it should. However, if it were shown that the third party acted in bad faith or with gross negligence, these “gatekeepers” could be held liable.<sup>28</sup> For this reason, we would recommend that, regardless of the potential use of gatekeepers, regulators should implement a kind of “regulatory sandbox” in which they work with the issuers in order to let them know the nature of their issuance and the applicable law.<sup>29</sup> If issuers follow these steps, good faith derived from their behavior should be an irrebuttable presumption. Moreover, they will receive protection without bearing the costs associated with the issuance of a formal legal opinion.

### 1.2 *The pre-sale of tokens*

As mentioned, tokens can either be functional or non-functional. Non-functional tokens have the sole use of acting as a fundraising mechanism and are offered to the public when the token network has not been developed. Non-functional tokens do not contain any features that are intrinsically-linked to a blockchain project. Thus, their value is driven only by speculation.<sup>30</sup> The pre-sale of tokens is not unusual. Around 70% of ICO

---

<sup>26</sup> *Munchee* was a California-based company that was seeking \$15 million in capital to improve an existing iPhone app focused on restaurant meal reviews. It sought to create an “ecosystem” in which *Munchee* and other companies would buy and sell goods and services using the tokens. The company communicated through its website, a white paper, and other means how the proceeds were used to create the ecosystem, including payments in tokens to users for writing food reviews and selling both advertising to restaurants and “in-app” purchases to app users in exchange for tokens. According to the white paper, during the offering, the company and other promoters emphasized that investors could expect that efforts by the company and others would lead to an increase in the value of the tokens. Based on this statement made by the company, the SEC decided to open an investigation for violation of federal securities regulation. *Munchee* consented to the SEC’s cease-and-desist order without admitting or denying the findings. See SEC Press Release, *Company Halts ICO After SEC Raises Registration Concerns*, Securities and Exchange Commission (December, 2017), available at <https://www.sec.gov/news/press-release/2017-227>

<sup>27</sup> These “third parties” are often called “gatekeepers”. In general, a gatekeeper can be defined as a professional who is positioned so as to be able to prevent wrongdoing by withholding necessary cooperation or consent. See Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 1 JOURNAL OF LAW, ECONOMICS AND ORGANIZATION 53. For an analysis of the concept of “gatekeepers” and how lawyers, auditors, securities analysts, credit rating agencies and investment bankers can serve as such players, see John Coffee, Jr., GATEKEEPERS: THE PROFESSIONS AND CORPORATE GOVERNANCE (Oxford University Press, 2006)

<sup>28</sup> Liability for legal opinions is a controversial issue. In general, it will depend on the jurisdiction and the role played by legal opinions in that particular jurisdiction. In the United States, for example, see Joseph L. Johnson, *Liability of Attorneys for Legal Opinions Under the Federal Securities Laws*, 27 BOSTON COLLEGE LAW REVIEW 325.

<sup>29</sup> This approach seems to have been followed by the Spanish Securities Market Authority (CNMV) in the ICO launched by Home Meal. See <http://www.europapress.es/economia/finanzas-00340/noticia-cnmv-dispuesta-colaborar-home-meal-duena-nostrum-lanzar-ico-espana-20180228164239.html>

<sup>30</sup> Alfonso Delgado et al. *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016), pp. 33.

tokens had been previously offered in a presale to a private investor group prior to the crowdsale.<sup>31</sup>

A pre-sale or a pre-ICO is a term that refers to the process that takes place before the crowdsale begins. It usually allows the investors to buy tokens before the crowdsale starts. Moreover, this token sale event usually has separate smart contracts from the main crowdsale event.<sup>32</sup> The main idea of a pre-sale is to provide discounts. The buyers that participate in the pre-sale often get cheaper prices per token. As ICOs impose a minimum and maximum threshold for their token crowdsales, blockchain startups often present discounted rates and merits for investors that purchase their crypto-tokens at an early stage.<sup>33</sup> Thus, investors in the crowdsale phase of the ICO are required to purchase tokens at a higher rate than early investors. In other words, ICO pre-sales provide benefits for early investors. According to blockchain investment funds and even Ethereum co-founder, Vitalik Buterin, since 2017, the incentivization system for early investors by popular ICOs has led to the network congestion of Ethereum, driving transaction fees above average. When a large number of ICOs are in the works, people will likely buy quantities of Ether so that they can invest in said ICOs—which may drive up the price of the cryptocurrency. During times when Ether’s price skyrockets, transaction fees can become more expensive. For instance in March of 2017, Ethereum co-founder Vitalik Buterin revealed that an investor in the ICO of BAT spent \$2,210 as a transaction fee for one payment to receive the advantages and discounts granted to early investors.<sup>34</sup>

Some companies decide to conduct the pre-sale of tokens only with “accredited” investors. By some informal accounts, funds from accredited investors make up between 60%-80% of the total funds raised in a direct token pre-sale.<sup>35</sup> These market players, including accredited investors such as hedge funds, are performing bump-and-dump practices in ICO markets when participating in pre-sales of tokens.<sup>36</sup>

Furthermore, in these token pre-sales, some issuers enter into a Simple Agreement for Future Tokens (“SAFT”) with these accredited investors. The SAFT is an investment contract whereby investors purchase the right to receive tokens in the subsequent token network launch. In exchange, the company promises to deliver tokens upon the launch of the token network for the investors’ promise to pay immediately. Under US law, the SAFT is considered a security.<sup>37</sup>

### 1.3 The crowdsale and distribution of tokens to the public

---

<sup>31</sup> This percentage is based on a sample of 450 ICOs. See Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner and Linus Föhr, *The ICO Gold Rush: It’s a scam, It’s a bubble, It’s a super challenge for regulators*. EUROPEAN BANKING INSTITUTE WORKING PAPER SERIES 2018 – NO. 18 (2018) pp. 11.

<sup>32</sup> See Hackernoon, *How is the Presale Different From the Crowdsale*. <https://hackernoon.com/how-is-the-presale-different-from-the-crowdsale-f369f484794d>

<sup>33</sup> These discount rates can go up to 30%. For example, in the ICO of the messaging application Kik, the pre-ICO sale allowed Blockchain Capital, Pantera Capital and Polychain Capital to purchase kin tokens at a 30 percent discounted rate. See <https://techcrunch.com/2017/08/29/kik-ico-september-125-million/> and [https://www.reddit.com/r/KinFoundation/comments/743eim/icos\\_must\\_stop\\_institutional\\_investors\\_from/](https://www.reddit.com/r/KinFoundation/comments/743eim/icos_must_stop_institutional_investors_from/)

<sup>34</sup> See <https://www.ccn.com/hedge-funds-investing-early-in-icos-is-abusive-cryptocurrency-investor/>

<sup>35</sup> See Juan Batiz-Benet, Jesse Clayburgh and Marco Santori. *The SAFT Project: Toward a Compliant Token Sale Framework*. Protocol Labs & Cooley LLP (2017) (available at: [https://saftproject.com/static/SAFT-Project-White paper.pdf](https://saftproject.com/static/SAFT-Project-White%20paper.pdf) ) pp. 4.

<sup>36</sup> *Hedge Funds Investing Early in ICOs is Abusive: Cryptocurrency Investor*. Altcoin Analysis (October, 2017) (available at: <https://www.ccn.com/hedge-funds-investing-early-in-icos-is-abusive-cryptocurrency-investor/> )

<sup>37</sup> This has been used only in pre-sales of non-security tokens. See Juan Batiz-Benet, Jesse Clayburgh and Marco Santori. *The SAFT Project: Toward a Compliant Token Sale Framework*. Protocol Labs & Cooley LLP (2017) (available at: [https://saftproject.com/static/SAFT-Project-White paper.pdf](https://saftproject.com/static/SAFT-Project-White%20paper.pdf) )

After the token pre-sale, the company can start to build the network or develop the project described in its white paper. As of the date of this paper, no empirical studies have measured the rate of token pre-sales that successfully progress into a real project and what percentage results in an undeveloped idea jeopardising buyers' interests. Therefore, completion or abandonment rates remain unclear and could be part of a future empirical study regarding ICOs.

Once the network is developed, the company sells part of its tokens in exchange for cryptocurrencies. Generally, such cryptocurrencies would be Bitcoin or Ether. The crowdsale is the core of an ICO. It is the process of raising funds from all type of buyers or investors. Developing a network may sound easy. However, the risk of not developing a project is relatively high –even in the absence of fraud– considering that many of these projects promise to develop some kind of product or service on a blockchain. And the success of these projects could be complex to achieve due to the operational risks and scalability problems of blockchain technology.<sup>38</sup>

For example, “The DAO”<sup>39</sup> investigation proved that vulnerabilities in the code can be exploited by hackers to make funds disappear. The DAO was launched on 30<sup>th</sup> April, 2016, with a 28-day funding window. It proved popular, raising over \$100m by 15<sup>th</sup> May, and by the end of the funding period, The DAO was the largest ICO at the time, having raised over \$150m from more than 11,000 individuals. During the crowdsale, several people expressed concern that the code was vulnerable to attacks.<sup>40</sup> A bug was exploited by a hacker who took more than \$3.6m worth of Ether by mid-June. Additionally, the price of Ether dropped from over \$20 to under \$13. This situation brought the project to an end.<sup>41</sup> To elaborate, ICOs tend to have a minimum threshold for funding – if this threshold is not met by the end of the funding period, the funds are usually returned to investors automatically in a process called “finalization”.<sup>42</sup> In today's ICOs, it is not clear what happens if the project is not developed and what is the enforcement mechanism for holding the developer accountable to the tokenholders. The degree of accountability also differs if the tokens are security tokens or non-security tokens.

## 2. The cryptocurrencies received in return

The cryptocurrencies accepted by issuers in an ICO are commonly-traded cryptocurrencies. Therefore, in exchange for issuing tokens, issuers usually receive cryptocurrencies such as Bitcoin or Ether. These commonly-traded cryptocurrencies may help companies to cash out the proceeds of the ICO. Typically, the issuer specifies in the white paper the type of cryptocurrencies accepted in exchange for the

---

<sup>38</sup> See Deloitte. *Blockchain risk management – Risk functions need to play an active role in shaping blockchain strategy.* (2017) (available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf>)

<sup>39</sup> A DAO is a Decentralized Autonomous Organization. Its goal is to codify the rules and decision-making apparatus of an organization, eliminating the need for documents and people in governing, creating a structure with decentralized control. “The DAO” is the name of a particular DAO, conceived of and programmed by the team behind German startup Slock.it - a company building “smart locks” that let people share their things (cars, boats, apartments) in a decentralized version of Airbnb.

<sup>40</sup> See *Understanding DAO hack.* Coindesk (2017) (available at: <https://www.coindesk.com/understanding-dao-hack-journalists/>)

<sup>41</sup> Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016), pp. 26.

<sup>42</sup> Alfonso Delgado *et al*. *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016), pp. 9.

tokens. For example, if the blockchain network used to develop the issuer's project is Ethereum, the issuer will likely require Ethers.

This represents an enormous difference between ICOs and traditional methods to raise funds. The companies launching ICOs must make an analysis of the assumed price of the cryptocurrency received from tokenholders. The value of the cryptocurrency varies during the course of the ICO and the development of the project. This feature of ICOs mandates an analysis of the risks and problems companies might face when receiving a volatile asset to fund the development of a project. We will address this issue in Part VII.

### 3. Blockchain: the technology behind Initial Coin Offerings

Data has commonly been stored in centralised databases.<sup>43</sup> A database is a structured collection of data that is stored on a computer, referred to as the server. Centralised databases are maintained by a central administrator and stored in a single server. This administrator is an intermediary that is trusted to maintain the data.<sup>44</sup> In turn, users who want to access the stored data must send a request to the administrator's server. While this centralized databased can reduce costs precisely due to centralization, this same attribute makes it more vulnerable to single point of failure issues<sup>45</sup> and to denial-of-service ("DoS") attacks.<sup>46</sup>

In contrast, a distributed database is a collection of multiple databases that are logically interrelated and distributed across a computer network.<sup>47</sup> In these systems, the data can be replicated and stored in separate physical locations to prevent single point of failure issues and DoS attacks. However, distributed databases are costlier to maintain, due to higher storage, maintenance and labour costs. It is also challenging to preserve the integrity (i.e. correctness and consistency) of the data across the network.<sup>48</sup>

In 2008, the world started to talk about blockchain technology<sup>49</sup> which aims to enable data to be stored and maintained by network users themselves, without having to rely on any "trusted" third parties. In a broad sense, blockchain is used to describe the suite of technologies that allow computers in a peer-to-peer network to reach agreement over shared data.<sup>50</sup> In a distributed peer-to-peer network, the participating computers

---

<sup>43</sup> Sebastian Meunier, *Blockchain technology – a very special kind of Distributed Database* (2016).

<sup>44</sup> See Alfonso Delgado and Nydia Remolina, *Foundations of Blockchain Technology*, IIDF Working Paper Series (2019).

<sup>45</sup> A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system. See Kevin Dooley, *Designing Large Scale Lans: Help for Network Designers*, O'REILLY MEDIA (2009), pp. 31.

<sup>46</sup> Where an external attacker temporarily prevents legitimate users from accessing the database by flooding the network with superfluous requests. See Alfonso Delgado and Nydia Remolina, *Foundations of Blockchain Technology*, IIDF Working Paper Series (2019).

<sup>47</sup> In distributed systems, not all storage devices are attached to a common processor.

<sup>48</sup> See Alfonso Delgado and Nydia Remolina, *Foundations of Blockchain Technology*. IIDF Working Paper Series (2019).

<sup>49</sup> In 2008 Satoshi Nakamoto, a pseudonym used by the inventor(s) of blockchain, published the Bitcoin paper and the source code on the Internet. In January 2009, New Liberty Standard opened the first Bitcoin trading platform. The initial exchange rate was 1,309.03 Bitcoin for one U.S. dollar. and in February 2010, the first payment in Bitcoin was processed at a price of 10,000 (more than \$140 million at today's exchange rate). The first large companies to accept Bitcoin were WordPress, Overstock.com, Zynga, and TigerDirect. See Satoshi Nakamoto, *A Peer to Peer Electronic Cash System*. (2008) Available at: <https://bitcoin.org/bitcoin.pdf>

<sup>50</sup> See Peter Van Valkenburgh, *What is "Blockchain" Anyway* (2017); Alfonso Delgado and Nydia Remolina, *Foundations of Blockchain Technology*, IIDF Working Paper Series (2019).

are commonly referred to as nodes (or peers). Importantly, the tasks are not controlled or coordinated by a central node or an intermediating trusted party. Rather, these tasks are distributed across the nodes that record data into the network. This shared data record is composed of a series of entries that are linked to accounts from users and show every transaction that has been confirmed by the nodes. A protocol provides a set of rules and procedures that nodes must follow to share and verify the data.

This 2008 idea was the base of the most famous case of blockchain technology usage: Bitcoin. From there, the blockchain hype became a reality and developers promised the world that blockchain would be disruptive, even stating that it could lead a revolution, similar to what the internet did for the world previously.<sup>51</sup> Inspired by cryptocurrencies, startups in particular blockchain-based companies, realized that they could raise capital through issuing digital assets without intermediaries. Generally, the funds raised are used to build a new blockchain network, develop a decentralized application<sup>52</sup> that runs on an existing blockchain network, or both.<sup>53</sup>

This has evolved rapidly in the last couple of years. In 2013, Mastercoin launched the first ICO, which raised \$5 million of Bitcoin equivalent.<sup>54</sup> After 2013, blockchain technology became the need of funding from many blockchain-based project developers. Even though it all started as a fundraising mechanism used mostly among the blockchain and technology community to boost innovative ideas, investors and projects are turning becoming mainstream. Recent examples have even included celebrity promoters such as Paris Hilton (LydianCoin), 'Ghostface Killah' from the Wu Tang Clan (Cream Capital), Jamie Foxx (Cobinhood) and Floyd Mayweather Jr. (Stox).<sup>55</sup> Furthermore, investors have become more interested in ICOs. These are not just investors with prior interest in technology-related investments but also retail investors who want to diversify their portfolios and find ICOs an attractive speculative investment.<sup>56</sup> Technology-based companies are not the only ones implementing blockchain. A broader set of companies desire to build networks or develop decentralized applications as well. These companies are using ICOs as a fundraising method as well.<sup>57</sup> In 2017 and 2018, sectors such as finance, gaming, internet of

---

<sup>51</sup> Blockchain technology reduces the role of intermediaries by allowing people to transfer digital assets - property or data -, in a safe, secure, and immutable way, the technology can create: digital registries (cryptocurrencies) that are not backed by any central authority; self-enforcing smart contracts, decentralized marketplaces; decentralized communications platforms. See Aaron Wright and Primavera de Filippi. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. CYBERSPACE LAW E-JOURNAL (2015), (available at [https://www.intgovforum.org/cms/wks2015/uploads/proposal\\_background\\_paper/SSRN-id2580664.pdf](https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf))

<sup>52</sup> The dApp concept is still in its nascent stage. A decentralized application (dApp) is an application that runs on a P2P network of computers rather than a single computer. See <https://hackernoon.com/what-are-decentralized-applications-dapps-explained-with-examples-7ff8f2c4a460>

<sup>53</sup> See Alfonso Delgado and Nydia Remolina, *Foundations of Blockchain Technology*, IIDF Working Paper Series (2019).

<sup>54</sup> Alfonso Delgado et al, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016).

<sup>55</sup> Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner and Linus Fôhr, *The ICO Gold Rush: It's a scam, It's a bubble, It's a super challenge for regulators*. EUROPEAN BANKING INSTITUTE WORKING PAPER SERIES 2018 – NO. 18 (2018)

<sup>56</sup> "Now we are seeing (...) that the latest ICOs are getting up to 80% of their funding from smaller buyers," says Daria Generalova, one of the founders of ICO Box in Vancouver. "The Bitcoin rate bleed can be considered as one of the underlying reasons for the upswing in token sales. Most of those tokens are paid for in bitcoin. But now that bitcoin is down, you will see investors holding onto it before they buy the smaller tokens in anticipation of a rate bounce." See Keneth Rapoza, *Is It Too Late To Make Your Fortune In Cryptocurrency ICOs?* FORBES (February 7, 2018) (available at: <https://www.forbes.com/sites/kenrapoza/2018/02/07/as-bitcoin-struggles-will-investor-interest-in-icos-weaken/#3c812fd6433a>)

<sup>57</sup> According to the hype cycle of blockchain technology, interest in blockchain continues unabated among enterprises in 2018 and it is expected to remain the same in 2019. Much of the focus is educational and

things, cloud computing and even restaurants used ICOs as a fundraising method, in contrast with 2014 when ICOs were mainly used by core tech businesses.<sup>58</sup>

#### 4. The White Paper

Developers of an ICO publish a document, known as a “white paper”, that explains how the project is to be funded. A white paper is essentially a business plan. Most ICOs will allow potential investors – or actually any interested reader – to download their white paper off their official website. Some websites also serve as databases for the most recent white papers published.<sup>59</sup> White papers are also one of the first elements of a project investors should look at prior to deciding if it is a solid investment or an attractive asset to buy.<sup>60</sup>

The first white paper, and clearly the one that was used as a model for ICOs, is Satoshi Nakamoto’s paper on Bitcoin. Since the structure of a white paper has not been regulated, market participants are starting to find a common ground on what should be the content of these documents. According to some empirical studies regarding ICOs and their white papers,<sup>61</sup> there is one consistent characteristic among them: a technical description of the underlying technology for which funding is sought as well as some description of the potential use and benefits of said technology. Basically, it is a general description of the project to be executed and the benefits and disruption that project can bring to the table.

ICO white papers may present certain issues. On the one hand, the paper may provide misleading information. For example, it can state that a token is not a security when it is, or it cannot stay the appropriate applicable law.<sup>62</sup> On the other hand, promoters may omit some relevant information they may disclose only those aspects that can be beneficial to them at the expense of the purchasers of tokens.<sup>63</sup>

---

experimental as executives struggle to understand concepts and applicability. Industries have made some progress, but maturity timelines are uncertain, and adoption at scale remains very scarce in a global context. See David Furlonger, Rajesh Kandaswamy. *Hype Cycle for Blockchain Business*. GARTNER INC. (2018) (available at: <https://www.gartner.com/doc/3884146/hype-cycle-blockchain-business>)

<sup>58</sup> See <https://next.autonomous.com/thoughts/jan-2018-ico-and-crypto-fund-numbers>.

<sup>59</sup> For example <http://white.paperdatabase.com/>

<sup>60</sup> As we will see in following sections, not all tokens are investments. For example, some of them only grant access to a platform or a discount. These tokens should not be considered necessarily as an investment contract.

<sup>61</sup> Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner and Linus Föhr, *The ICO Gold Rush: It’s a scam, It’s a bubble, It’s a super challenge for regulators*, EUROPEAN BANKING INSTITUTE WORKING PAPER SERIES 2018 – NO. 18 (2018).

<sup>62</sup> Only 31% of the ICOs in a sample of 450 ICOs mention the law applicable to the ICO. In 37.7% of the cases the white paper excluded investors from certain countries from participation. In 86.5% of the cases there is no information at all as to the regulatory status of the ICO. This also included cavalier disregard of the need to inform a participant as to where precisely their funds are going. See Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner and Linus Föhr, *The ICO Gold Rush: It’s a scam, It’s a bubble, It’s a super challenge for regulators*, EUROPEAN BANKING INSTITUTE WORKING PAPER SERIES 2018 – NO. 18 (2018).

<sup>63</sup> The risks of selective disclosure and the benefits associated with harmonization and comparability may justify mandatory disclosure in capital markets. For a discussion on this issue, see Armour *et al*, PRINCIPLES OF FINANCIAL REGULATION (Oxford University Press, 2016), pp. 164-167; Luca Enriques and Sergio Gilotta, *Disclosure and Financial Market Regulation*, in Ellis Ferran, Niamh Moloney and Jennifer Payne (eds), THE OXFORD HANDBOOK ON FINANCIAL REGULATION (Oxford University Press, 2015), pp. 511-25; Merrit Fox, *Retaining Mandatory Securities Disclosure: Why Issuer Choice is not Investor Empowerment*, 85 VIRGINIA LAW REVIEW 1335 (1999); Zohar Goshen and Gideon Parchomovsky, *The Essential Role of Securities Regulation* 55 DUKE LAW JOURNAL 711 (2006). Pointing out the benefits of standardization in some particular rules (e.g., accounting), see John Armour *et al*, THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH (Oxford University Press, 2017), pp. 19. Likewise, using Akerlof’s seminal work about asymmetries of information, it can be argued that the lack of enough information about all issuers may lead to an adverse selection problem: investors will not be able to distinguish “good” and “bad” issuers. Therefore, they might be reluctant to provide finance, or they will

These asymmetries of information might be corrected by either setting out which elements should be included as a minimum in the white papers by an overarching body, or letting markets decide the best way to guarantee a certain degree of standardization, for example using analysts or law firms as advisors in structuring ICOs or through peer reviews.<sup>64</sup> Companies might also engage in public discourse, defending the white paper and even advertising an upcoming token sale. As a result of this marketing, advertising and public discourse, some pre-sales could make many tokens meet the definition of 'security' under some countries' securities laws.<sup>65</sup>

When the white paper is first published, usually developers have little more than the description of what they want to achieve after the ICO. However, in some white papers, part of the code is published. Thus, the tokens offered in this stage are not functional for using the platforms. Even though those tokens cannot be utilized, they can still be traded during pre-sales of tokens.

## 5. Differences between ICOs and other methods to raise capital

ICOs present some similarities with other financing methods, such as venture capital, angel investment, initial public offerings and especially crowdfunding. Actually, ICOs are sometimes considered as an application of the crowdfunding mechanism to blockchain-based companies or projects.<sup>66</sup> Since there are no empirical studies determining why companies may prefer ICOs over other fundraising methods, we will try to describe the main differences and similarities between these methods from a functional, finance and regulatory perspective. Thus, it will be easier to identify those aspects that make an ICO a more or less attractive method to raise capital.

Table 1. Differences and Similarities between ICOs and other sources of financing

	IPO	Crowdfunding	Venture Capital	ICO
<b>Level of regulatory compliance</b>	IPOs are heavily regulated in all jurisdictions by securities regulations. This process often requires the intervention of an underwriter (one or more investment banks) and law firms.	Crowdfunding is not regulated in most jurisdictions. However, in the US, UK and some continental European countries, it is already regulated. (e.g. US regulations of crowdfunding have been in place since 2012). Some countries in Latin America enacted	Venture capital funds are subject to the same basic regulations as other forms of private securities investments. Additionally, private equity firms often have to register with securities regulators and are subject to some	ICOs are regulated in some jurisdictions. Only those considered securities are subject to securities regulations. <sup>67</sup> There are almost no barriers to entry for those who wish to conduct an ICO (especially if the

do so at a higher cost for everyone, considering that, in the absence of mandatory (and standardized) disclosure, many "bad issuers" may decide to provide just "selective disclosure" of what it can be only in their interest. For a general analysis of this problem, see George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 THE QUARTERLY JOURNAL OF ECONOMICS 488 (1970). In the context of ICOs, Professor Chris Brummer has advocated for standardizing disclosure in white papers. See <https://bitcoinmagazine.com/articles/congressional-hearings-we-must-distinguish-digital-commodities-icos/>

<sup>64</sup> Some advisors and law firms are specialized now in review ICO papers, and some of them are "certified" by a peer review.

<sup>65</sup> The SAFT transaction might rely on Rule 506(c) of the Securities Act (United States federal securities regulation) which allows for general solicitation of investors, but requires that the offering must be limited, in the end, only to verified accredited investors.

<sup>66</sup> Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016).

<sup>67</sup> We will describe the different regulatory approaches in Section II.

		primary legislation regarding crowdfunding in recent years as well (i.e. Mexico, Argentina, Colombia).	reporting requirements.	token is a non-security token). Some basic coding skills to generate tokens is the only entry barrier <sup>68</sup> .
<b>Limits /caps</b>	No limits.	In almost all jurisdictions, crowdfunding is capped at certain amounts.	No limits in investing but the venture capital funds have a fixed life.	No limits.
<b>“Investors”</b>	Institutional investors and retail investors participate in the distribution of securities through IPOs.	Funds raised from members of the public, many of whom are not professional / institutional investors. However, crowdfunding campaigns generally take place through an intermediating platform that extracts fees from issuers	A venture capitalist is a person who makes venture investments and these venture capitalists are expected to bring managerial and technical expertise as well as capital to their investments. Venture capital funds are typically managed by a venture capital firm, which often employs individuals with technology backgrounds (scientists, researchers), business training and/or deep industry experience.	None of the regulatory approaches so far have limited ICOs. <sup>69</sup> It follows that current investors would refer to institutional investors and retail investors.
<b>Disclosure requirements</b>	IPOs require the preparation of a prospectus, which structure and content is highly regulated.	Companies issuing equity (or debt) via crowdfunding platforms are required to disclose essential information to investors	Venture capital funds are accountable to their own investors. This provides an incentive to screen and monitor investments carefully	The content of a white paper is not regulated.
<b>Secondary market of the instruments issued</b>	The securities will have a secondary market which is determined in the prospectus. The securities, when issued, are registered in a stock exchange.	Securities are privately-held and, generally, there is no secondary market to trade them	These funds have a fixed term.	Depending on the structure of the token, some will have a secondary market. This feature could mean in some jurisdictions that the token is a security.
<b>Pricing</b>	IPOs have different mechanisms for pricing: Fixed price, Dutch auction,	The platform is responsible for the valuation and pricing of the projects in almost all jurisdictions. The	In return for financing one to two years of a company’s start-up, venture capitalists expect a ten times	Price comes from issuer and it is subjective.  The ICO mechanism allows

<sup>68</sup> The Ethereum’s introductory tutorial teaches this basic coding skills. See Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016)

<sup>69</sup> This statement excludes jurisdictions that have prohibited ICOs, such as China.

	Bookbuilding (which is the most common method)	platforms is a supervised entity.	return of capital over five years. <sup>70</sup>	entrepreneurs to generate buyer competition for the token, which, in turn, reveals consumer value without the entrepreneurs having to know, <i>ex ante</i> , consumer's willingness to pay.
<b>What is being sold</b>	Generally shares (equity)	Generally securities that can be classified as equity (equity crowdfunding) or debt (crowdlending).	Generally shares (equity)	Coins or tokens, which can be classified as securities or non-security tokens, and equity or debt, depending on the features of the token.
<b>Accountability</b>	Issuers, law firms and underwriters in an IPO may be liable for misrepresentations or omissions in a prospectus.	The funding portals or platforms are subject to registration and supervision from the securities market authorities.	Venture capital funds are accountable to their own investors. This provides an incentive to screen and monitor investments carefully.	ICOs can be securities offerings and they may need to be registered.

Source: Alfonso Delgado *et al* (2016) and authors' elaboration

Despite these similarities and substantially different regulatory approaches to ICOs among jurisdictions, which makes the comparison harder, the ICO market was 40% of the size of the IPO market and 30% the size of the venture capital market during the first quarter of 2018.<sup>71</sup> The size of this phenomenon has perked the interest of regulators. The following section analyzes how different jurisdictions and regulators are coping with ICOs and provides a new safe but efficient system to deal with this method to raise funds.

## II. Regulatory approaches to deal with ICOs

Regulators around the world approach ICOs very differently.<sup>72</sup> For example, some countries, such as China<sup>73</sup> and South Korea,<sup>74</sup> have opted to prohibit ICOs. In other jurisdictions, including the United States,<sup>75</sup> Singapore,<sup>76</sup> and Switzerland,<sup>77</sup> tokens are

<sup>70</sup> Bob Zider. *How Venture Capital Works*. HARVARD BUSINESS REVIEW. (1998) (available at: <https://hbr.org/1998/11/how-venture-capital-works>)

<sup>71</sup> Caitlin Long. *6 Facts Institutional Investors Should Know about Crypto*. (April, 2018). <https://caitlin-long.com/2018/04/24/6-facts-institutional-investors-should-know-about-crypto/>

<sup>72</sup> For an analysis of the statements issued by many securities regulator about ICOs, and how some of them plan to deal with ICOs, see <https://www.iosco.org/publications/?subsection=ico-statements>

<sup>73</sup> The details of this prohibition can be found in several sources. For instance, see <https://www.ft.com/content/3fa8f60a-9156-11e7-a9e6-11d2f0ebb7f0>

<sup>74</sup> Analyzing the recent ban of South Korea, see <https://www.reuters.com/article/us-southkorea-bitcoin/south-korea-bans-raising-money-through-initial-coin-offerings-idUSKCN1C408N>

<sup>75</sup> The U.S. Securities and Exchange Commission's statements on ICOs can be found here: <https://www.sec.gov/ICO>

allowed. However, issuers need to comply with existing securities laws if the token is classified as a ‘security’ under the relevant country’s securities law. Finally, in other countries like Mexico,<sup>78</sup> any issuance of tokens have to be authorized by the regulator. Therefore, regardless whether they are security or non-security tokens, the issuer must attain the approval of the regulator before proceeding with any issuance of tokens.

As it will be discussed, all of the existing regulatory approaches present some flaws. For this reason, we will propose a new model to regulate ICOs that, while facilitating the use of ICOs as a source of finance, seeks to (ii) enhance the protection of the purchasers of tokens; and (iii) create a safe, fair and efficient regulatory environment.

## 1. Existing regulatory approaches

### 1.1. Contractual Approach

One possible approach may consist of excluding tokens from the scope of securities regulation. Under this approach, any issuance of tokens –and the terms provided in the white papers– would be exclusively subject to the law of contracts. In countries with a definition of ‘securities’ based on a closed catalogue of financial products (e.g., shares or bonds), as it is the case in Singapore, this approach will be easily achieved. The regulator should not need to enact new legislation. If things remain *status quo*, all issuances of tokens would be excluded from securities law, unless the token can be classified as a share, bond or other product included in the definition of security.<sup>79</sup>

By contrast, in countries with a functional concept of securities, as it happens in the United States, where the economic substance prevails over the legal form, an adoption of this model may require action by the regulators. Namely, it may force the regulator to enact legislation prescribing that even if a token meets the requirements to be deemed a security, it will not be subject to securities regulation. This regulatory approach would specifically exclude tokens from securities laws. As a result, ICOs would be exclusively governed by the law of contracts.

This contractual model may reduce regulatory costs associated with an issuance of tokens. Therefore, it can make ICOs a more attractive method to raise capital. However, it would create several problems. First, this approach would not provide a level playing field. By allowing functionally similar products to be subject to different regulatory frameworks, the regulator would unfairly discriminate those products subject to securities laws. Since these latter products would be subject to a higher regulatory burden, the regulatory costs borne by an issuer of tokens would be lower, even when,

---

<sup>76</sup> The Monetary Authority of Singapore’s statement on ICOs can be found here: <http://www.mas.gov.sg/News-and-Publications/Monographs-and-Information-Papers/2017/Guidance-on-Digital-Token-Offerings.aspx>.

<sup>77</sup> The Swiss securities regulator has provided a coherent and thoughtful guidance on ICOs: <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>

<sup>78</sup> See Mexico Fintech Law (In Spanish: *Ley para regular las Instituciones de Tecnología Financiera*). Available at: [http://www.senado.gob.mx/sqsp/gaceta/63/3/2017-10-12-1/assets/documentos/Iniciativa\\_Ejecitvo\\_Federal.pdf](http://www.senado.gob.mx/sqsp/gaceta/63/3/2017-10-12-1/assets/documentos/Iniciativa_Ejecitvo_Federal.pdf)

<sup>79</sup> While this is very unlikely in most jurisdictions, where shares or bonds are defined in a more formal way rather than on a functional basis, this scenario can be possible under Singapore law. See Monetary Authority of Singapore, *A Guide to Digital Token Offerings* (2018), pp. 3 allowing tokens to be considered “shares” when it confers or represents ownership interest in a corporation. Therefore, if a token confers or represent ownership interest in a corporation, can be considered a “share”. And if so, it will be a security.

from a functional perspective, they offer a similar product. Moreover, in countries in which the concept of security is defined from a functional perspective, this approach would also be inconsistent with the definition of security. Therefore, the adoption of this model would also require a modification of the concept of security.

Second, this approach would also be riskier for investors in several ways. On the one hand, since no mandatory disclosure would be required, the issuer would be free to select the amount of information provided to investors and how this information is disclosed. Therefore, the issuer can take advantage of this situation to include obscure terms and omit some relevant information. On the other hand, the lack of mandatory disclosure would also make harder the comparison of ICOs. Therefore, it will be more difficult (or at least costlier) to identify credible, value-creating projects providing a greater level of protection to the purchasers of tokens. Finally, by excluding these products from the scope of securities regulation, the purchasers of token would not be protected by the securities supervisor. Therefore, unless the power to protect consumers by overseeing the terms of the white papers are transferred to another regulatory agency (for example, a Consumer Protection Bureau), the level of protection to the purchasers of tokens will be significantly reduced. And it will be reduced not only for the higher asymmetries of information potentially created between issuers and tokenholders, but also for the higher risk of fraud, or at least opportunism, existing in a world in which the issuer knows, from an *ex ante* perspective, that the issuance and terms associated with the ICO will not be subject to the supervision of any regulatory authority.

## 1.2. *Bans*

Another regulatory approach may consist of banning ICOs. This prohibition may take several forms. First, the regulator may decide to prohibit any type of ICO, as it happens in China and South Korea. This prohibition may be due to several factors. For example, the regulator may consider that the risks associated with this new source of finance (especially in terms of fraud, money laundering and opportunistic behavior over naïve consumers) exceed its benefits. Therefore, it does not make sense to promote this fundraising method, at least while the regulator does not come up with an appropriate regulatory framework to deal with the risks of ICOs. Likewise, the use of ICOs may also have adverse effects for a country's economic and monetary policy. After all, an issuance of tokens not only involves companies raising cryptocurrencies rather than official currencies, but also that purchasers of those tokens have previously acquired cryptocurrencies in order to be allowed to participate in the ICO. Therefore, the amount of official currencies might be significantly reduced, while the investment and consumption in the country may increase or at least remain stable. As a result, the Government may lose control over some relevant factors that may affect the economy and monetary policy of the country.

Second, regulators may decide to prohibit ICOs for certain constituencies. For instance, the regulator may decide to prohibit retail consumers to be involved in an ICO due to the fact that, as a result of the higher asymmetries of information that they face, they might be more exposed to the promoters' opportunism. Likewise, the regulator may also ban commercial banks and some institutional investors from purchasing

tokens. After all, not only they manage other people's money, but several reasons mainly associated with systemic risk seem to recommend a more risk-averse investment policy in these entities. And the purchase of tokens is highly risky.

Finally, the regulator may decide to ban the purchase of tokens upon the reaching of certain limits. In other words, it can impose limitations in the amount of tokens potentially acquired by certain purchasers, as it seems to be the approach followed in Russia.<sup>80</sup> By implementing this restriction, the regulator would limit the potential losses that tokenholders may lose in case of being involved in a fraudulent or just unsuccessful ICO.

In our view, while the reasons to ban the purchase and issuance of ICOs may seem plausible (especially taking into account that more than 80% of ICOs are scams<sup>81</sup>), this policy followed in China and South Korea may prevent many firms and early-stage ventures from receiving finance to develop their projects. Moreover, if the primary concerns of the regulator have to do with the risk of fraudulent behavior and the economic and monetary consequences of the risk of ICOs, there are more efficient ways to deal with these issues, as will be discussed in our proposal to create a safe regulatory framework for ICOs. As for the limitation in the amount of tokens potentially acquired by a single purchaser, we believe that it just solves part of the problem. Namely, it reduces the individual losses potentially borne by a failed (or even fraudulent) ICO. However, it does not generate any benefit from an aggregate or social-welfare perspective. Issuers can still take advantage of the asymmetries of information faced by consumers, and some fraudulent behavior can be committed. For this reason, we do not find this proposal entirely convincing. In the case of restricting the purchase of tokens to certain actors, for example, the situation might be different. In the context of individuals, we believe that regulators should not ban the purchase of tokens by individuals. Instead, they should invest resources in warning investors, through advertisement and education, about the risks of ICOs. Thus, the regulator would be able to preserve individuals' freedom to purchase tokens while minimizing the risks of being ripped off. For commercial banks and institutional investors, however, we do believe that some bans should be imposed. For this reason, certain limitations for these special market participants will be imposed in our proposal to deal with ICOs, discussed in section 2 below.

### 1.3. *Security Token Registration*

Many jurisdictions around the world, including the United States, Switzerland, and Singapore, subject the issuance of security tokens to general securities laws. Therefore, if a token is not classified as a security, the issuance of tokens will be exclusively governed by the law of contract. By contrast, if the token is deemed to be a security, the issuance of tokens will be subject to securities law. Therefore, it will be subject to the general rules governing the preparation and registration of prospectus, as well as the supervision of the securities regulator. Likewise, if certain requirements

---

<sup>80</sup> See <http://bitcoinist.com/russia-unveils-ico-regulations-ruble/>

<sup>81</sup> See <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams>

are met, the issuer might enjoy the exemptions generally provided by securities regulators to certain issuances of securities.<sup>82</sup> Therefore, even though it will be subject to the oversight of the securities regulator, it may be waived from the costly procedures generally associated with the preparation and registration of prospectus.

In our opinion, this model has various advantages. First, it provides a level playing field by not discriminating among functionally similar products. Therefore, regardless of their legal form, products with similar features and functions will be subject to the same rules of the game. Second, by subjecting the issuance of security tokens to securities regulation, the regulator will provide a greater level of protection to the purchasers of security tokens. Finally, the lack of regulation of non-security tokens may reduce the regulatory burden of some tokens that, due to their particular features, might not need the same level of protection existing in security tokens. Therefore, by reducing the regulatory costs associated with the issuance of these tokens, regulators may facilitate fundraising to many ventures that may have trouble getting access to other sources of finance.

Despite the general benefits associated with this regulatory model, we do not find it entirely convincing. On the one hand, it is not clear whether the general framework existing in securities law will be enough to protect security tokenholders. Indeed, even though, from a functional perspective, some tokens can look like securities, the issuance of tokens presents other particular features that cannot be found in other types of securities. First, unlike what happens with shareholders, tokenholders are not protected by corporate law. Second, in the context of ICOs, there is no market for corporate control to discipline managers. That is, the promoter of the ICO cannot be subject to any hostile takeovers and ultimately be removed from its position. Therefore, the potential situation of opportunism of issuers vis-à-vis investors will be higher in the context of ICOs, since the promoter will unlikely face the risk of being removed for a poor governance or performance, as it may happen in equity markets. Third, while equity markets can be relatively efficient, in the sense that they reflect all publicly available information, the same cannot be applied to market of tokens. In these latter markets, the lack of a deep secondary market (or even the existence of a secondary market) as well the smaller number of analysts and investors will make very unlikely that the price of a token reflects all publicly available information. As a result, tokenholders will find it more difficult to know the intrinsic value of their assets, and this lack of information may distort their ability to make wise financial decision. Fourth, tokenholders probably face more asymmetries of information than a regular

---

<sup>82</sup> For a general view of exemptions, see John Armour *et al*, PRINCIPLES OF FINANCIAL REGULATION (Oxford University Press, 2016), pp. 167-173. For a US perspective, see John Coffee, Jr. and Hillary A. Sale, SECURITIES REGULATION: CASES AND MATERIALS (Foundation Press, 12<sup>th</sup> Edition, 2012), 328-407. In the European Union, see the Regulation No 2017/1129 of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market. This regulation repealed the Directive 2003/71/EC which governed the offer of securities in the European Union since 2005. In Singapore, an offer may be exempt from the Prospectus Requirements where, amongst others, the offer is a small offer of securities of an entity, or units in a CIS, that does not exceed S\$5 million (or its equivalent in a foreign currency) within any 12-month period, subject to certain conditions; the offer is a private placement offer made to no more than 50 persons within any 12-month period, subject to certain conditions; the offer is made to institutional investors only; or the offer is made to accredited investors, subject to certain conditions. See Monetary Authority of Singapore, *A guide to digital token offerings* (2018), pp. 5-6. Similar requirements apply in other jurisdictions.

shareholder in a public company. This is due not only to the complexity of the white project or the project behind the ICO, but more importantly to the inability of the market to project retail investors, as it has been mentioned in above. Finally, the cryptocurrency world seems to be involved in a 'hype' that may exacerbate the ability of many tokenholders to make thoughtful decisions. Therefore, the risk of making wrong the decisions will be higher in the context of ICOs. As a result, perhaps the general rules governing securities law might not be enough to protect investors, and some further steps should be taken by the regulators.

On the other hand, even if it were assumed that the regulatory approach existing in jurisdictions like the United States, Switzerland and Singapore provides a reasonable level of protection to security tokenholders, there are still two additional regulatory challenges to be addressed: (i) the protection of non-security tokenholders; and (ii) making sure that all security tokens comply with securities laws.

In our opinion, these jurisdictions fail to protect non-security tokens. Indeed, while many steps have been taken to protect security tokenholders, regulators have not seriously thought about the protection of non-security tokenholders. This lack of protection is probably due to the fact that most of the discussion of ICOs has been generated in the capital market space, and the protection of non-security tokens probably exceeds the scope of securities regulators. Therefore, perhaps this discussion should be led by other regulatory authorities. Likewise, we also believe that the regulatory model existing in these countries fail to avoid the problem associated with not subjecting security tokens to securities regulation. On the one hand, the issuer may have perverse incentives to avoid the regulatory burden associated with securities regulation. For this reason, it may classify its tokens as non-security tokens even when they meet all the requirements to be classified as securities. In our opinion, even though this problem will be reduced in countries with an active enforcement department and severe sanctions imposed to those issuers failing to comply with securities laws, the deterrence effect created by getting caught and sanctioned might not be enough to prevent misbehavior – especially in a sector where more than 80% of the issuances are scams. Moreover, even if the issuer is caught, it will be difficult to repair the damage to both investors and the market as a whole.

In addition, there will be circumstances in which it is not clear whether a particular token should be classified as a security, as shown in the United States by cases such as *SEC v Howey*, *Munchee*, or *Reves v Ernst & Young*.<sup>83</sup> Moreover, many issuers might fail to comply with existing securities law even in good faith.

---

<sup>83</sup> These cases were decided in the United States. For the concept of "security" in the United States, see John Coffee, Jr. and Hillary A. Sale, *SECURITIES REGULATION: CASES AND MATERIALS* (Foundation Press, 12<sup>th</sup> Edition, 2012), 246-327; Hal S. Scott and Anna Gerlpern, *INTERNATIONAL FINANCE: TRANSACTIONS, POLICY AND REGULATION* (Foundation Press, 21<sup>st</sup> edition, 2016). For a comparison between the United States and Europe, see Philipp Hacker and Dr. Chris Thomale, *Crypto-securities regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, 17-36. For the concept of security in Singapore, for example, see Hans Tjio, Wan Wai Yee, and Yee Know Hon, *PRINCIPLES AND PRACTICE OF SECURITIES REGULATIONS IN SINGAPORE* (LexisNexis, 3<sup>rd</sup> Edition, 2017). For an analysis of the concept of securities in the United Kingdom, Australia, South Africa and India, see Frederick H. C. Mazando, *The Taxonomy of Global Securities: is the U. S. Definition of a Security too Broad?* NORTHWESTERN JOURNAL OF INTERNATIONAL LAW & BUSINESS 121, 148-176.

In our opinion, the regulatory model existing in the United States, Switzerland, and Singapore makes it particularly difficult to investigate an ICO if the promoter has not submitted any files or prospectus to the securities regulators. In these situations, the securities regulators will likely hear about the ICO from others, sometimes when something bad has already happened. For this reason, we believe that a system of *ex ante* control might be needed in these countries. Namely, it will be proposed in section 2 that any issuance of tokens, no matter whether they are security tokens or non-security tokens, should be *disclosed* to the security regulators or any other public regulatory agency. Thus, by making it easier to the regulator to facilitate the investigation of all issuance of tokens, issuers will think twice how to classify their tokens and, if so, whether complying with securities regulation.

#### 1.4. *Comprehensive Token Registration*

Other countries, such as Mexico, have opted for imposing a system of full control *ex ante* over all issuances of tokens.<sup>84</sup> According to this approach, any issuance of tokens should be registered and authorized by the regulator.<sup>85</sup> Then, depending of the type of tokens, existing securities laws may apply or not. Thus while a security token will be subject to the full gamut of disclosure and procedural requirements and obligations existing in securities law, the regulatory burden for an issuance of non-security tokens will be notably reduced.<sup>86</sup>

The Mexican solution solves the problem associated with not having control over the issuance of non-security tokens, or even security tokens not registered before the securities regulator. Therefore, it may fix part of the flaws of the regulatory model existing in the United States, Switzerland and Singapore. Nevertheless, the solution adopted by Mexico is far from perfect. Among other aspects, it imposes more costs for issuers and regulators. From the perspective of the issuers, the issuance of tokens will probably involve more time and money. From the perspective of the regulator, this model would require more people to be trained and hired to monitor, analyze, classify and approve the issuance of tokens. Therefore, it will be costlier. And while this investment in hiring and training people to deal with ICOs may be valuable in some cases, there will be many situations in which it is not worth it (e.g., when a token consists of just a redeemable voucher in a company). As a result, even though the Mexican approach solves part of the problems existing in other regulatory models, it creates other costs. For this reason, it does not sound entirely convincing either.

## 2. **Toward a safe but efficient system to deal with ICOs**

As it has been mentioned previously, all the existing regulatory models to deal with ICOs present some flaws. For this reason, we propose a new model that, while

---

<sup>84</sup> However, Mexico's Fintech law only mentions "digital assets". It does not refer to ICOs or tokens. Nonetheless, "digital assets" is broader enough to consider tokens and ICOs subject to Mexican Fintech law according to our interpretation.

<sup>85</sup> Interestingly, in Mexico, the issuance of tokens does not have to be authorized by the securities regulator but by the Central Bank.

<sup>86</sup> It is not clear how the Mexican approach will operate in practice. While writing this article, Mexico has just enacted a Fintech Law saying that any issuance of "cryptocurrencies" will be subject to the authorization of the regulator.

protecting tokenholders, market integrity, market supervision, and the stability of the financial system, can still facilitate the use of ICOs as an affordable method to raise finance. Our proposal is built on four core pillars.

First, all issuance of tokens, no matter whether they are security or non-security tokens, should be disclosed to the regulator. The way to do so may consist of requiring issuers to submit a simple, harmonized *electronic form* to the securities regulator or any other public authority.<sup>87</sup> This electronic form should contain some basic information about the issuance. This basic information may include the promoter's location, problem and proposed technology solution, description of the token, blockchain governance, qualifications of the technical team, and risk factors.<sup>88</sup> Likewise, we also believe that the form should include other factors potentially relevant for the purchasers of tokens, including identity of the promoters, legal advisors, accounting and finance aspects of the ICO, and any legal or contractual provisions available to protect tokenholders.

By submitting this electronic form, not only the regulator will be in a better position to monitor any issuance of tokens, but it will also be easier for analysts and investors to compare ICOs since issuers will be required to provide a minimum level of standardized information. Therefore, this comparability could serve as an additional tool to protect tokenholders, while facilitating to the regulatory authorities the analysis of the information provided by the ICO's promoter. As a result, this higher scrutiny will incentivize promoters to behave in a more honest and diligent manner, since this regulatory model will make easier for regulators to investigate and, if so, sanction any fraudulent ICOs, as well as those issuances of securities tokens –sometimes publicized as non-security tokens– failing to comply with securities laws.

Second, as non-security tokenholders are not protected under securities law, we believe that several strategies should be implemented to protect these purchasers. Namely, we argue that regulators should protect non-security tokenholders by implementing some regulatory strategies existing to protect consumers and financial consumers. As it will be discussed in section V, these strategies will include cooling off periods, the prohibition of certain terms and products, the imposition of conduct obligations on the issuer, and the use of certain litigation rules to favor the non-security tokenholder in case of a potential lawsuit.

Third, being involved in a pre-sale of tokens is even riskier than participating in other types of ICOs since the tokenholder will be entitled to something that does not exist yet – and based on the number of scams, it seems quite probable that it might not exist ever. Therefore, we believe that *commercial banks* and *pension funds* should not be allowed to purchase these tokens since they invest money from the general public and

---

<sup>87</sup> Moreover, companies required to prepare and submit financial statements should be required to mention any issuance of tokens in the notes to the financial statements.

<sup>88</sup> This basic information has been suggested for white papers. See Chris Brummer, *What should be in an ICO white paper?* (available at <https://cointelegraph.com/news/what-should-be-in-an-ico-white-paper-expert-take>). For a deeper analysis, see Chris Brummer, Trevor Kiviat, and Jai R. Massari, *What Should Be Disclosed in an Initial Coin Offering?* (2018) (available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3293311](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3293311)).

their potential failure could have severe consequences for the stability of the financial system.<sup>89</sup> Therefore, they should not engage in this type of risky activities.

Fourth, several factors make the purchase of tokens particularly risky, including the high probability of scams, the lack of effective devices to protect tokenholders, the larger asymmetries of information between founders and tokenholders, and the high risk of irrational behavior that might take place in the crypto markets.<sup>90</sup> For this reason, we believe that the regulator should spend more resources and efforts in warning *retail tokenholders* about the risks associated with the purchase of tokens.

### III. Accounting and finance aspects of ICOs

Another critical aspect raised by the issuance of tokens concerns the accounting and finance aspects of ICOs. In other methods to raise capital, it seems relatively clear, from an accounting and finance perspective, what a company gives to investors, and what the issuer receives in return. For example, in an IPO, a company gives shares (equity) to public investors, and it receives cash in return. In a debenture, a company gives bonds (debt) in exchange for cash. Moreover, in this type of transactions, the way the company's counterparty is classified from an accounting and finance perspective is also relatively clear. In an issuance of shares, the company's counterparties are equityholders. Therefore, they will be part of the company's net assets (or equity) within the balance-sheet. In an issuance of bonds, the company's counterparties are debtholders. Hence, they will be part of the company's liabilities.

Table 2. Registration of tokens from an accounting's perspective

Issuer's balance-sheet	
Cryptocurrencies (assets)	Tokens (Debt/Equity)

  

Tokenholder's balance-sheet	
Tokens (assets)	Cryptocurrencies (assets)

The classification of the company's counterparty from an accounting and finance perspective may have different implications. For example, it may affect the company's governance and cost of capital, and more importantly from a legal perspective, the

<sup>89</sup> Due to the size and the particular features of these institutions, their failure may generate various negative externalities, including lack of confidence, contagion, connectedness and more generally systemic risk. For an analysis of these concepts, see Hal Scott Hal S. Scott, *CONNECTEDNESS AND CONTAGION: PROTECTING THE FINANCIAL SYSTEM FROM PANICS* (MIT Press, 2016); Steven L. Schwarcz, *Systemic Risk*, 97 *GEORGETOWN LAW JOURNAL* 193 (2008); Viral Acharya, *A theory of systemic risk and design of prudential bank regulation*, 6 *JOURNAL OF FINANCIAL STABILITY* 224 (2009). For an analysis of the importance of pension funds and other institutional investors in capital markets, see Ronald J. Gilson and Jeffrey N. Gordon, *The Agency Costs of Agency Capitalism: Activist Investors and The Revaluation of Governance Rights*, 863 *COLUMBIA LAW REVIEW* 928 (2013).

<sup>90</sup> See Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016), pp. 26-28.

company's financial ratios and covenants.<sup>91</sup> Indeed, since some of the contractual terms potentially agreed between issuers and lenders may specify that the company should maintain certain debt/equity ratios, or even certain levels of current versus non-current liabilities, the classification of an issuance of tokens as debt or equity, or as current liabilities or non-current liabilities, may ultimately affect the company's existing loan agreements. Therefore, it seems particularly relevant to analyze the anatomy of an ICO from an accounting and finance perspective.

As it has been mentioned in previous sections, a promoter issues tokens and it receives *cryptocurrencies* in return. Therefore, since the cryptocurrencies will represent a right for the company, they will be registered as an *asset* in the company's balance-sheet. As a general rule, they will represent a current asset, due to the ability of most cryptocurrencies to be converted into cash in a short period of time.

More problems arise when we analyze the registration of the issuance of tokens. In this case, the *tokens* issued by the company can be classified as equity or debt. In our opinion, this classification will depend on the features of the tokens. When the white paper gives tokenholders economic and political rights similar to those held by shareholders, the tokenholders should be classified, at least from an accounting and finance perspective, as *equityholders*. Therefore, the issuance of tokens will be registered in the company's net assets (equity). By contrast, in those cases in which the features of the token seem to reflect that the tokenholders will be entitled to future services or fixed payments, those tokenholders should be classified as *debtholders*. Therefore, they will be part of the company's liabilities. And depending on the maturity of those rights held by tokenholders, the issuance of tokens will be registered as non-current liabilities (if the maturity is more than a year) or current liabilities (if the maturity is less or equal than a year).

From the perspective of the tokenholder, the registration of tokens seems a bit clearer. Since tokenholders give cryptocurrencies to the issuer in exchange for acquiring the promoter's tokens, those cryptocurrencies should be registered as a decrease in the tokenholder's assets. Simultaneously, as the tokenholder receives some rights (tokens) in return for the cryptocurrencies, these rights will increase the tokenholder's assets.

Another critical aspect of ICOs from an accounting and finance perspective involves the valuation and, if so, the impairment of value experienced by the cryptocurrencies

---

<sup>91</sup> For a pioneer study about the impact of the capital structure on the value of the firm, see Franco Modigliani and Merton Miller, *The Cost of Capital, Corporation Finance and The Theory of Investment*, 48 THE AMERICAN ECONOMIC REVIEW 261 (1958). These authors establish that the value of the firm was independent of the capital structure. However, they make this assertion in a world without asymmetries of information, transaction costs, taxes, and costs of bankruptcy. Once these variables are included in the model, the use of debt seems to generate more benefits for firms. See Michael C. Jensen, *Agency Cost Of Free Cash Flow, Corporate Finance, and Takeovers*, 76 AMERICAN ECONOMIC REVIEW 323 (1986); Richard Brealey, Steward Myers, and Franklin Allen, PRINCIPLES OF CORPORATE FINANCE (McGraw-Hill, 10<sup>th</sup> Edition, 2011), pp. 460-462; Aurelio Gurrea-Martinez, *The Impact of the Tax Benefits of Debt in the Capital Structure of Firms and the Stability of the Financial Systems*, OXFORD BUSINESS LAW BLOG, March 2017. For a general analysis of the capital structure of firms from a legal and finance perspective, see Elis Ferran and Look Chan Ho, PRINCIPLES OF CORPORATE FINANCE LAW (Cambridge University Press, 2<sup>nd</sup> Edition, 2014).

held in the issuer's balance-sheet. This aspect becomes particularly problematic in the context of cryptocurrencies due to their volatility.<sup>92</sup> Moreover, if, as some authors have pointed out,<sup>93</sup> there is a bubble in some cryptocurrencies' markets, and this bubble bursts, the issuer will have to register significant losses in their balance-sheet. Therefore, from an accounting perspective, the valuation and impairment of these assets can be particularly relevant not only for the company's financial statements but also for a variety of legal issues. These legal issues may from existing covenants, to distribution of dividends, or –in some jurisdictions– even the duties and liability of directors if the company's net assets fall below a certain amount of the company's legal capital.<sup>94</sup>

Likewise, from the perspective of the *tokenholder*, the fact that many projects fail may force them to register a loss in their assets. Therefore, taking into account that volume and value of ICOs are becoming more and more important, we believe that regulators should pay special attention to the accounting and finance aspects of ICOs. Otherwise, we face the risk of observing something similar to what happened in the 2008 financial crisis: the unexpected registration of losses in many companies' balance-sheets may end up harming not only the financial situation of these firms and their investors but also –if the volume of tokens is large the enough, and the parties involved are financial institutions– the stability of the financial system.<sup>95</sup>

#### IV. Corporate governance issues

##### 1. The concept and nature of tokenholders

The classification of a tokenholder will mainly depend on the nature, features and distribution of tokens. From a legal perspective, tokens can be classified as security or non-security tokens. Therefore, the purchasers of security tokens will be classified as 'security tokenholders', while the holders of non-security tokens will be considered 'non-security tokenholders'. From an accounting and finance perspective, however, the classification may seem more unclear. On the one hand, non-security tokenholders should generally be classified as debtholders, since they will probably be entitled to future products or services. On the other hand, *security tokenholders* can be classified as either equityholders or debtholders, depending on whether they are entitled to the company's ownership or future returns or just to a fixed return, respectively.

Table 3. Legal and finance classification of tokens

---

<sup>92</sup> The best example can be found in the bitcoin. For the evolution of its price, see <https://bitvol.info/>

<sup>93</sup> These authors include some Nobel Prizes in Economics such as Professor Robert Shiller: <https://qz.com/1067557/robert-shiller-wrote-the-book-on-bubbles-he-says-the-best-example-right-now-is-bitcoin/>

<sup>94</sup> See Luca Enriques and Jonathan Macey, *Creditors Versos Capital Formation: The Case Against The European Legal Capital Rules*, 86 CORNELL LAW REVIEW 1165 (2001); Aurelio Gurrea-Martínez, Aurelio Gurrea-Martínez, *The Impact of the Tax Benefits of Debt in the Capital Structure of Firms and the Stability of the Financial Systems*, OXFORD BUSINESS LAW BLOG, March 2017.

<sup>95</sup> This situation would create a problem of correlation and connectedness. For an analysis of these concepts, see Hal S. Scott, *CONNECTEDNESS AND CONTAGION: PROTECTING THE FINANCIAL SYSTEM FROM PANICS* (MIT Press, 2016).

Legal classification	Finance classification
<b>Security tokenholder</b>	<b>Debtholder/equityholder</b>
<i>Equity-based securities</i>	Equityholders
<i>Debt-based securities</i>	Debtholders
<b>Non-security tokenholder</b>	<b>Debtholder</b>

The fact that a security tokenholder (legal classification) is an equityholder (finance classification) does not mean that these tokenholders should be considered “shareholders”, even if they have similar rights. Indeed, in our opinion, unless a particular jurisdiction allows classifying as shares some particular financial products that look like shares but they do not represent a fraction of a company’s legal capital, a tokenholder should never be considered a shareholder.<sup>96</sup> We do not believe so for several reasons. First, it is not clear what a shareholder is exactly entitled to. Indeed, while there are some general rights usually held by shareholders (e.g., rights to the company’s future returns, rights to the company’s residual assets, right to call the shareholders’ meeting, right to sue the managers for a breach of fiduciary duties, etc.), the use of preferred shares or dual-class shares structure show that many shareholders can be considered as such without having some rights generally associated with the condition of shareholders (e.g., vote). Therefore, while there are some indicia that may help us identify what a shareholder looks like, it is not always clear.

Second, and perhaps more importantly, even though financial markets and institutions should be analyzed from a functional approach with particular focus on the economic substance rather than its legal form, this functional analysis does not mean that different legal institutions should be considered similar entities but instead that they should be subject to similar regulations. For example, in our opinion, even if investment banks and commercial banks were performing similar functions, they should not be considered similar legal entities. Nevertheless, they should be subject to similar regulations. Therefore, a functional approach to financial regulation should not be interpreted as understanding different institutions as equal legal entities but treating functionally equivalent institutions similarly. Therefore, in this context, even though a shareholder should be distinguished from equity tokenholders entitled to similar rights, they both should be subject to a similar treatment. Hence, they both should be part of the company’s equity or they both should be subordinated in bankruptcy.

---

<sup>96</sup> Our opinion seems to differ here from the Monetary Authority of Singapore. See Monetary Authority of Singapore, *A Guide to Digital Token Offerings* (2018), p. 3 allowing tokens to be considered “shares” when it confers or represents ownership interest in a corporation, represents liability of the token holder in the corporation, and represents mutual covenants with other token holders in the corporation *inter se*. However, in Singapore, the law seems to distinguish between “stocks” and “shares” – this latter concept seems to be broader. See section 2(1) of the SFA, read with section 4(1) of the Companies Act (Cap. 50), expressing that “share” means “a share in the share capital of a corporation and includes stock except where a distinction between stocks and share is expressed or implied”. See also Ricardo Torres, *Problemática jurídica de las ICOs: Un análisis desde el Derecho de sociedades*, BLOG DEL INSTITUTO IBEROAMERICANO DE DERECHO Y FINANZAS, 20 March 2018 (available at <http://derechoyfinanzas.org/blog/problematika-juridica-de-las-icos-un-analisis-desde-el-derecho-de-sociedades/>).

Third, in some countries, existing shareholders have preemption rights with the purpose of avoiding dilution when a company raises capital. Therefore, if a court or regulator interprets *ex post* that a tokenholder should be considered as a shareholder, existing shareholders can lose a right that, regardless of its desirability, the legislator wants them to have. Therefore, even though the legislator can solve this problem by requiring shareholder vote for any issuance of tokens, this solution might not seem the most desirable one for a fundraising method that was probably, among other aspects, to save transaction costs. Moreover, even in the absence of transactions costs, if old shareholders really want to make tokenholders new shareholders, it may seem more consistent –and more desirable to promote legal certainty for both shareholders and tokenholders– to issue shares rather than tokens.

Finally, the classification of equitytokenholders as shareholders may also make unclear the beneficiaries of managers' fiduciary duties. In other words, it may make even more unclear to whom the managers owe fiduciary duties, and what types of legal rights can be exercised –and by who– in the case of a breach of fiduciary duties. Therefore, this interpretation may not may crease legal uncertainty but it can also reduce the accountability of the board of directors.

For these reasons, we believe that, even when tokenholder have similar rights than those generally held by shareholders, they will just be considered *equityholders* from an accounting and finance perspective, or *security tokenholders* from a legal perspective, but never 'shareholders'. A different conclusion not only would create legal uncertainty but it would also be inconsistent with the proper application of the functional approach that should prevail in financial regulation. In any case, if, under a particular jurisdiction, financial products similar to shares can be classified as such, and the issuance of shares requires approval by the shareholders' meeting, we would suggest that the issuance of security tokens should be approved by the shareholders' meeting, just in case a court eventually finds that those tokens should be classified as shares, and therefore shareholders' rights can be affected.

## **2. Protecting tokenholders from the promoter's opportunism**

### *2.1. Agency problems in a world of tokenholders*

While the use of ICOs may serve as a new method to allow individuals and firms to raise capital and therefore be able to develop their projects and ideas, the evidence suggests that more than 80% of ICOs are scams.<sup>97</sup> Therefore, the purchase of tokens should be considered a risky activity since the tokenholder is highly exposed to the opportunism of the promoter. In some cases, the promoter might not even pursue the promised projects.<sup>98</sup> In others, the promoters may just waste tokenholders' money when pursuing its goals. In both cases, there is a type of agency problem, or a higher risk of opportunism, that should be addressed.

---

<sup>97</sup> Some authors even speak about "Initial Coin Scams". See <https://www.project-syndicate.org/commentary/ico-cryptocurrency-scams-by-nouriel-roubini-2018-05>

<sup>98</sup> Corporate governance is, after all, about promises between managers and investors. See Jonathan Macey, *CORPORATE GOVERNANCE: PROMISES KEPT, PROMISES BROKEN* (Princeton University Press, 2008).

This higher risk of opportunism of promoters vis-à-vis tokenholders derives from several factors. First, tokenholders do not usually have the ability to appoint, remove and remunerate the directors. Therefore, unlike what happens when the suppliers of funds are shareholders entitled to vote, the managers might not have enough incentives to maximize the interests of the tokenholders, since their jobs will not be at risk. Second, white papers may not cover how managers should behave in many cases in which the interests of the tokenholders may be at stake. Moreover, unlike what happens in a typical relationship between directors and shareholders where fiduciary duties may help fill some gaps<sup>99</sup>, promoters do not usually owe fiduciary duties to tokenholders. Therefore, white papers may become more incomplete than a typical corporate contract. Besides, even if they were able to fill these gaps, it is not clear how (if so) the rights potentially provided to the tokenholders in the white paper will be enforced. Third, while managers in listed companies are subject to public scrutiny and a market for corporate control that may encourage them to maximize the value of the firm for the interests of the shareholders,<sup>100</sup> these market forces will unlikely exist in a private company issuing tokens. Fourth, unlike shareholders, tokenholders are not protected by a country's company laws. In fact, non-security tokenholders do not even get the protection of securities law. Fifth and therefore due to the lower disclosure requirements imposed to promoters and the complexity behind many ICOs, there might be more asymmetries of information between issuers and tokenholders. Sixth, there seems to be a type of market euphoria in the crypto-assets market that may increase the level of irrational decisions made when purchasing tokens.<sup>101</sup> Therefore, all of these factors expose tokenholders to a higher risk of opportunism by promoters.

Several strategies can be implemented to reduce agency problems between promoters and tokenholders. First, managers can be required to buy a certain percentage of tokens. By doing so, they would have more skin in the game, and therefore they would be incentivized to make wiser investment decisions. Otherwise, they might end up losing as much as the tokenholders.

Second, tokenholders may be empowered with some political rights. For instance, they can be allowed to appoint and remove the directors, or even to have a vote on some relevant decisions. Thus, the managers would have more incentives to maximize the interests of the tokenholders. Otherwise, the tokenholders could easily remove the managers.

---

<sup>99</sup> A corporate contract is, by definition, an incomplete contract. The parties cannot agree *ex ante* on any single contingencies. For these reasons, fiduciary duties and other general provisions may help fill some of the gaps existing in corporate contracts. For an analysis of the literature about incomplete contracts in the context of the firm and a firm's capital structures, see Oliver Hart, *FIRMS, CONTRACTS, AND FINANCIAL STRUCTURE* (Oxford University Press, 1995); Oliver Hart and John Moore, *Property Rights and the Nature of the Firm*, 98 *JOURNAL OF POLITICAL ECONOMY* 1119 (1990); Oliver Hart and John Moore, *Foundations of Incomplete Contracts*, 66 *THE REVIEW OF ECONOMIC STUDIES* 115 (1999); Philippe Aghion and Patrick Bolton, *An Incomplete Contracts Approach to Financial Contracting* 59 *THE REVIEW OF ECONOMIC STUDIES* 473 (1992).

<sup>100</sup> See Henry G. Manne, *Mergers and the Market for Corporate Control*, 73 *THE JOURNAL OF POLITICAL ECONOMY* 110 (1965); Frank H. Easterbook and Daniel R. Fischel, *The Proper Role of the Target's Management in Responding to a Tender Offer*, 94 *HARVARD LAW REVIEW* 1161 (1981).

<sup>101</sup> Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016), pp. 26-28.

Third, some market mechanisms can be promoted to protect tokenholders. One of them can be the use of platforms to assess issuers and projects, as well as the use of intermediaries in the token industry. Another market device may consist of the development of secondary markets for tokens. Thus, tokenholders will be protected through the use of an easy exit right –which may lead in return to “price” founders’ behavior.

Nevertheless, while these mechanisms may reduce managerial agency problems,<sup>102</sup> they may generate other issues. First, while the fact of requiring insiders to hold a certain percentages of tokens would align the interests of managers and tokenholders, promoters might not have resources to buy enough tokens as to credibly have skin in the game. In fact, that is why they may decide to launch an ICO rather than funding the project by themselves. And even if the promoter were able to keep some tokens for free, this measure would not work either. On the one hand, if the promoter has not paid for those tokens, it would not have enough skin in the game. On the other hand, keeping tokens by founders and/or insiders would generate an opportunity cost, since the more tokens insiders keep, the less cryptocurrencies (and therefore funding) they will be able to raise. Thus, this measure may end up harming the firms’ ability to raise finance.

Second, while empowering tokenholders may align the interests of managers and tokenholders, this solution may also generate several problems. On the one hand, this power given to tokenholders may increase “principal costs”, that is, the costs associated with letting investors decide.<sup>103</sup> Moreover, these principal costs can be higher in the context of ICOs, since the fact of making business decisions about technical projects may require more expertise than for other businesses. On the other hand, if the white paper confers significant power to the tokenholders, and they have the ability to decide some relevant business decisions, tokenholders may face the risk of being considered as *de facto* directors.<sup>104</sup> And if so, they may end up being liable for some damages. Therefore, tokenholders’ rights should be designed in a manner that help reduce managerial opportunism without increasing principal costs or putting tokenholders at risk. Finally, empowering tokenholders will make the managers more accountable to them at the expense of the shareholders. And if so, a type of agency problem among the different suppliers of finance may exist due to their potentially

---

<sup>102</sup> Michael C. Jensen and William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 JOURNAL OF FINANCIAL ECONOMICS 305 (1976).

<sup>103</sup> For a novel explanation of principal costs, and how corporate governance should reduce both agency costs and principal costs, see Zohar Goshen and Richard Squire, *Principal Costs: A New Theory for Corporate Law and Governance*, 117 COLUMBIA LAW REVIEW 767 (2017). Providing various arguments to empower the board, see Stephen M. Bainbridge, *Director Primacy: The Means and Ends of Corporate Governance*, 97 NORWESTERN UNIVERSITY LAW REVIEW 547, 573 (2003). See also Martin Lipton, *Takeover Bids in the Target’s Boardroom*, 35 BUSINESS LAWYER 101 (1979) and Martijn Cremers and Simone M. Sepe, *The Shareholder Value of Empowered Boards*, 68 STANFORD LAW REVIEW 67 (2016). In favor of empowering investors, however, see Lucian A. Bebchuk, *The Case for Increasing Shareholder Power*, 118 HARVARD LAW REVIEW 833 (2005); Aurelio Gurrea Martínez, *New Agency Problems: New Legal Rules? Rethinking Takeover Regulation in the US and Europe*, INSTITUTO IBEROAMERICANO DE DERECHO Y FINANZAS, WORKING PAPER SERIES 3/2016.

<sup>104</sup> For an analysis of this concept, see Roy Goode, *PRINCIPLES OF CORPORATE INSOLVENCY LAW* (Sweet & Maxwell, 4<sup>th</sup> Edition, 2011), pp. 641-647.

different preferences in terms of risks and returns.<sup>105</sup> For example, while the shareholders, due to their limited liability, variable returns and diversified portfolios, are usually more inclined to take risks, creditors usually prefer a less risky business strategy. This divergence of interests can be also found between shareholders and tokenholders and even among tokenholders. For instance, if the returns of a group of powerful tokenholders depend exclusively on a single investment project, they may force the managers to invest more time and resources in this project, even if that is not the most desirable strategy for other stakeholders or even the company as a whole. Therefore, a type of 'horizontal agency' problem can be created since the managers would be maximizing the interests of a group of investors at the expense of others.<sup>106</sup>

## 2.2. Legal strategies to protect tokenholders

One of the primary concerns existing in the ICO markets comes from the lack of effective tools to protect tokenholders. On the one hand, security tokenholders enjoy a type of protection, such as securities law, that might not enough or even adequate for them due to several reasons, including the lack of an effective market for corporate control to discipline promoters, the higher asymmetries of information probably faced by tokenholders, or the more pronounced irrational behavior that may exist in the crypto market. Moreover, in many circumstances, the purchasers of security tokens might not even enjoy the protection provided by securities laws, since many promoters might not even register their issuance of tokens alleging that they are issuing non-security tokens. On the other hand, non-security tokenholders are just protected by a private document, such as the white paper, whose ability to be enforced is not even clear. Therefore, it should be a priority for the regulator to implement new legal tools to protect tokenholders.

### 2.2.1. Protecting security tokenholders

Security tokenholders are currently protected by two primary mechanisms: (i) the apparatus provided by securities law, which include disclosure obligations, procedural rules, supervision by the securities regulator, and a market of securities lawyers monitoring whether companies are complying with securities laws to otherwise sue them on behalf of investors; and (ii) the white paper. Nevertheless, as it has been mentioned, the white paper does not provide an effective tool to protect tokenholders since, due to the absence of mandatory disclosure for white papers, the promotor may just establish and disclose whatever it can be in its interest. Likewise, current securities law might not be enough, or even appropriate, to protect tokenholders. For this reason, we believe that securities regulators should implement a new legal strategy to protect security tokenholders. This strategy, as mentioned in section II, should consist on requiring promoters to submit an *electronic form* to the security regulator or any other

---

<sup>105</sup> For an analysis of these conflicts among shareholders, see John Armour, Henry Hansmann, and Reinier Kraakman, Agency Problems and Legal Strategies, in John Armour, Luca Enriques *et al*, THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH (Oxford University Press, 2017), pp. 29-30; Mark J. Roe, *The Institutions of Corporate Governance*, in Claude Ménard and Mary M. Shirley (eds.), HANDBOOK OF NEW INSTITUTIONAL ECONOMICS (Kluwer, 2005).

<sup>106</sup> For the concept of 'horizontal agency problems' in corporate governance, see Mark J. Roe, *The Institutions of Corporate Governance*, in Claude Ménard and Mary M. Shirley (eds.), HANDBOOK OF NEW INSTITUTIONAL ECONOMICS (Springer, 2005), pp. 371–377.

public authority disclosing certain information particularly relevant for the protection of tokenholders. The information provided in this electronic form may include the promoter's location, problem and proposed technology solution, description of the token, blockchain governance, qualifications of the technical team, risk factors, identity of the promoters, legal advisors, accounting and finance aspects of the ICO, and legal or contractual provisions available to protect tokenholders (if any). Moreover, the information provided in the electronic form should be based on a system of smart disclosure, in which more attention will be paid to the type of information provided in the form, as well as the way issuers provide this information, rather than the amount of information itself.

### 2.2.2. Protecting non-security tokenholders

In addition to the protection provided by the electronic form imposed to any issuance of tokens, we think that other legal devices should be implemented to protect non-security tokenholders. After all, they are not protected by securities laws, as it may happen with security tokenholders. In our opinion, these legal devices to protect tokenholders can be inspired on those generally used to protect *consumers* and more especially *financial consumers*.

First, regulators may impose *cooling off periods* on any issuance of non-security tokens. Thus, non-security tokenholders will be able to return the token within a given period of time without bearing any cost. This measure not only will protect non-security tokenholders *ex post*, but it will also encourage many issuers to think twice what they are going to sell.

Second, policy-makers may also opt for *regulating products*. Through this mechanism, the regulator may think of prohibiting certain terms particularly obscure or even tokens.

Third, as it has been developed in the context of financial consumers after the failure of some of the previous strategies, regulators may also decide to impose *conduct obligations* on the issuer. Namely, it may require issuers to take into account the interest of tokenholders, avoiding situations in which the issuer seeks to exploit non-security tokenholders' biases and mistakes.

Finally, an additional tool to protect non-security tokenholders may consist on using *litigation rules*. For instance, the legislator may establish that any unclear provision established in the white paper should be interpreted in favor of non-security tokenholders. By doing that, not only non-security tokenholders will enjoy *ex post* a higher level of protection, but issuers will also have incentives to draft the clauses established in the white paper in a clearer and more protective way to favor the understanding of these clauses by tokenholders.<sup>107</sup>

---

<sup>107</sup> For a general view about the challenges faced by consumer when they make decisions and how regulators can improve consumer protection, see Oren Bar-Gill, *SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER MARKETS* (Oxford University Press 2012); and Omri Ban Shagar and Carl E. Schneider, *MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE* (Princeton University Press, 2014). Focusing on financial consumers, and different regulatory approaches to protect financial

### 2.3. Market devices to protect tokenholders

In addition to the legal and regulatory devices to protect security and non-security tokenholders, we believe that some market mechanisms may also reduce the agency problems existing between issuers and tokenholder. For example, the development of a liquid secondary market for tokens may provide a greater level of protection to tokenholders. Moreover, it would do so in several ways. First, a more liquid market for tokens would make easier for tokenholders to sell their tokens. Therefore, these 'exit rights' could serve as *ex post* mechanism to protect tokenholders.

Second, the existence of a liquid market may contribute to "price" the behavior of many projects and promoters. Namely, by observing whether tokenholders buy or sell shares, and therefore whether the price of a given token goes up or down, the market can infer the promoters' behavior. Therefore, promoters, or at least those interested in issuing future tokens, will have strong incentives to behave in an efficient and honest manner.

Third, if these markets are developed, there will be more platforms and analysts providing advice and 'grading' projects and promoters.<sup>108</sup> Nevertheless, while this market of intermediaries can generate several benefits for tokenholders, regulators should pay close attention to the potential conflicts of interests faced by these actors. Indeed, the lessons learnt in the past from auditors<sup>109</sup>, credit rating agencies<sup>110</sup> and proxy advisors<sup>111</sup> show that these "gatekeepers" can be subject to a variety of conflicts of interests. Therefore, regulators can use some of the regulatory strategies implemented for auditors, credit rating agencies and proxy advisors to deal with the problems associated with the rise of platforms and analysts in the ICO industry. These strategies may include disclosure obligations (especially when the analyst has been paid by the issuer for any other professional service), restrictions in the variety of professional services potentially provided by these analysts, as well as liability rules.

---

consumers, see John Armour *et al*, *PRINCIPLES OF FINANCIAL REGULATION* (Oxford University Press, 2016), pp. 205-223 and 255-271

<sup>108</sup> Some of these platforms already exist, as it can be the case of websites like "icoratings.com", "icoalert.com" and "icomonitor.io". See Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016), pp. 28.

<sup>109</sup> Arie Goldman and Benzion Barlev, *The Auditor-Firm Conflict of Interests: Its Implications for Independence*, 49 *THE ACCOUNTING REVIEW* 707 (1974); Matthew J. Barrett, *Enron and Andersen - What Went Wrong and Why Similar Audit Failures Could Happen Again*, in Nancy B. Rapoport and Bala G. Dharan (eds.), *ENRON: CORPORATE FIASCOS AND THEIR IMPLICATIONS* (Foundation Press 2004), pp. 155-168; Walter Doralt, Andreas Martin Fleckner, Klaus J. Hopt, Christoph Kumpan, Felix Steffek, Reinhard Zimmermann, Alexander Hellgardt, Susanne Augenhöfer, *Auditor Independence at the Crossroads – Regulation and Incentives*, 13 *EUROPEAN BUSINESS ORGANIZATION LAW REVIEW* 89 (2012).

<sup>110</sup> Frank Partnoy, *How and Why Credit Rating Agencies are Not Like Other Gatekeepers*, *Financial Gatekeepers: Can they protect investors?* San Diego Legal Studies Paper No. 07-46 (2006); Carol Ann Frost, *Credit Rating Agencies in Capital Markets: A Review of Research Evidence on Selected Criticisms of the Agencies*, 22 *JOURNAL OF ACCOUNTING, AUDITING AND FINANCE* 1 (2007).

<sup>111</sup> The conflicts of interest of proxy advisors have not been that evident. They were identified more recently. See Guy Rolnik, *The Powerful Private Regulator and the Effects of Conflicts of Interest*, ProMarket, May 3, 2017 (<https://promarket.org/powerful-private-regulator-effects-conflicts-interest/>); Tao Li, *Outsourcing Corporate Governance: Conflicts of Interest Within the Proxy Advisory Industry*, *MANAGEMENT SCIENCE* (2018); ESMA, *Discussion Paper An Overview of the Proxy Advisory Industry: Considerations on Possible Policy Options* (2012) (<https://www.esma.europa.eu/sites/default/files/library/2015/11/2012-212.pdf>)

## V. Anti-Money Laundering implications of ICOS

Tokens created on a blockchain are decentralized and encrypted, sometimes making it harder to track each of the transactions made, and the individuals behind them. Therefore, in theory, anyone with an internet connection and a digital wallet can be part of a token sale event. That can leave room for people to launder money or finance terrorism activities and engage in other fraudulent behaviors. Additionally, taking into account how easy it is to launch a token pre-sale, these mechanisms could be used in countries where illegal activities such as corruption are above average in order to move resources without oversight. Nonetheless, we could not find available data showing how much money is being laundered through ICOs.

Regulators in the United States and Singapore have been particularly active highlighting the risks of money laundering and frauds that investors face when buying tokens. Singapore's financial regulatory body and central bank, the Monetary Authority of Singapore ("MAS"), stated that: *"ICOs are vulnerable to money laundering and terrorist financing (ML/TF) risks due to the anonymous nature of the transactions, and the ease with which large sums of monies may be raised in a short period of time"*.<sup>112</sup> MAS' media release of 13 March 2014 had communicated that while virtual currencies per se were not regulated, intermediaries in virtual currencies would be regulated for ML/TF risks. MAS is currently assessing how to regulate ML/TF risks associated with activities involving digital tokens that do not function solely as virtual currency.<sup>113</sup>

For MAS, even digital tokens that perform functions which may not be within MAS' regulatory purview for not fitting into the legal category of securities, may nonetheless be subject to legislation for combating money laundering and terrorism financing. MAS highlights in particular the following: (i) obligations to report suspicious transactions with the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force, and (ii) prohibitions from dealing with or providing financial services to designated individuals and entities pursuant to the Terrorism (Suppression of Financing) Act and various regulations giving effect to United Nations Security Council Resolutions.

Moreover, issuers of tokens could be subject to licensing requirements under the Securities and Futures Act and the Financial Advisers Act. In addition, platforms facilitating secondary trading of such tokens would also have to be approved or recognized by MAS as an approved exchange or recognized market operator respectively. This regulatory authority also announced the drafting of a new payments services framework that will include rules to address money laundering and terrorism financing risks relating to the dealing or exchange of cryptocurrencies for fiat or other digital assets such as tokens. Such intermediaries will be required to put in place policies, procedures and controls to address such risks. These will include requirements to conduct customer due diligence, monitor transactions, perform screening, report suspicious transactions and keep adequate records.<sup>114</sup>

Along the same lines, United States Authorities delivered similar statements in regard of AML compliance and ICOs. On one hand, the Securities and Exchange Commission (SEC) provided guidelines on its website for investors to consider before participating

---

<sup>112</sup> MAS clarifies regulatory position on the offer on digital tokens in Singapore. Monetary Authority of Singapore (August, 2017) (available at: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx>)

<sup>113</sup> MAS clarifies regulatory position on the offer on digital tokens in Singapore. Monetary Authority of Singapore (August, 2017) (available at: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx>)

<sup>114</sup> Monetary Authority of Singapore, *A Guide to Digital Token Offerings* (2018)

in token sales. Some of the key points the SEC asks potential buyers to consider are that there are ways to identify fraudulent investment schemes.<sup>115</sup> On the other hand, the Financial Crimes Enforcement Network (FinCEN) published a letter indicating that the U.S. agency will apply its regulations to ICOs. In the letter, FinCEN explained that both developers/issuers/sellers and exchanges involved in the sale of an ICO-derived token would be liable to register as a money transmitter and comply with the relevant statutes around anti-money laundering and know-your-customer rules.<sup>116</sup>

The FinCEN letter recognizes that ICOs vary not only from the functional or legally but approach, but also that there are jurisdictional differences depending on the structure of an ICO and its associated token. In sum, FinCEN asserted that it considers the transmission of newly-issued digital tokens derived from ICOs to be subject to the money transmitter rules under the Bank Secrecy Act . This means that developers and exchanges that sell ICO coins or tokens, or exchange them for other virtual currency or something else of value, must register as money services businesses and comply with (i) the Bank Secrecy Act rules regarding Know-Your-Customer obligations, (ii) the implementation of an anti-money laundering and combating the financing of terrorism compliance program, and (iii) the filing of suspicious activity reports. FinCEN also reminded that U.S. persons must comply with all applicable Office of Foreign Assets Control financial sanctions obligations.

FinCEN reported to the Senate that since 2014 it has examined roughly one-third of the approximately 100 virtual currency businesses that have registered and has initiated several investigations and enforcement actions against firms and individuals. However, it is important to clarify that this letter is not yet a formal FinCEN guidance.

Regarding the European Union, in February 2018, the European Commission launches the European Union Blockchain Observatory and Forum which will highlight key developments of the blockchain technology, promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities.<sup>117</sup> Even though, tokens and ICOs remain unanalyzed by policy makers and regulators by European central authorities, the Council of the European Union approved the 5<sup>th</sup> AML Directive and, among other changes, introduced AML obligations applicable to exchange platforms of virtual currencies.<sup>118</sup> Providers of exchange services between virtual and fiat currencies, and custodian wallet providers will have to comply with the AML Directive. Despite this, it is doubtful whether these provisions are suitable to put an end to money laundering using virtual currencies, because virtual currencies can still be exchanged between private actors without any monitoring. Actually, there is no reference in the Directive to ICOs.<sup>119</sup>

---

<sup>115</sup> The SEC even launched in May, 2018 a fake ICO, pre-selling a coin called Howey Coin, to show how easy it is to scam investors. See <https://www.marketwatch.com/story/the-sec-created-a-mock-ico-website-to-show-just-how-easy-it-is-for-investors-to-get-fleeced-2018-05-16> and <https://www.howeycoins.com/index.html>

<sup>116</sup> See Letter from Financial Crime Enforcement Network to Committee on Finance, United States Senate. (February, 2018) (available at: <https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf>)

<sup>117</sup> See [http://europa.eu/rapid/press-release\\_IP-18-521\\_en.pdf](http://europa.eu/rapid/press-release_IP-18-521_en.pdf).

<sup>118</sup> Neither tokens or ICOs.

<sup>119</sup> It seems that the definition of exchanges does not encompass ICO companies as they do not – generally, but with some exceptions - enable their users to change their tokens into fiat money. It also seems that they do not fall within the definition of wallet providers as the funds, which they receive within the ICO, belong to the company, not to the tokenholders. Developers do not hold their users' private keys for the users' wallets, but only holds private keys for its own wallets. However, most developers exchange the raised cryptocurrencies to fiat and deposit them at a bank account for their operational needs. Therefore some could argue that they facilitate an exchange from

Given the regulatory uncertainty, several crypto exchanges in these jurisdictions where they are clearly subject to AML compliance, and also banks, may refuse to work with ICO projects or ICO founders which do not identify buyers of their tokens. This market behavior will possibly force ICOs to voluntarily comply with the AML regulation, or at least to identify the buyers of the tokens. We do not have available data to confirm this hypothesis though.

This means that regulators still need to work on how the best way is to prevent money laundering when operating on a blockchain where the jurisdictional limits become more confusing or non-existing, and where players operate through online platforms rather than physical markets. Perhaps the understanding of these features will lead to different solutions for preventing money laundering in blockchain-based markets, for example, working with digital identity mechanisms to countering the anonymities of ICOs nowadays.<sup>120</sup>

## VI. New challenges for privacy law and data protection

The rise of cryptocurrencies, ICOs and, in general, blockchain use cases, is also generating several issues with regards to privacy law and protection of personal data. The nature of the public blockchain means that every transaction taking place will be published and linked to a published public key that represents a particular user. However, that key is encrypted, and no one would be able to directly identify the users settling transactions on a blockchain.<sup>121</sup> In a blockchain, each block contains a reference to the preceding block by including a cryptographic hash of the data within the preceding block. If the data in a block is altered, the hash of the block changes too, and this falsification of the records can therefore be detected.<sup>122</sup>

However, this operation give rise to some issues regarding personal data, especially in countries that follow the European Union standard of the General Data Protection Regulation Directive (“GDPR”). Data protection rules do not apply to anonymized data and some could consider that because of hashing and encryption, blockchain anonymizes data. This could be debated because anonymized qualification of data is very strict, particularly under European rules. Hashing permits records to be linked, thus it will generally be considered a pseudonymization technique, not an anonymization.<sup>123</sup>

Additionally, Data stored on a blockchain is tamper proof, so deleting it later on is not an option. Moreover, transactions on a blockchain are “immutable”, which really means that once a blockchain transaction has received a sufficient level of validation, some

---

cryptocurrencies to money. See Nejc Novak. *EU Introduces Anti-money Laundering Regulation*. (2018) <https://medium.com/@nejcnovaklaw/eu-introduces-crypto-anti-money-laundering-regulation-d6ab0ddedd3>

<sup>120</sup> See World Economic Forum. *Digital Identity. On the Threshold of a Digital Identity Revolution*. White paper (January, 2018) (available at: [http://www3.weforum.org/docs/White\\_Paper\\_Digital\\_Identity\\_Threshold\\_Digital\\_Identity\\_Revolution\\_report\\_2018.pdf](http://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf))

See Also *Digital Identity is the key to the Blockchain Economy*. <https://dailyfintech.com/2018/03/24/digital-identity-is-the-key-to-the-blockchain-economy/>

See also [https://www.bbva.com/wp-content/uploads/2018/02/Digital-Identity\\_the-current-state-of-affairs.pdf](https://www.bbva.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf)

<sup>121</sup> See *How Blockchain Encryption works*. TechRepublic (November, 2017), available at: <https://www.techrepublic.com/article/how-blockchain-encryption-works-its-all-about-math/>

<sup>122</sup> See *What is Hashing? under the Hood of Blockchain*, Blockgeeks (2017), Available at: <https://blockgeeks.com/guides/what-is-hashing/>

<sup>123</sup> Hogan Lovells LLP, *A Guide to Blockchain and Data Protection*, available at: <https://www.hlgengage.com/uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf>

cryptography ensures that it can never be replaced or reversed.<sup>124</sup> Thus, this data cannot be deleted once it is inserted in blockchain. This feature could be also conflictive with privacy laws and the Right to be Forgotten or Right to Erasure.<sup>125</sup> This consists in the right to obtain from the controller the erasure of personal data without undue delay. However, it is not clear what *erasure of data* actually means. The GDPR initiative probably did not have in mind a distributed data storage mechanism such as blockchain, but only a centralized or non-distributed data controller. The fact that this unique feature of blockchain technology does not match with privacy rules creates some friction and uncertainty for compliance.

This takes us to the next problem regarding privacy law and blockchain. Who is the data controller on a blockchain? Due to the distributed nature of blockchain, there is not any centralized entity gathering and managing this information. In consequence, more than one party may qualify as controller, which means that several participants of the network could be responsible for compliance with privacy regulations. Governance agreements might be necessary among participants to define the responsibilities as data controllers or data processors.

The applicable jurisdiction can also be a problem for blockchain use cases. Blockchains usually have a cross-border nature and an important aspect for privacy laws. In some jurisdictions, privacy law differs from contract law because parties are not allowed to establish the applicable law. The applicable law depends on factors listed in GDPR,<sup>126</sup> for example. As a result, the way blockchain technology operates (based on a system of encryption and hashing) does not seem to be compatible with the traditional system to protect personal data. Therefore, if policy-makers want to promote the use of blockchain technologies, as we believe they should, the approach to deal with personal data should be changed. Regarding blockchain use cases in general, there is still a long way for developers and policy makers to clarify how blockchain fits into the privacy rules world.

## VII. Insolvency

The rise of ICOs may also generate some problems in case of insolvency. Indeed, if the debtor's assets are not sufficient to pay all its debts, the way the ranking of claims in the scheme of distribution may become a very sensitive issue.<sup>127</sup> In a world of tokenholder, one may wonder in which position tokenholders should be paid. To answer this question, it seems relevant to distinguish between equity-tokenholders and debt-tokenholders.

Following the absolute priority rule,<sup>128</sup> it seems clear that debt-tokenholders should always be paid ahead of equity-tokenholders, since the latter are functionally equivalent to shareholders and shareholders cannot get paid ahead of the creditors in an event of insolvency. The situation becomes more controversial in the context of

---

<sup>124</sup> See Gideon Greenspan, *The Blockchain Immutability Myth*, Coindesk (May, 2017), available at: <https://www.coindesk.com/blockchain-immutability-myth/>

<sup>125</sup> See Section 3, Article 17, GDPR. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

<sup>126</sup> See Article 3 of the GDPR, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

<sup>127</sup> This work uses the word "bankruptcy procedures" and "insolvency proceeding" as synonyms.

<sup>128</sup> According to this principle existing in most insolvency jurisdictions, junior creditors cannot get paid until senior creditors have been paid in full, and shareholders cannot get any value out of the firm until the company's creditors have been paid in full. For a deeper analysis of this principle, see Douglas G. Baird, *ELEMENTS OF BANKRUPTCY* (Foundation Press, 5<sup>th</sup> Edition, 2010), pp. 71-77.

debtholders vis-à-vis other creditors, or even between equityholders and shareholders. In these cases, we believe that the solution should depend on whether the white paper mentions something. If the white paper does not specify how debtholders should be paid, they should be paid as general unsecured creditors. Therefore, they will be paid pro rata according to the *pari passu* principle.<sup>129</sup> Likewise, equity-tokenholders would be paid ahead of shareholders, since the latter is the one legally entitled to the company's residual assets.

However, the white paper may establish the treatment of tokenholders in bankruptcy. In those cases, the treatment of tokenholders in bankruptcy will depend on the views taken on insolvency procedures. If a country follows a contractual approach to bankruptcy, these rights should be preserved.<sup>130</sup> Therefore, equity-tokenholders may end up getting paid after or along with the shareholders if the white paper says so, and debt-tokenholders may be ranked ahead or after general unsecured creditors.

However, it is far from clear that this contractual approach will be applied in practice. Namely, we believe that a subordination clause will probably be applied, since it does not harm other creditors – in fact, it will be for the benefit of the other creditors due to the fact that, following the absolute priority rule, subordination creditors will only get paid if more senior creditors have been paid in full. More problems may arise, however, if the white paper gives a priority claim to the tokenholders in case of bankruptcy. Under this scenario, unless the insolvency legislation recognizes this priority or “any priority created by contract”, this preferential treatment may not be enforceable. Therefore, tokenholders should carefully analyze how they would be paid in bankruptcy, and whether the treatment proposed in bankruptcy would be enforceable or not under a particular jurisdiction.

In addition to dealing with claims, an insolvency procedure also deals with assets. After all, the assets will determine whether and, if so, how and how much, the creditors are getting paid. In the context of an ICO, the person or entity in charge of managing the insolvency proceeding will face two primary problems: (i) the valuation of these assets associated with the ICO (that is, the cryptocurrencies received in exchange for the tokens); and (ii) the ability of those assets to be converted to cash (liquidity). When the cryptocurrencies received by the issuer are generally accepted in the market (e.g., Bitcoin, Ethers, etc.), the liquidity problem will unlikely exist. Nevertheless, the valuation problem may still be relevant. Indeed, as it was mentioned above, cryptocurrencies are very volatile assets. In other words, their value may rise or drop rapidly. As a result, this volatility may create some problems not only for the trustee or debtor in possession but also for the creditors, whose rights and decisions may be affected by the volatility of these assets. For example, if they know that the cryptocurrencies held by the issuer can be sold and get enough cash to repay their debts, perhaps they may prefer liquidation over reorganization. However, if the liquidation value of the company is not enough to pay even part of their claims (among other reasons, due to the lack of value of the cryptocurrencies), a creditor may have incentives to preserve reorganization over liquidation – especially if the issuer's future cash-flows are positive. Therefore, we believe that trustees or debtor in possession should warn creditors about the importance of the volatility of the cryptocurrencies potentially held by the issuer, since it may be a factor potentially relevant for their decisions in bankruptcy.

---

<sup>129</sup> For an analysis of this principle, see Roy Goode, *PRINCIPLES OF CORPORATE INSOLVENCY LAW* (Sweet & Maxwell, 4<sup>th</sup> Edition, 2011), pp. 235-240.

<sup>130</sup> However, this is not the general rules. Most insolvency jurisdictions provide a mandatory state-provided set of bankruptcy rules. So far, the contractual approach has been proposed just in the literature. See Robert Rasmussen, *Debtor's Choice: A Menu Approach to Corporate Bankruptcy*, 71 *TEXAS LAW REVIEW* 51 (1992); Alan Schwartz, *A Contract Theory Approach to Business Bankruptcy*, 107 *THE YALE LAW JOURNAL* 1807 (1998);

Additionally, along with the valuation of the cryptocurrencies received by the issuer, another problem potentially existing in the context of ICOs is the valuation of the tokens. While this problem will not be relevant for the insolvency proceeding of the issuer, it will be in the case that the tokenholder becomes insolvent. In these situations, the trustee or debtor in possession will face the challenge to value those tokens, which can be particularly difficult in the absence of a secondary market. Therefore, in these circumstances, the trustee or debtor in possession will be required to use some general methods to value assets, including their ability to generate future cash flows. For that purpose, it will be relevant to determine whether the issuer will finally be able to honor the obligations assumed with the tokenholder. If not, the value of the token will be close to zero.

## **VIII. International challenges and cooperation in ICOs**

Most securities regulators are issuing some guidance regarding ICOs. In fact, IOSCO has even created a section on its website to include statements issued by many securities regulators around the world with regards to ICOs.<sup>131</sup> This is a desirable initiative to contribute to the understanding and “brainstorming” about how regulators should address ICOs. Namely, by being able to know how other jurisdictions are addressing the same challenge, regulators and policy-makers will be able to come up with more ideas to regulate ICOs in a more efficient and effective manner.

However, these initiatives are not enough. On the one hand, it is very costly to analyze each country’s regulatory approach to deal with ICOs. On the other hand, the work developed by international organizations in this space does not analyze the pros and cons of each regulatory solution. For this reason, it would seem desirable if an international organization such as IOSCO issues some guidance on ICOs, at least to establish: (i) the rationale and operation of ICOs; (ii) a proposed explanation and classification of tokens; (iii) the different regulatory approaches that may be implemented to deal with ICOs; (iv) the applicable law that should govern ICOs; (v) the costs and benefits of each regulatory approach; (vi) other issues potential relevant for securities regulators, such as how to protect tokenholders, or how to deal with other challenges raised by ICOs such as anti-money laundering. Thus, even though each securities regulator will be able to choose one model or another, all of them will have the opportunity to know and assess each model in order to decide which one fits best in their financial system, taking into account the priorities of the regulator (e.g., investor protection, innovation, financial stability, prevention of financial crime, etc.), as well as the particular features of the country (e.g., type of investors –institutional or retail–existing in their capital markets, size and expertise of the regulator, etc.). In addition, we also believe that the International Accounting Standard Board (“IASB”) should also issue an International Financial Reporting Standard (“IFRS”) to clarify how to register an issuance of tokens.

Finally, we also believe financial cooperation and the understanding of each country’s laws and corresponding regulatory model to deal with ICOs, is relevant as a mechanism to know the scope of each country’s jurisdiction. For example, while some countries may apply their laws just to any issuance of tokens taking place in their countries, other jurisdictions may find: (i) their enforcement regimes effective enough to require issuers to comply with their existing securities laws (or at least to submit the proposed form in their countries); (ii) to initiate investigations and enforcement actions because the issuer is registered or incorporated in the country; or (iii) just because some of tokenholders are from their jurisdictions.

---

<sup>131</sup> See <https://www.iosco.org/publications/?subsection=ico-statements>

For this reason, and taking into account the different regulatory models existing to deal with ICOs, we think that issuers, regulators and tokenholders should be aware of the applicable law (and competent regulator) to a given issuance of tokens. Otherwise, the issuance may be subject to legal uncertainty at the expense of not only the issuer but also –and perhaps more importantly– the tokenholders and the financial authorities in charge of protecting these tokenholders. Therefore, in the absence of a global regulatory framework for ICOs, which seems very unlikely, we propose that an international agreement to deal with some procedural (mainly jurisdictional) aspects of ICOs would be desirable.

## **IX. Future of capital markets, finance and corporate governance in a world of tokenized securities**

Tokenization may bring positive paradigm shifts to finance, law, government, and more. It can represent changes in the ways we consume goods or replace traditional investments in capital markets. Perhaps, companies and regulators can learn from ICOs and start thinking about improving markets by using blockchain as a new way for delivering goods and distributing securities.

Due to the absence of financial intermediaries, which means less transactions costs, and the possibility for developers to fund long-term projects where it may take years to capture value,<sup>132</sup> ICOs allow companies to raise an important amount of funds in the early stages of a project. Also, the features of tokens vary, providing founders and investors different types of instruments to offer or buy in these markets. Additionally, since tokens fund networks, the buyers – specially retail buyers – of a token are highly interested in making these networks grow.<sup>133</sup> These characteristics of token sales make us believe that the trend of tokenizing securities or goods is attractive for capital markets.

Essentially, tokenization is a method that converts rights to an asset into a digital token. Blockchain hype made the world interested in exploring ways to successfully tokenize real-world assets. This encompasses usage cases of blockchain that are trying to bring this technology to the traditional registry of shares. For example, in May 2016, the Delaware Blockchain Initiative was launched<sup>134</sup> and is currently in an implementation stage. The Delaware General Corporation Law was amended in order to make it legal for entities incorporated in Delaware to use blockchain technology for recordkeeping

---

<sup>132</sup> Since ICOs mostly fund blockchain-based projects. Some of these ideas promise to be disruptive in many markets or industries as use cases of this new technology. Because of this, the implementation of the use cases could take some time to be accepted as a mainstream in many industries. See also Alfonso Delgado *et al*, *Towards a Sustainable ICO Process: Community Guidelines on Regulation and Best Practices* (2016).

<sup>133</sup> This statement is probably not applicable to qualified investors, particularly those funds that are known for participating in pre-sales of tokens and then dump their investments only to make profits.

<sup>134</sup> In May, 2016 Jack Markell – Governor of the State of Delaware – announced an initiative by the State of Delaware to embrace the emerging blockchain and smart contract technology industry, which can help the public and enterprises lower their transactional costs, speed up and automate manual processes, and reduce fraud. This announcement took place in Consensus 2016 conference, which is currently one of the most important international conferences on blockchain currently. See the entire speech here: <https://www.youtube.com/watch?v=-mgxEhIvSTY> Analyzing the features and challenges of this initiative, see Nydia Remolina, *La incorporación de blockchain en el Derecho de sociedades de Delaware*, BLOG DEL INSTITUTO IBEROAMERICANO DE DERECHO Y FINANZAS, 28 August 2017 (available at <http://www.derechoyfinanzas.org/la-incorporacion-de-blockchain-en-el-derecho-de-sociedades-de-delaware/>).

and administration of stock ledgers.<sup>135</sup> This is impressive since Delaware is regarded as one of the most important states for corporate law in United States and the world. In 2015, 86% of all IPOs chose to incorporate in Delaware; more than half of all United States publicly traded companies and 66% of Fortune 500 companies are incorporated in Delaware as well.<sup>136</sup>

In December 2016, Overstock.com Inc. became the first publicly traded company to issue stock via blockchain thanks to the Delaware Blockchain Initiative<sup>137</sup>. One year later Overstock.com Inc launched an ICO (only pre-sale) through its subsidiary tZERO to fund the development of an exchange to facilitate the trading of blockchain-based assets, including securities.<sup>138</sup> However, Overstock.com Inc. announced the U.S. Securities and Exchange Commission is investigating the tZERO Coin pre-sale,<sup>139</sup> therefore the project will probably be delayed indefinitely.

Despite the uncertainty that these cases portray for the implementation of blockchain technology for stock ledgers, the advantages of using it should be explored in depth. Initiatives such as Delaware could bring the benefits investors and companies are experiencing with ICOs to a much broader audience and enhance the development of capital markets, finance and corporate governance. Many years ago, the securities markets went digital and now there are not many investors holding physical certificates of, for example, shares. However, true benefits of digitization will only reach the securities industry when its layers of settlement processes are finally streamlined, so that securities issuers and investors can again interact directly, which is something that could be achieved by blockchain technology.<sup>140</sup> With blockchain, buyers of shares and corporations are expected to have a clear ownership record, lenders holding security interests in pledged stock are expected to be able to foreclose after a triggering event, distribution of dividends and payments are expected clearer as well.<sup>141</sup> Knowing who owns which shares is a fundamental corporate governance requirement. Blockchain technology should make it easy to know at a specific moment the number of shares that a shareholder owns and who exactly are those shareholders. Nowadays corporations – especially publicly-traded corporations– rely on intermediaries to know this information (i.e. when using omnibus accounts, central depositories, etc.).

---

<sup>135</sup> See Delaware Eyeing Blockchain to Improve Corporate Processes (April, 2017), available at: <https://www.bna.com/delaware-eyeing-blockchain-n57982086257/>

<sup>136</sup> See Delaware Division of Corporations 2015 Annual Report, available at: [https://corp.delaware.gov/Corporations\\_2015%20Annual%20Report.pdf](https://corp.delaware.gov/Corporations_2015%20Annual%20Report.pdf) .

<sup>137</sup> See Michael Del Castillo, *Overstock Could Rise \$30 Million With Blockchain Stock Offering*. Coindesk (November, 2016), available at: <https://www.coindesk.com/overstock-raise-30-million-blockchain-stock-offering/>

<sup>138</sup> See Bradly Dale, *The Next Step In Overstock's Master Blockchain Plan is Underway*, Coindesk (December, 2017), available at: <https://www.coindesk.com/tzeros-ico-one-part-overstocks-master-blockchain-plan/>

<sup>139</sup> Overstock.com Inc. (2018). Form 8-K 2018.

<sup>140</sup> For a detailed explanation of the Delaware Blockchain Initiative see Andrea Tinianow and Caitlin Long. *Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION BLOG, available at: <https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/>. See also Nydia Remolina, *La incorporación de Blockchain en el Derecho de Sociedades de Delaware*. BLOG DEL INSTITUTO IBEROAMERICANO DE DERECHO Y FINANZAS (2018), available at: <http://derechoyfinanzas.org/blog/la-incorporacion-del-blockchain-en-el-derecho-de-sociedades-de-delaware/>

<sup>141</sup> Wonnie Song, *Bullish on Blockchain: Examining Delaware's Approach to Distributed Ledger Technology in Corporate Governance Law and Beyond*. HARVARD BUSINESS LAW REVIEW (2018), available at <http://www.hblr.org/2018/01/bullish-on-blockchain-examining-delawares-approach-to-distributed-ledger-technology-in-corporate-governance-law-and-beyond/>

The Dole Food Company, Inc class action is an example of why accurate stock ownership is not achieved in markets today. In this case, there were more than 36 million shares in the class, but claimants submitted facially valid claims for more than 49 million shares which is 33% more Dole common stock than those that actually existed. Clearly, no single ledger kept track –in real time– of stock ownership. When an investor buys a share of common stock in a listed corporation, the investor typically does not hold that share directly. Generally, from the corporation’s perspective, a company called Cede & Co. (a nominee of the Depository Trust Company (“DTC”))<sup>142</sup> is the “record owner” of all the stock, all the time. Investor’s broker keeps an entry in its database showing you as the stock’s beneficial owner, and DTC keeps an entry in its database of the investor broker’s ownership.<sup>143</sup>

Dell’s 2013 go-private merger is another type of case detailing how blockchain technology could potentially help to prevent proxy voting mistakes derived from direct versus indirect ownership of shares. T. Rowe Price lost standing to seek appraisal even though it had vocally opposed and repeatedly tried to vote against the merger. In order to vote on the Dell buyout, T. Rowe Price had to send its vote through intermediaries. A service provider, which was a third party, later provided an updated record related to the merger. This updated record triggered T. Rowe Price’s automated voting system, which was set to vote in favor of any management-recommended merger, like the Dell merger was. Despite T. Rowe Price’s intention to oppose the Dell merger, it ultimately voted in favor, losing standing to sue for appraisal. T. Rowe Price ended up paying \$194 million to compensate its clients for actions for loss of appraisal rights derived from this proxy voting mistake.<sup>144</sup>

Using smart contracts opens a world of possibilities for corporations, even for compliance processes and corporate governance matters. For example, a corporation could use blockchain to record directors’ votes to ensure they act accordingly to regulation and internal policies. A corporation could also program shares issued in a private placement to be issuable only to the digital wallets of those who qualify as accredited investors. Tokenized shares could also be programmed to facilitate the execution of covenants agreed in financing contracts with creditors.<sup>145</sup> And there are more applications to explore for shares issued in a blockchain as tokens in ICOs.

Some other states are following Delaware’s ideas. Wyoming is one example. The Wyoming Blockchain Coalition is focused on encouraging the adoption of blockchain technology in Wyoming and, so far, has been incredibly successful. In fact Wyoming has approved blockchain-friendly bills defining utility tokens and has also exempted them from the state’s money transmission licenses. The coalition has in mind the

---

<sup>142</sup> Cede and Company, also known as "Cede and Co." or "Cede & Co.", is a specialist United States financial institution that processes transfers of stock certificates on behalf of Depository Trust Company, the central securities depository used by the United States National Market System, which includes the New York Stock Exchange, Nasdaq, and other exchanges together with associated clearinghouses. Cede & Co. owns substantially all of the publicly issued stock in the United States. Thus, investors do not themselves hold direct property rights in stock, but rather have contractual rights that are part of a chain of contractual rights involving Cede. See Bloomberg’s Company Overview of Cede & Company, available at: <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=22429124>

<sup>143</sup> See Matt Levine, *Dole Food had too many shares; It's enough to make you wish for a blockchain*. Bloomberg (February, 2017), available at: <https://www.bloomberg.com/view/articles/2017-02-17/dole-food-had-too-many-shares>

See also Joshua Ashley Klayman et al, *Why the Delaware Blockchain Initiative Matters to all Dealmakers*. Forbes (September, 2017), available at <https://www.forbes.com/sites/grouphink/2017/09/20/why-the-delaware-blockchain-initiative-matters-to-all-dealmakers/#2ee375f27550>

See also *In re Dole Food Co. Inc.*, No. CV 8703-VCL, 2017 WL 624843 (Del. Ch. Feb. 15, 2017).

<sup>144</sup> *In re Appraisal of Dell Inc.*, 143 A.3d 20 (Del. Ch. 2016).

<sup>145</sup> For example, dividend covenants.

implementation of a similar initiative to the one passed in Delaware.<sup>146</sup> European markets are being influenced by this initiative. In Germany, for example, models have been developed in which a nominee holds the company's shares as a registered shareholder with tokens. These tokens embed smart contracts that provide for a type of trust agreement between the respective token holder and the nominee. The smart contract is supported by traditional legal solutions (written agreements), thus making the token holder only an indirect shareholder through the written agreement.<sup>147</sup>

In sum, using blockchain technology in the corporate context could revolutionize corporate record-keeping, governance, finance and capital markets. The ICOs experience could bring knowledge to the table for regulators and companies to embrace this new technology in benefit of capital markets development. So far, developers incorporated through a simple Delaware corporation will probably take advantage of the Delaware Blockchain Initiative that would allow the entity to itself incorporate directly on a blockchain.

## X. Conclusion

This paper has sought to provide an understanding of the legal and financial challenges of Initial Coin Offerings. For that purpose, we have started by proposing a concept of tokens based on both their functionality and their legal nature. From a legal perspective, tokens can be classified as security or non-security tokens. From a functional perspective, we have used the classification suggested by FINMA. Therefore, we have categorized tokens into utility tokens, payment tokens and asset tokens. This paper argues that the classification of tokens as 'utility tokens' or 'security tokens' used by many authors and regulators is not only technically incorrect but also misleading since many 'utility tokens' can perfectly be classified as 'security tokens'. Therefore, this classification should be abandoned. After analyzing this issue, it has been argued that the legal classification of the token will depend on the features, structure, distribution and marketing of the issuance of tokens, as well as a particular country's applicable law. Therefore, even though the functionality of the token may provide some guidance about the legal nature of the token, a further analysis will be required in order to determine its legal classification.

We have then analyzed the existing regulatory models to deal with ICOs, explaining why all of them present some flaws. For this reason, we have proposed a new system to deal with ICOs based on four primary pillars. First, any issuance of tokens, regardless of whether they are security or non-security tokens, should be disclosed to the regulator through an electronic form providing a minimum level of information. Second, the purchase of token pre-sales should be prohibited for commercial banks and pension funds. Third, regulators should protect non-security tokens through a variety of tools currently existing to protect consumers. Fourth, regulators should spend more resources in providing information to consumers and investors about the risks associated with ICOs.

After proposing a safe regulatory environment for ICOs, the paper has also analyzed a variety of legal and financial aspects of ICOs, including how to register an issuance of

---

<sup>146</sup> See Wyoming Blockchain Coalition website: <http://wyomingblockchain.io/>

<sup>147</sup> See André Eggert and Yamila Eraso, *Delaware Blockchain Initiative: Revitalizing European Companies' Funding Efforts*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION (September, 2017), available at <https://corpgov.law.harvard.edu/2017/09/21/delaware-blockchain-initiative-revitalizing-european-companies-funding-efforts/>

tokens from an accounting perspective, why the classification of tokens as debt or equity can be relevant, how a situation of insolvency may affect the buyers or sellers of tokens, and the particular challenges of ICOs from the perspective of data protection, privacy law and anti-money laundering. The paper concluded by analyzing the implications of the tokenization of securities for the future of capital markets. By providing a comprehensive and interdisciplinary analysis of ICOs, this paper seeks to help regulators and policy-makers to deal with ICOs in a way that may promote innovation and firms' access to finance without harming consumer and investor protection, market integrity and the stability of the financial system.