Corporate and Financial Markets Law

The New ICO Intermediaries

Vanessa Villanueva Collao* and Verity Winship**

Abstract

Smart contracts promise a world without intermediaries. However, that promise has quickly proved elusive, including in the context of Initial Coin Offerings (ICOs), a vehicle for funding startups built on smart contracts and blockchain. Particularly as ICOs attract retail investors who are not code-literate, the question arises: is there a role for new intermediaries? This article assesses the possibility of an ICO auditor, providing a framework for understanding potential audit functions. In particular, it identifies three main roles: to *translate* the code for retail investors who are not code-sophisticates, to *reconcile* the code with promises made in other materials aimed at ICO participants, and to *verify* offline activity and identity where these remain important to the transactions. It then maps these functions onto emerging models.

I. Introduction

At the beginnings of the crypto anarchist movement, the *Crypto Anarchist Manifesto*[1] announced that the technological revolution would change dramatically the perception of concepts such as property, expression, and identity. Hence, current legal rules would be deemed obsolete. Recession and distrust of financial markets following the 2008 financial crisis had incentivized the crypto community to develop private coinage, looking for a way to protect money from politics. The cyberpunk movement started thinking about a new currency based entirely on trust among its participants or 'consensus'.[2]

Intermediaries were viewed with suspicion, in part because they were considered complicit in the financial crisis. By design, technology rendered them unnecessary. Blockchain would be intermediary-free by its very nature, eliminating the need for the institutions that traditionally served as middlemen in the financial markets.

One of the applications of blockchain is as the underlying technology for raising money for startups in the Initial Coin Offering (ICO) process. ICO

* JSD Candidate, University of Illinois College of Law.

** Professor of Law, University of Illinois College of Law. We appreciate the assistance of Stephanie Davidson and the University of Illinois Law Library.

[1] T. May, 'The Crypto Anarchist Manifesto' available at https://perma.cc/P3XW-J5GA (last visited 30 December 2019).

[2] P. De Filippi and A. Wright, *Blockchain and The Law: The Rule of Code* (Cambridge (MA): Harvard University Press, 2018), 22.

promoters ask participants to send funds (often in cryptocurrency) to a smart contract, which is designed to issue the startup's internal digital currency (tokens or coins) in exchange.[3] The funds are used to support a range of cryptoenterprises (*criptoattività*).

The promise that ICOs would be free of intermediaries lies in part in their use of smart contracts, a type of blockchain architecture that makes certain terms self-executing.[4] Smart contracts built on blockchain were, at least in theory, entirely self-contained, including both the terms of the agreement and the means for execution.[5] This atomization allowed decentralization and promised a world without the (suspect) middlemen. The promised avoidance of the existing infrastructure for accessing funds is so fundamental to the structure of the ICO that regulators point to it as one of the ICO's distinguishing characteristics.[6]

The mechanism relied in part on the ability of potential investors to read and understand the code. It was often made available ahead of time and coders could review and correct, testing for security and execution. Technical security issues tended to be the focus.

When code-sophisticates were the only investors this model may have worked, but the mix of investors has shifted to include retail investors as well.[7] During the 2018 crypto exploit, retail investors relied on popular channels of information (Youtube, Instagram, the web) and, guided by word of mouth, invested in projects

[3] Bitcoin Magazine, 'What Is an ICO?' available at https://perma.cc/MT6M-9D5R (last visited 30 December 2019).

[4] The coinage of the name smart contracts by Nick Szabo during the 1990s originally designated what we would call today electronic or automatized contracts, N. Szabo, 'Smart Contracts: Building Blocks for Digital Markets' available at https://perma.cc/XD5C-K49V (last visited 30 December 2019). This article uses the term in its current meaning (as highlighted in J. Frankenfield, 'Smart contracts' *Investopedia*, available at https://perma.cc/X6YX-H6GR (last visited 30 December 2019) and 'Smart contract' *Wikipedia,* available at https://perma.cc/KKV7-3D3C (last visited 30 December 2019).

[5] F. Möslein, 'Legal Boundaries of Blockchain Technologies: Smart Contracts as Self-Help?', in A. De Franceschi, R. Schulze et al eds, *Digital Revolution – New Challenges for Law* (München: C.H. Beck, 2019). Forthcoming, available at https://tinyurl.com/y64f4aak (last visited 30 December 2019).

[6] In a 2019 consultation paper, CONSOB (Commissione Nazionale per la Società e la Borsa) defined blockchain as a technology capable of offsetting the typical intermediate infrastructures: '*Le ICOs si caratterizzano, rispetto a quanto tradizionalmente avviene per le offerte di strumenti finanziari, per: l'utilizzo della tecnologia blockchain, che permette di disintermediare le infrastrutture tipiche dei mercati dei capitali (es. banca depositaria, consorzio di collocamento, mercati secondari)* (…)' (ICOs are characterized, compared to traditional offers of financial instruments, by: the use of blockchain technology that allows disintermediation of the typical infrastructure of the capital markets (especially deposit banks, underwriters, secondary markets) (…)). Consob, 'Le offerte iniziali e gli scambi di cripto-attività. Documento per la discussione', 19 March 2019, available at https://perma.cc/A6QE-JTCX (last visited 30 December 2019).

[7] S. Cohney et al, 'Coin-Operated Capitalism' 119 *Columbia Law Review*, 591 (2019); US Securities and Exchange Commission (US SEC), 'Statement on Cryptocurrencies and Initial Coin Offerings' 11 December 2017, available at https://perma.cc/P6NC-9ZKF (last visited 30 December 2019).

of doubtful reliability.[8] Some jokesters even issued tokens such as 'PonzICO' and 'Useless Ethereum Token' – reportedly making money despite the cautionary names.[9] Even the more ambiguously named 'Confido' simply disappeared with several hundred thousand US dollars of investor money.[10]

Crypto investors may never have previously engaged in financial markets – the ICO is the first investment. A series of podcasts aimed at crypto investors features hosts that are leading figures in the cryptomarket, such as CEOs of billionaire blockchains' enterprises.[11] The recurrent opening question is 'Have you ever invested in traditional capital markets?' The common reply is negative.

While the cryptocurrencies' market may have been prepared to be joined by coders, it was not well structured for retail investors, and has been compared to gold rushes in the 'Wild West'. This shift has intensified the need to address investor confidence in the marketplace and the perennial problem of fraud in the financial markets – or crypto-lemons.[12]

Certainly introducing new intermediaries is in tension with the most utopian view of an anonymous, intermediary-less, decentralized system. However, it does not require the replication of all intermediaries or complete absorption of ICOs into existing frameworks. Nor does it require complete ban.[13]

Moreover, the claim here is not that auditors, as intermediaries, should be or are an exclusive means of addressing issues in the ICO marketplace. Rather they may be part of a reasonable response to activity that is an awkward fit with existing regulatory frameworks and that poses a challenge for regulators and laws. The activity is not just cross-border, but could be characterized as borderless, which is challenging for regulators whose jurisdiction is traditionally based on

[8] Most ICO teams, possibly blinded by the cyberpunk aspirations, launched ICOs that were easy to target and uncover by administrative agencies. This was the case for Centra (Ticker: CTR), SEC Press Release 2018-53, 'SEC Halts Fraudulent Scheme Involving Unregistered ICO' available at https://perma.cc/8QG5-QE6N (last visited 30 December 2019).

[9] C. Brownell, 'Perils of the Crypto Currency Gold Rush' *National Post* (*Canada*), available at https://tinyurl.com/snb7l9j (last visited 30 December 2019).

[10] A. Kharpal, 'Crytocurrency start-up Confido disappears with $375,000 from an ICO, and nobody can find the finders' *CNBC Tech*, available at https://perma.cc/M9WJ-3A2M (last visited 30 December 2019).

[11] See Flippening, available at https://perma.cc/DEX9-MTLG (last visited 15 October 2019).

[12] This focus on avoiding or punishing fraud is not entirely antithetical to a cyberlibertarian position, which might approve sporadic regulatory intervention in the cases of market malfunction, as in the case in ICO's fraud. F.A. Hayek, *Choice in Currency, A way to stop inflation* (London: Institute of Economic Affairs, 1976).

[13] China announced in September 2017 that 'fundraising through coin offering shall be banned immediately', calling coin offerings 'unauthorized and illegal public fundraising (…). suspected of involving in (sic) criminal activities such as illegal selling of tokens, illegal issuance of securities, illegal fundraising, financial fraud and pyramid schemes.' The Central Bank of the People's Republic of China, 'Public Notice of the PBC, CAC, MIIT, SAIC, CBRC, CSRC and CIRC on Preventing Risks of Fundraising through Coin Offering' 8 September 2017, available at https://tinyurl.com/tmuzsjs (last visited 30 December 2019).

physical geography. Categorizing crypto-assets has also been difficult,[14] leading to uncertainty about how they fit with existing legal frameworks and jurisdictional lines based on asset class.

These challenges drive us to analyze the ICO auditor in terms of its functions. These functions can then be mapped onto existing models and emerging regulatory schemes, and can also adapt to changing and hybrid technologies. The article identifies key areas in which the new intermediaries might act in the interface between the offline world and digital realities, translating between computational and other requirements. In other words, it proposes a framework to address the difficult sorting questions about what can be automated and what (still) needs outside validation and review.

This article identifies three main roles of an ICO auditor: to *translate*, *reconcile*, and *verify*. First, even if the codes were self-contained and self-executing, the movement away from investment exclusively by code-sophisticates requires the communication of the meaning of key terms of that code. In other words, it requires translation by an actor who is able both to read the code and to translate it for others.

Second, some promises may be external to the code, communicated, for instance, through a white paper or other marketing materials. A third party could reconcile these promises with the code, ensuring that promises made to potential participants are effectively encoded.

Third, offline activities and identities are also important to some aspects of the transaction. Offline activity may matter for the fulfillment of triggering conditions within an agreement, and the offline identity of the actors may sometimes matter to investors. This verification function reflects one of the advantages of identifying categories of auditor tasks and a framework rather than a static picture or prescription. In particular, the framework is able to accommodate a shifting line between digital and offline as the Internet of Things digitalizes an increasing amount of information from the traditionally offline world.

The article begins in Part Two by examining the structure and process of ICOs. It introduces the technical aspects, especially the relationship among ICOs,

[14] The ESMA in the ICO and crypto-assets advice paper acknowledges that there is no current legal definition of 'crypto-assets'. At the same time, it distinguishes utility tokens from security tokens: 'Investment-type crypto-asset: A type of crypto-asset that resembles a financial instrument. Utility-type crypto-asset: a type of crypto-asset that provides some 'utility' function other than as a means of payment or exchange for external goods or services'. ESMA 50-157-1391, 'Initial Coin Offering and Crypto-Assets' January 2019, 43. For a recent classification of tokens from European perspective, see, F. Annunziata, 'Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings' *Bocconi Legal Studies*, Research Paper no 2636561 (2019), available at https://tinyurl.com/y6rabud4 (last visited 30 December 2019). The author identifies digital assets (tokens) in three main categories: Payment tokens, Utility and Financial Investment tokens. For another system of categorization, see P. Hacker, C. Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' 15 *European Company and Financial Law Review*, 645 (2018).

blockchain, and smart contracts. It then traces the process of an ICO, highlighting the similarities and differences with an Initial Public Offering (IPO). Part Three provides a framework for understanding the possible functions of ICO auditors, with particular focus on the auditor's role in relationship to the code, the white paper, and offline activity. Part Four points to existing models that incorporate some of the functions the article identifies, both to provide evidence of the need for these functions and also to suggest possible routes to effectuating this role. The article then briefly concludes.

II. The Structure of ICOs

The new blockchain industry goal is to provide financing through a fundraising mechanism, the Initial Coin Offering (ICO), which involves minting (or coinage).[15] This process is accomplished by the exchange of fiat currencies (such as Euro or US dollars) or cryptocurrencies (such as Ether or Bitcoin)[16] conveyed to the platform in exchange for digital assets. Participants send funds to a smart contract, which is designed to issue an equivalent value of ICO tokens or coins.[17]

Smart contracts are a type of blockchain architecture. These DApps (decentralized applications) are built on top of a very well-known platform, Ethereum.[18] Recollection and *recordation*[19] of information are secured through a

[15] The minting process is distinct from the most popular mining process. V. Buterin, Ethereum whitepaper, 'A Next-Generation Smart Contract and Decentralized Application Platform' available at https://perma.cc/CCA3-R76T (last visited 30 December 2019). In the minting process, the participant exchanges x ETH for x SNT tokens. The computer program creates a business logic function. This logic function establish the total number of tokens (usually less than a max hard cap), the exchange rate and the amount of ETH transferred. Moreover, the program must establish how these tokens are generated, how to update the balance and transfers from the initial system, called system zero address (SNT), to the token buyer.

[16] Bitcoin and Ethereum are the most common cryptocurrencies and possess similar features. For example, both Bitcoin and Ethereum are Proof-of-Work (PoW). Decentralized nature in blockchain does not rely on a central point of control but implies a network made of globally connected computers, peer or nodes. The network constantly puts its own digital signature to batches of transactions (blocks). The blocks are built within a process called *mining*; namely, a network of computers receive an input and apply a function to gather a 'single random-output' – the *Hash* function. Miners solve a complicated mathematical puzzle, or algorithm, in the shortest possible way and in exchange for this output they are rewarded with Bitcoins. If two or more miners have solved the problem at the same time, then the one that has the longest code answer wins. PoW system operates in this way. The *hash* function is generated whenever the server suspects a Denial of Service Attack, puts into motion the entire mining mechanism and releases the answer called *hash*. N. Sakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' available at https://perma.cc/A2FM-DD53 (last visited 30 December 2019).

[17] Bitcoin Magazine, n 3 above.

[18] V. Buterin, n 15 above.

[19] The recollection and aggregation of information at a large scale, Big Data, is a current issue in the European framework post-GDPR (European Parliament and of the Council Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC -

consensus mechanism, which is virtually impossible to infringe assuring security and privacy of the transaction through ledger verification.[20]

ICOs raise money for startups (cryptoenterprise: *criptoattività*), often those composed of a small group of persons with solely ideas and no influence over the market more broadly. CONSOB (Commissione Nazionale per la Società e la Borsa) has described ICOs as a fundraising mechanism initiated by corporations, individuals or network of programmers, giving high emphasis to startups as the main actor in the issuance of tokens.[21]

The resemblance to traditional Initial Public Offerings (IPOs) is striking, although the ICO form emerged regardless of any intermediary or regulation. The rules governing IPOs have been relaxed to facilitate capital injection to the market, in the United States through legislation, the Jumpstart Our Business Startups Act (JOBS Act),[22] and in Italy by the *Borsa Italiana* through the *Regolamento Alternativo del Capitale* (AIM Italia).[23] Nonetheless, there is still an appetite for ICOs, particularly in early stage technological entrepreneurships.

In some markets, Kickstarter and other forms of crowdfunding play a partial role in allowing small, early stage start-ups to access the capital markets. These are predecessors of ICOs, and one could crowdfund through the sale of tokens, tightening the comparison.

In at least one example, the relationship to crowdfunding has been formalized. In 2019, CONSOB delivered a consultation paper on ICOs and crypto-assets.[24] This consultation paper aims to assess the extent of cryptoassets in Italy, while waiting for a more accurate framework at the European level. The paper described the venue of cryptoassets's offers as the online platform,[25] without

General Data Protection Regulation). V. Zeno-Zencovich, 'Ten Legal Perspectives on the "Big Data Revolution" ' *Concorrenza e mercato*, 50 (2016). The data within blockchain, although shielded by anonymity may conflict with the GDPR's principles enclosed in the above-mentioned regulation. In particular, the unavailability of a deletion function to erase the code (ie: the transaction) is the main issue European regulators might face.

[20] P. De Filippi and A. Wright, n 2 above, 22.

[21] Consob, n 6 above, 3.

[22] Jumpstart Our Business Startups Act, Pub L No 112-106, 126 Stat 306 (2012) (codified at 15 U.S.C. §§ 77a-77r, 78a-780).

[23] In Italy, the *Borsa Italiana* through the *Regolamento Alternativo del Capitale* (AIM Italia) – *Regolamento Emittenti* 1 Marzo 2012, has built up an entire sector devoted to facilitate the entrance on the so-called Alternative Capital Markets for small and medium type business. These entities enjoy a particular structure that goes from the appointment of a nominated advisor – that takes the function of the underwriters –, coupled with the Partner Equity Markets. The latest is a network of highly-qualified institutions (advisory companies, law firms and auditing firms) that follow international standard practices, offering support throughout the life cycle of the enterprise. Borsa Italiana, 'Private Equity Markets' available at https://perma.cc/2XYW-QPS2 (last visited 30 December 2019).

[24] Consob, n 6 above. The consultation paper was open to different actors in the crypto market targeting Italian investors, as well as academics, for commentaries addressed to the Public Hearing that took place in May 2019.

[25] Riquadro 2. Consob, n 6 above, 8.

describing how this platform may operate. Notably it forwarded inquiries and assistance to the *gestori di portali per la raccolta di capitali di rischio* (web providers for the collection of risk capital) already regulated by the crowdfunding regulation.[26] CONSOB's consultation paper does not exclude the possibility of a different type of counsel, not tied to crowdfunding specialists, but even that would need to meet the crowfunding regulation requirements.

One main difference between this type of crowdfunding and ICOs is the wider public that ICOs are able to attract.[27] Indeed, some crowdfunding structures may be a bad fit due to the divergence of audience (domestic in the crowdfunding, potentially global in the case of ICOs), and the difference of the assets exchanged. In the case of crowdfunding the capital is requested in exchange for either a pre-order (in the best case scenario) of those assets or a thank you note. In contrast, in the ICO what is given in exchange are digital assets that enclose a variety of rights, commonly voting and dividends.

In financial markets, centralized intermediaries assist companies going public, employed mainly as an interface between exchanges and companies dealing with regulation, establishing the procedures for trading securities,[28] and significantly, keeping the record of the transactions. Blockchain had substituted this role, by being (allegedly) tamper-resistant, transparent and establishing a reliable record of all the transactions with one action.[29]

Information about ICOs is available to investors, but not in the canonical way. The code is at the same time the contract itself and the source of information available to the public. This code provides valuable information that can help distinguish bad projects from good ones, as well as incorporating the price into the token.

Information in the blockchain environment is open source and most code is publicly available on github.[30] An empirical study showed that about ninety percent of ICO codes were published before the ICO.[31] The success of the project is

[26] Regolamento Consob 26 June 2013 no 18592 (Regolamento Crowdfunding).

[27] SEC, Securities and Exchange Commission, 'Investor Bulletin: Initial Coin Offerings' 25 July 2017, available at https://perma.cc/A5KE-8RNE (last visited 30 December 2019).

[28] The nature of tokens, as a security, remains uncertain. Recent studies have highlighted the resemblance of tokens to equity securities. For example, see, E. Lyandres et al, 'Do Tokens Behave like Securities? An Anatomy of Initial Coin Offerings' (2019) available at https://tinyurl.com/y3kekcbl (last visited 30 December 2019). Another empirical analysis – considering a sample of 1000 ICOs' white papers – shows that fourteen point two percent are of the equity type. See D. Zetzsche et al, 'The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators' *University of Luxembourg Law*, Working Paper no 11/2017; *UNSW Law* Research Paper no 83; *University of Hong Kong Faculty of Law*, Research Paper no 2017/035; *European Banking Institute*, Working Paper Series 18/2018; 63 *Harvard Internationl Law Journal* (2019) forthcoming, available at https://tinyurl.com/y2e9cfls (last visited 30 December 2019).

[29] P. De Filippi and A. Wright, n 2 above, 93.

[30] Github, Inc, available at https://tinyurl.com/4dyt6b (last visited 30 December 2019).

[31] S. Adhami et al, 'Why do businesses go crypto? An empirical analysis of initial coin offerings' 100 *Journal of Economics and Business*, 64-75 (2018).

tied to the release of the code. When the code is published, more money is raised.[32] Because of review by the crowd of coders, the idea was that problems with the code would be identified and fixed before the ICO. Indeed, Ethereum provided a cautionary tale about the perils of ignoring coder comments. It went forward in the ICO process notwithstanding the continuous 'warnings' of the community regarding the multiple vulnerabilities of the code and ultimately had to spend more money than it earned to fix it.[33] The process relies on an opinion network to review the code and anticipate the offering. ICO's advertisement generally comes only after the code is public for a bit; Gnosis, for example, spent a year revising its code.[34]

The 2018 Italian legislation[35] defining and regulating cryptoassets is a good example of the emphasis on self-contained and self-executing code. The legislation defines a smart contract as software[36] (*programma per elaboratore*) that binds the parties. It thus reaffirms its contractual nature and at the same time equates the smart contract to a written agreement satisfying the formalities for its efficacy under Art 2720 of the Italian Civil code. The strong relationship between smart contract and blockchain is visible in this definition, which is narrow, cutting off all the types of smart contracts outside the blockchain.[37] The description of blockchain-based smart contracts as 'self-executing contract(s) expressed through software' is another precise definition that has been proposed.[38]

[32] ibid 73.

[33] SEC, 'Securities and Exchange Commission, Release No. 81207/July 25, 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO'; hereinafter the DAO report.

[34] Gnosis raised in April 2017 twelve point five million USD using a reverse Dutch auction, after two years of pre-public engagement and one year of post-public engagement. Commonly, the pre-public engagement takes between six months to one year while post-public engagement (namely, when the launch of the ICO is announced) takes up to three months. This shorter period is aimed to maintain the public attention and involvement; the choice of a larger period will probably dissipate interest in the ICO. See, Gnosis, 'White paper ed. December 2017: 2. Roadmap', available at https://perma.cc/3JJD-YVZT (last visited 30 December 2019), 10-11. For the method employed by Gnosis in the reverse Dutch auction see, V. Buterin's website, 'Analyzing Token Sale Models', available at https://tinyurl.com/y5j9xk5b (last visited 30 December 2019).

[35] Legge di conversione 11 February 2019 no 12 of decreto legge 14 December 2018 no 135, *recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione* (Decree no 135, bearing urgent provisions for support and streamlined compliance procedures of private companies and public administration).

[36] ibid Art 8-*ter*, comma 2.

[37] This definition gives legal certainty to the smart contract, treating it as an electronic document both *ad substantiam* and *ad probationem* (the latest due to the timestamp function). However, it is unclear which type of timestamp by electronic validation is mentioned. The electronic Identification Authentication and Signature regulation (eIDAS) asserts the distinction between qualified and non-qualified electronic time stamp, the latest judicially ascertained. Art 41, European Parliament and of the Council Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, [2014] OJ L257/13.

[38] C. Bomprezzi, 'Commento in materia di blockchain e smart contract, alla luce del nuovo Decreto Semplificazioni' *Diritto, Mercato e Tecnologia*, 27 February 2019.

Unlike the IPO, the ICO launch – which evolved without a regulatory framework – provides little information regarding the enterprise itself. The practice of issuing a white paper emerged over time, and evolved into a source of information about the ICO. Some evidence suggests that the white paper is more robust when the code itself is not released, indicating that it sometimes serves as a substitute source of information. The code may not be released in cases where the originality of the project (the know how) is considered valuable, and needs to be protected by non-disclosing it. Moreover, the availability of the programming code source increases hacking chances.[39]

The white paper might have a unique role when promises that may be important to investors and ICO promoters – and that are routine in lawyer-drafted contracts – are difficult or impossible to encode. One such example is *force majeur* or hardship clauses, which would appear in a lawyer-drafted contract but that, even if included in a white paper, would be difficult to express in code.[40]

While some are freestanding online documents, clearly labeled white paper,[41] the term 'white paper' is sometimes a formal label for what is essentially a webpage and some social media communications marketing the ICO.[42] The white paper may be the sole source of information available to retail investors who are not code-literate. It accomplishes a very specific function: to drive information to retail investors in the crucial moment of the ICO process, before the token sales.[43]

The white paper is not a formal prospectus; it likely never crossed the minds of programmers to have one. Some white papers include an explicit statement that they are *not* to be considered a prospectus and should not trigger the accompanying regulation and requirements.[44] Nonetheless, white papers have the connotations of an unofficial prospectus. CONSOB's definition of the white

[39] S. Adhami et al, n 31 above, 4.

[40] C. Dannen, *Introducing Ethereum and Solidity. Foundations of Cryptocurrency and Blockchain Programming for Beginners* (Brooklyn, New York: Apress, 2017), 78; T. Butler et al, 'Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop' 36 *Banking & Financial Services Policy Report*, 1, 4 (2017).

[41] Eg Paragon, 'Whitepaper version 1.0', available at https://perma.cc/R7WP-RBT3 (last visited 30 December 2019).

[42] Eg Tron (Ticker: TRX) focused primarily on the visual content of their website with the purpose of showing a solid company. However, under the rubric 'developers documentation,' in a confined angle of their website, are available three types of whitepapers. Electroneum (Ticker: ETN) has its own youtube channel where all the news related to the enterprise are updated. See, Electroneum youtube, available at https://perma.cc/6CQT-YQMK (last visited 30 December 2019). Ripple (Ticker: XRP) does not provide a whitepaper on their website but two versions are available online. In most cases, such as the case of Ripple, the white paper is mentioned as a source for historical or educational purposes and does not reflect the current protocol. See, 'Ripple Protocol Consensus Algorithm' available at https://perma.cc/UL6P-D26L (last visited 30 December 2019). Compare with B. Chase and E. MacBrough, 'Analysis of the XRP Ledger Consensus Protocol' *Ripple Research* (2018). The latter has a level of sophistication difficult to process.

[43] S. Cohney et al, n 7 above.

[44] JUR, Decentralized Dispute Resolution Infrastructure, 'White Paper v.0.3' (2) available at https://perma.cc/P5KN-5MCE (last visited 30 December 2019).

paper, as a publication in which the principal characteristics of the (project or) operation[45] and the object of the offer, gives the sense that we are dealing with some sort of informal prospectus. The analogy to a prospectus is also supported by existing ICO white papers that include information typical of a prospectus such as risk factors;[46] others are even titled 'prospectus'.[47]

Treatment of the white paper as a prospectus is also the approach of Malta, one of the first governments to regulate cryptoassets. Malta's 2018 Virtual Financial Assets Act (VFA)[48] provides that certain types of decentralized ledger technology assets (DLT)[49] are subject to a particular prospectus regulation.[50] Another provision in the Maltese regulation of cryptoassets requires an auditor, appointed by the license holder, and further exonerates her from any type of professional responsibility while reporting issues to the competent authority (Malta Financial Services Authority), incentivizing disclosures and extending these duties to VFA agents and issuers.[51] However, the liabilities for the issuer[52] are referred solely to the white paper or other human readable contents described in the website.[53] This and other provisions allocate the white paper, and further readable information, as prospectus *per relationem*.

[45] *Operazione*. Understood as the project itself. CONSOB, n 6 above.

[46] Paragon, n 41 above.

[47] Polybius, 'Polybius Prospectus: A Project of a Regulated Bank for the Digital Generation' (2019), available at https://perma.cc/83AT-GZYP (last visited 30 December 2019).

[48] The VFA Act aims to provide investor's protection and is tied to the European directive on Money Laundering. European Parliament and of the Council Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) no 2012/648 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L471/73.

[49] Regulated by the Innovative Technology arrangements and Services Act (ITAS). Chapter 592, Act XXXIII of 2018. AN ACT to provide for the regulation of designated innovative technology arrangements referred to in this Act, as well as of designated innovative technology services referred to in this Act, and for the exercise by or on behalf of the Malta Digital Innovation Authority of regulatory functions with regard thereto.

[50] Art 47 of Virtual Financial Assets Act (VFA). Chapter 590, Act XXX of 2018. AN ACT to regulate the field of Initial Virtual Financial Asset Offerings and Virtual Financial Assets and to make provision for matters ancillary or incidental thereto or connected therewith. The act distinguishes among asset types. Competent authority must introduce a test excluding from the definition of *virtual financial assets* those tokens that are *virtual tokens* (which in turn are utility tokens), *financial instruments* (subject to MiFID II regulation) and *fiat currency in electronic form*. The VFA Act does not regulate those partially centralized technologies that deal with cryptoassets, as well as hybrids (ibid).

[51] ibid Art 50 et seq Part VIII, Duty of Auditors. The regulation does not develop the auditor's role beyond the mention of the duties of the auditor.

[52] The VFA refers to an issuer as a 'legal person duly formed under any law for the time being in force in Malta which issues or proposes to issue virtual financial assets in or from within Malta', leaving the door open to DAOs as possible issuers if recognized as legal persons. Art 1 (2), VFA. Note that in the ICO process there is no issuer in the conventional sense; its decentralized nature makes the entire network the real issuer. See F. Annunziata, n 14 above, 28.

[53] ibid Art 10.

In sum, despite its novelty, the ICO shares some features with the IPO and other existing forms of accessing capital. However, in addition to underlying assets and the current dearth of regulatory structure, a key difference is the source of information accessible to participants. The ICO and its terms are communicated to participants through the code and/or the white paper and other human readable promotional materials.

III. ICO Auditors

Originally, ICOs were targeted to a specific market of 'sophisticated investors' (read coders), capable of deconstructing the code and analyzing the feasibility of the project.[54] The open assets in blockchain may have some impact on sophisticated investors capable of reading and understanding the code. However, many projects rely on a high volume of capital to achieve their purposes, so target retail investors more broadly. During 2017, within the cryptocurrencies' boom, the market for cryptocurrencies shifted from the sophisticated investors to include retail investors as well.[55] Here the complexities of the unregulated market became visible.

ICOs rely on the code to communicate terms, but the entry of retail investors who are not code-sophisticates complicates such reliance and gives rise to the need for new intermediaries. ICO auditors are needed to bridge the elements of the ICO process – the code, the white paper, and, in some circumstances, related offline activity. After examining pros and cons, this section analyses each of the functions in turn: translation of the code for retail investors, reconciliation of the code with other information targeted at ICO participants, and verification of offline activity and identity.

1. Advantages and Disadvantages

The efficacy of ICO auditors relies on their role as reputational renters. A useful definition of these gatekeepers is as 'reputational intermediaries' whose value lies in being

> 'repeat players who provide certification or verification services to investors, vouching for someone else who has a greater incentive than they to deceive'.[56]

Auditors accomplish a double task, first *i)* control the operations of the company that required the audit and, second but most importantly, *ii)* create a

[54] S. Adhami et al , n 31 above.

[55] S. Cohney et al, n 7 above, 19. For a contrary view, C. Catalini and J.S. Gans, 'Some Simple Economics of the Blockchain' *Rotman School of Management*, Working Paper no 2874598; *MIT Sloan* Research Paper no 5191-16 (September 21, 2017), available at https://tinyurl.com/yxsmpnfk (last visited 30 December 2019).

[56] J. Coffee, *Gatekeepers: The Professions and Corporate Governance* (New York: Oxford University Press, 2006), 2.

transparent market 'assuming a public responsibility transcending any employment relationship with the client'.[57] Through their auditing, these companies send to the general public a message of quality and guarantee of accuracy and reliability of the business they have audited, which is necessary to tackle the market for lemons.[58] The credibility of auditing companies rests in the fact that they are repeat players[59] with reputational capital acquired through the years.

Information asymmetry is reduced by these intermediaries, since they come into play at an early stage of the transaction, when the promise of ICOs/ Tokens is released through the code and white paper. The ICO auditor could protect investors directly, by an *ex ante* verification at the time of the ICO minting process. The ICO auditor might also have a role *ex post*, protecting the private interests of investors in smart contract's enterprises, screening the information in the code with the information provided after the ICO has taken place.[60]

Ex ante review of the terms is particularly important in the context of ICOs because of barriers to remedies. Once the smart contract satisfies the condition for which it was programmed, there is no way to reverse the transaction. The only remedy (if any) available is under restitution.[61] However, the shielded identities of the parties makes this *ex post* remedy impractical.

Because there is no current alternative of a legislative system capable of regulating decentralized markets, reliance on a reputational intermediary is a concrete and appealing option. The introduction of an auditor does not necessarily recreate a centralized system of intermediaries. In fact, part of the appeal is that the auditor could be a signal of quality even in a decentralized marketplace. Examples have emerged of developing social norms and decentralized jurisdictions that try to recreate a regulated environment.[62]

Moreover, regulating these startups by an incisive role of the auditor is less expensive than regulating end-users. The more data collected in cyberspace, the

[57] United States v Arthur Young & Co 465 US 805, 818 (1984).

[58] G.A. Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' 84 *Quarterly Journal of Economics*, 488 (1970).

[59] M. Galanter, 'Why the "Haves" Come out Ahead: Speculations on the Limits of Legal Change' 9 *Law & Society Review, Litigation and Dispute Processing: Part One*, 96-98 (1974).

[60] C. Tedeschi, 'L'indipendenza dei revisori: a proposito della nuova normativa sulla revisione legale dei conti' *Giurisprudenza Commerciale*, 771 (2010). J. Cohen et al, 'Corporate Governance and the Audit Process' 19 *Contemporary Accounting Research*, 573 (2002).

[61] In the Italian panorama, it has been argued that the subject matter of this 'contract' is determinable at a later future time, when the condition enclosed in the promise is satisfied. Hence the contractual content is not known at the time it is performed but becomes known when the condition is performed. See, G. Finocchiaro, 'Il contratto nell'intelligenza artificiale' *Rivista Trimestrale di Diritto e Procedura Civile*, 452 (2018). However, as noted along these lines, a definite conditioned promise does not exclude parties' information asymmetry. The potential investor may be incapable of understanding the extent and significance of the encoded promise, it is more than merely ambiguous, and it falls short of being unconscionable.

[62] eg Aragon Network, 'White Paper' available at https://perma.cc/FUM7-ES8E (last visited 30 December 2019).

more chances to target individuals. Notwithstanding, end-user regulation is expensive and frustrating, since users can be located outside the boundaries of specific jurisdictions.[63] The object of regulation[64] in blockchain disappears as it is replaced by a code.

That said, ICO auditors are not a panacea. In fact, they face some of the same issues as traditional financial auditors and other gatekeepers. Much of the discussion and critique has revolved around auditor independence, particularly when they are paid by the companies they audit. As one author summed up: 'one problem overshadows all others: typically, the party paying the gatekeeper will be the party that the gatekeeper is expected to monitor'.[65] European Union regulation has encouraged alternatives in the auditor's description to embrace the real role of auditors in financial markets.[66] For obvious reasons, the auditor cannot be totally unrelated to the company that is audited.[67] It may be more realistic to opt for an alternative word for this requisite such as objectivity, autonomy, self-determination, professionalism, etc.[68]

Another way to address the problems of independence is through a so-called statutory auditor, appointed by the state to provide certification and auditing. This is already done in practice for small and medium enterprises (which is the same target of tech startups).[69] Notaries – discussed further below – are also a good example of a hybrid system, where the notary has duties and

[63] P. De Filippi and A. Wright, n 2 above, 176. Other ideas of regulating the Internet proposed by De Filippi and Wright involve the Internet, ie, the TCP/IP protocol. The transparency of the blockchain operates by sharing publicly the code. The Internet Service Provider can be regulated by blocking the traffic on a specific blockchain-based application, limiting their services. Nevertheless, the use of Tor browsers can shield the traffic encrypting it.

[64] The so-called *pathetic dot*. L. Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), 122-125. For a contrary opinion, where the object of regulation is always present in online activities. See G. Resta and V. Zeno-Zencovich, 'Volontà e consenso nella fruizione dei servizi in rete' *Rivista Trimestrale di Diritto e Procedura Civile*, 441 (2018).

[65] J. Coffee, n 56 above, 3. However, the gatekeeper activity is also tied to the regulator which has a primarily interest in making information emerge, as a stakekeeper in financial markets. C. Alves, 'Corporate Governance Auditoria e Regulação: Há Conflito de Interesses' (Corporate Governance Audit and Regulation: Conflict of Interest) 55 *Cadernos do Mercado de Valores Mobiliários* (December 2016), 121. Furthermore, the constant interaction with the administrative agencies makes the gatekeeper role a conjoint task. See J. Correia de Miranda and S. Coimbra Henriquez, 'Riscos de auto-revisão e interesse pessoal – Contributos para a compreensão das amenaças ao dever de independência dos auditores' (Risks of self-review and personal interest – Contributions to the understanding of the threats to the duty of independence of auditors) 55 *Cadernos do Mercado de Valores Mobiliários* (December 2016), 152.

[66] European Commission, 'Green Paper, Audit Policy: Lessons from the Crisis' COM (2010), 561.

[67] C. Tedeschi, n 60 above, 779.

[68] Moreover, auditor's independence is described in a negative way, highlighting circumstances in which this requisite is lacking. European Parliament and the Council Regulation (EU) 2014/537 of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC [2014] OJ L158/77.

[69] Borsa Italiana, 'AIM Italia – Mercato Alternativo del Capitale' available at https://perma.cc/W44T-TA46 (last visited 30 December 2019).

regulation of a public officer, but is paid by private parties seeking the service.[70]

Despite these caveats, in a decentralized and disorganized market that crosses jurisdictional boundaries, these sorts of third-party intermediaries may serve an important role.[71]

2. The Functions of an ICO Auditor

What type of intermediary is suitable for ICOs? This section identifies and analyzes three main roles for the ICO auditor: to translate the code for retail investors, to reconcile the code with promises made in other materials, and to verify offline activity and identity.

a) Translate

One issue in these decentralized markets is the reliability of the encoded promise. Before retail investors had access to this emergent market, coders were (mostly) capable of improving and perfecting the publicly available code. Therefore, technical security issues were of most interest for the community.

The centrality of the code is also built into emerging legal approaches. The CONSOB consultation paper provides some insights regarding ICOs and traditional financial markets, as well as their interaction with existing European regulations (MiFID II).[72] For example, it assimilates token released in the minting process to a certificate constituting legal title for the transmission and incorporation of the rights embedded in the token. Following this reasoning, the extent of those rights would be totally encoded. The real project or operation, as CONSOB calls it – mirroring the financial operation regularly described in formal prospectuses – is described in the code.[73]

It is not always an easy task to read the code, even for experts, in part because of the cumulative and additive nature of the code writing built into the pre-ICO public availability and crowd review. Some may be available only in machine-readable form such as bytecode, which is publicly available in theory, but not easily accessible.[74] The role of the ICO auditor is accordingly as a code reader and translator, who can inform investors of the important encoded terms of the ICO. Asymmetry of information would be reduced also among sophisticated investors in regulated markets.[75]

[70] A. Anselmi, *Principi di arte notarile*, (Roma: Libreria Forense - Editrice, 1952), 24.

[71] The need of a supranational regulation is desirable, however utopic. The concepts developed in each legal order reflect a policy choice, which is difficult to merge. P. Maume and M. Fromberger, 'Regulations of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws' 19 *Chicago Journal of International Law*, 548, 585 (2019).

[72] CONSOB, n 6 above.

[73] ibid.

[74] S. Cohney et al, n 7 above, 47.

[75] L. Lin and D. Nestarcova, 'Venture Capital in the Rise of Crypto Economy: Problems and Prospects' 16 *Berkeley Business Law Journal* (2019) forthcoming, *NUS Law*, Working

b) Reconcile

Whereas the role of translator is focused on making the main features of the code intelligible to non-code-sophisticates, the reconciliation function is all about the intersection between the code and other information. Contractual promises are complex, included inside the code as well as outside of it. Although in the idealized ICO, the code contains everything, often the main information accessible to the retail investor is the surrounding information online, including in the white paper. This surrounding information may include promises. Someone who is not able to read the code cannot confirm that the promises are encoded; they cannot, in other words, reconcile the code and the white paper (or other non-code materials promoting the ICO).

In this context, auditors can accomplish a specific function: verify the consistency between the white paper and the code. It is possible to leave the blockchain unaltered and, at the same time, require an auditor to pre-monitor the extent of the promise (what is advertised and declared, by any means of information) integrating this promise into the code.[76] The role is to check that additional promises made in materials such as white papers are actually encoded: a mind-the-gap function reviewing the correspondence of code with the other available information. The importance of the continuous aggregation of information is crucial for prospective ICO holders, as well as for holders in the post-ICO process, in order to attenuate the opaqueness of the quality of ICO characteristics.[77]

This concept overlaps with the translation function discussed above, in that it assumes that one of the needs for an auditor is as a code reader. What is additional here, however, is that the focus is not on the code alone and explaining what is encoded, but on the relationship between the code and other information. It requires dual expertise – someone who reads and understands the code and who reads and understands (and cares about) the additional available material. On this account, the rise of legal engineers that handle basic notions of cryptography would be helpful to the realms of law.[78]

The need for such a function is supported by the available data. One empirical study examined three categories of terms that have been important to protecting traditional investors: supply restrictions, restrictions on insider transfers, and immutability, in particular whether ICO promoters retain the right to modify

Paper no 2019/003, *NUS Centre for Banking & Finance Law*, Working Paper 19/01, available at https://tinyurl.com/ygmnarrg (last visited 30 December 2019).

[76] S. Cohney et al, n 7 above.

[77] Bancor (BNT) ICO reached its hard cap and ignored it, continuing to issue tokens. E. Lyandres et al, n 28 above. The hard cap (total issuance of a coin) is one of the elements that future holders consider relevant ie, the creation of scarcity, avoidance of dilution and the match between the project funds raised and the roadmap. All those elements indicate an increased future value of digital assets.

[78] K. Werbach and N. Cornell, 'Contracts Ex Machina' 67 *Duke Law Journal*, 313 (2017).

the code.[79] In its sample of large ICOs from 2017, the study identified significant gaps between what was encoded and what was promised to participants through white papers and other information.[80]

So far, this description assumes that the auditor's role is backwards looking, assessing existing white papers and other information. One can also imagine a system where the ICO auditor is involved in ensuring the quality of the information in the white paper or even in drafting the white paper based on its reading of the code. Accordingly, the translation function described above and the reconciliation functions may very well overlap.

Finally, more established markets rely on mandatory disclosure to avoid information asymmetry. The contents of the IPO prospectus are dictated by statute and regulation.[81] But it is worth noting that mandatory disclosure is not the only possible mechanism. If ICOs are interested in signaling quality, they might make some voluntary disclosures. The ICO Governance Foundation, a non-governmental organization, has even designed a form – Form IGF-1 – to structure voluntary disclosure in the ICO context.[82]

c) Verify

The last category addresses the persistent intersection between the digital and the offline. Offline information is important to know whether offline conditions are satisfied. In regular contractual agreements the intention of parties, the conditions imposed, and other features make the promise as clear and intelligible as it can be for the subscriber. In smart contracts these aspects of the contractual language, the denotational aspects, do not appear. A contract possesses operational and non operational parts, whereas the smart contract has the operational parts but lacks most of the non operational parts, such as conditioned terms.

Emerging intermediaries specifically target the intersection between the digital and the offline. As one put it:

> 'Building a truly valuable smart contract requires the use of multiple inputs to prove contractual performance. (…) Smart contracts require secure middleware to connect them to real world data. This external data will trigger the contract, creating the need for its high reliability'.[83]

In other words, verifying offline performance of a condition remains a task

[79] S. Cohney et al, n 7 above, 6.
[80] ibid 51 & Appendix C.
[81] eg US Securities Act of 1933.
[82] M. Matsumura, 'ICO Governance: a Protocol-Based Self-Regulation of Token Sales in Decentralized Capital Markets' December 2017, available at https://perma.cc/X58W-WH2T (last visited 30 December 2019)
[83] ChainLink Features, available at https://perma.cc/6CJ9-AFJB (last visited 30 December 2019).

that cannot be executed through the code alone.

Considering the fast progress of technology, the line between offline and virtual is not static. It is possible to include information in the code through the expansion of the Internet of Things, and mixed automated devices (such as GPS devices). Nevertheless, what will constitute the added value of the auditor consists in the verification and validation of the code by the offline recording of transactions, wherever that line is drawn.[84]

The identity of those involved with the startup and those investing may also matter. One of the promises of transactions based on blockchain was that those involved could remain anonymous (or pseudonymous).[85] The *Manifesto* acknowledged that this would lead to money laundering and illicit trades,[86] but was unconcerned with this possibility. In some ways this function for an ICO auditor stems from a disagreement about the premise. If we are troubled by money laundering, then offline identity may very well matter. Even outside these more extreme possibilities, the identity of those involved in a startup may matter to investors, and certainly regulators may want to know, particularly as participants expand beyond code-sophisticates.

Anonymity is not the only concern. Online descriptions may claim identities and credentials that are fictitious when compared to the offline identity and that may raise concerns about fraud. For instance, reportedly copy writers advertising on China's Taobao offered to draft white papers with little connection to the offline identity: service providers reportedly advertised that they could

> '(…) "falsify the education and professional background of these ICO teams. Harvard, Yale, Stanford, Cambridge, Apple, Google, you name it. And we will ensure their profile pictures remain unsearchable on the internet" '.[87]

Offline identity of ICO promoters may inform decisions to invest and need some mechanism to verify this identity.

Because it is not possible to assess the identity of the person involved in the startup from the digital information alone, the alleged transparency of the code (which is public) seems also not to be adequate protection against the potential risk of market manipulation and insider dealing. ICO auditors, through their verification of the offline, might address these concerns about offline contractual conditions and the relevance of offline identity.

[84] C. Catalini and J.S. Gans, n 55 above, 11.

[85] T. May, n 1 above. 'Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other'.

[86] ibid.

[87] W. Zhao, '$600 Fraud? Fake ICO White Papers Are Drawing Scrutiny' *CoinDesk*, available at https://perma.cc/5BFH-D7WR (last visited 30 December 2019). The article quoted a Beijing news story available at https://perma.cc/RB9Z-K9M8 (last visited 30 December 2019).

Collateralized stablecoins[88] provide another example of the need for verification. Stablecoin – also called the anti-bitcoin – is a type of cryptocurrency that maintains a stable value, a ratio of 1:1USD.[89] Verification is needed of the amount of off-chain collateral. One of the first stablecoins, Tether (Ticker: USDT), lost credibility after suspicions arose regarding the exact amount and consistency of the cash reserves held as a collateral. The distrust generated in the community placed USDT in a dangerous position backed by USD at a ratio of 1:0.96. Moreover, an unofficial audit showed that Tether USD funds backed 74% of its reserves.[90] An external off-chain audit might be helpful in assessing the extent of the amounts collateralized, all while preserving decentralization.[91]

The transparency offered to the public does not stop at the nature and composition of the reserved funds. In an immature virtual financial market, tracing operations is fundamental to ferret out issues such as commingling of assets, as these types of vehicles facilitate opaque activities.[92]

IV. Implementation and Existing Models

We have identified broad functions of a third-party auditor in the ICO context. This section examines examples of existing models. Despite the promise of trust without intermediaries, as soon as the platform developed, intermediaries began to emerge. They both indicate the need for such intermediaries and suggest possible routes for integrating these functions.

1. Consulting and Auditing Services

[88] See M. Dell'Erba, 'Stablecoins in Cryptoeconomics. From Initial Coin Offerings (ICOS) to Central Bank Digital Currencies (CBDCS)' 51 *New York University Journal of Legislation and Public Policy*, Forthcoming, available at https://tinyurl.com/yhe6fmt6 (2019) (last visited 30 December 2019).

[89] Liquid collateral could be gold, USD or algorithmic mechanisms of stabilization. ibid.

[90] W. Suberg, 'Fractional Reserve Stablecoin Tether Only 74% Backed by Fiat Currency Say Lawyers' *Cointelegraph*, 30 April 2019, available at https://perma.cc/X2BT-5LSD (last visited 30 December 2019).

[91] The need for off-chain audits of collateral is related to proposals to use escrow accounts to structure the ICO market. See, E. da Cruz Rodrigues e Silva, *Legal framework of initial coin offerings* (2018) available at https://tinyurl.com/ykxww4ps (last visited 30 December 2019). See U. Rodrigues, 'Semi-Public Offerings? Pushing the Boundaries of Securities Law' *University of Georgia School of Law Legal Studies*, Research Paper no 2018-30, available at https://tinyurl.com/yekkvyj4 (last visited 30 December 2019).

[92] New York Attorney General, Letitia James, issued a preliminary injunction freezing a $900 million line-of-credit transaction indefinitely, fruit of a settlement agreement between Tether Holdings Limited, Tether Operations Limited, Tether Limited and Tether International Limited (Tether issuer) and the alleged controlling trading platform Bitfinex (operated by BFXNA Inc, NFXWW Inc, and iFinex, Inc). The latter holding a significant amount of Tether's reserves. The allegations involve fraud, commingling of assets and duty of loyalty violations. Press Release, 25 April 2019, available at https://perma.cc/QZ9F-MLZZ (last visited 30 December 2019).

The existing smart contract and blockchain auditing and consulting companies provide code auditing and sometimes white paper writing and consulting. The most common audit service is a code-based, technical one, based on security grounds. One of these examples is Zeppelin,[93] which provides a cybersecurity audit of smart contracts.

However, given uncertainty about how these assets and activity will be regulated, a technical audit may not be enough.[94] In this field, CodeLegit has established partnerships with law firms to provide a complete package of security, in cyberspace and the real world. Moreover, its services embrace dispute resolution through arbitration. The arbitrator is appointed by the parties and is both a technical and legal expert.[95]

IBCGroup, instead, assumes a propulsive role in the ICO process, offering consulting services that are not mere code audit but also legal audit. Among its services, IBCGroup provides fund liquidation and distribution, marketing and advertising, and white paper analysis.[96]

2. Oracles

The contradiction of the smart contracts technologies lies in the impossibility of entirely eradicating the intermediaries. Oracles are proof of it. While banning middlemen those startups have introduced middlewares which fulfill some of the same tasks of traditional intermediaries without the protection provided in centralized/regulated markets.

An oracle is a third party (individuals or programs) capable of introducing external data into the smart contract. Its role is determinative for the smart contracts' development due to its interaction with the real world persons and reaction to events. These external data need to be transferred in a safe and reliable manner. Indeed, in the decentralized environment, the oracle works in a decentralized way, though using multiple external sources, which are centralized. Coders associate centralization in this context, usually through banks, with lack of reliability[97] because it introduces vulnerabilities when assets are transferred

[93] See Zeppelin 'Zeppelin verifies that your decentralized systems work as intended by performing an audit. Our engineers fully review your system's architecture and codebase, then write a thorough report with actionable feedback for every issue found'. Zeppelin, 'Security Audits for High Impact Projects' available at https://perma.cc/8E53-P696 (last visited 30 December 2019).

[94] See CodeLegit, 'Mission: Technical Compliance' available at https://perma.cc/6AXR-64U4 (last visited 30 December 2019) ('All technological compliance audits are carried out by Codelegit as the technical auditor in cooperation with leading law firms as the legal auditor. This integrated approach of technical and legal expertise allows Codelegit to offer true LegalTech products').

[95] CodeLegit, 'CodeLegit White Paper on Blockchain Arbitration' available at https://perma.cc/EW92-P8PT (last visited 30 December 2019).

[96] IBCGroup, available at https://perma.cc/PE95-7PXA (last visited 30 December 2019).

[97] With especial attention to centralized applications such as Ripple. See P. Eze et al, 'A Triplicate Smart Contract Model Using Blockchain Technology' 1 *Disruptive Computing, Cyber-Physical Systems (CPS), and Internet of Everything (IoE)*, 4 (2017).

electronically. However, oracle intervention makes the transaction more reliable since it is linked to real world situations enhancing trust in the flux of information transmitted.[98] These could be described as mathematical auditors in the Ethereum platform.[99]

The most feasible way to bring into play a gatekeeper is through such oracles. The information received by means of white paper or voting decisions (commonly through blogs of prospective ICOs) can update, incorporate or decide the final outcome,[100] and the performance of a particular contract. Ambiguous terminology, as common in contracts, is exacerbated in smart contracts.[101] Essentially, the written language of coders in the white paper reflects computational thinking, which is unsuitable to provide enough information and disclosure of the risks of the enterprise.[102]

Solidity, one of the most common languages for smart contracts, allows for the use of oracles to reconcile the code with offline activity. It has a way to combine the mathematical proof of the working section or operational parts of the smart contract with the denotational parts claimed in the white paper (and other official sources such as ICO blogs) through oracles. The ICO auditor here assumes a specific role in the assessment of legal, technical and semantic terms. Then this new gatekeeper will exclude bad programs by using machine-checkable proof (the program of programs), to verify mathematically that the program is doing what it's supposed to do[103] and by validation of the results (a human input given via oracles).

a) ChainLink

ChainLink, an oracle enterprise, presents a mixture of blockchain parts based on smart contracts and offline/offchain parts of decentralized nature.[104] The combination of both and its aggregation in nodes supplies an important characteristic of the market makers/OTC operations, the meeting of demand and

[98] N. Attico, *Blockchain. Guida All'ecosistema. Tecnologia, business, società* (Milano: Guerini Next, 2018), 178.

[99] Up until now, the issue in decentralized technologies/blockchain consists in the missing economical (and legal) thinking and reasoning of the coders/programmers. In fact, the main flaws in cryptocurrencies belong to the lack of business models of these startups that create new projects on top of Ethereum without considering important factors of success such as a basic business plan or cash flow. T. Butler et al, 'Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop' 36 *Banking & Financial Services Policy Report*, 1 (2017).

[100] P. Ortolani, 'Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin' 36 *Oxford Journal of Legal Studies*, 595-629 (2016).

[101] P. De Filippi and A. Wright, n 2 above, 75.

[102] D. Di Sabato, 'Gli *smart contracts*: *robot* che gestiscono il rischio contrattuale' *Contratto e Impresa*, 379 (2017).

[103] C. Dannen, Introducing Ethereum and Solidity. Foundations of Cryptocurrency and Blockchain Programming for Beginners (Brooklyn, New York: Apress, 2017), 78.

[104] *ChainLink* has its native/intrinsic token. As per *ChainLink* features: 'Smart contracts require secure middleware to connect them to real world data. This external data will trigger the contract, creating the need for its high reliability', see n 83 above.

supply. The online parts of *ChainLink* generate requests of information (demand) while the offline parts decide whether or not to provide a reply. The nodes are reputational renters of this type of market, and frequently provide bond postings to assure the transparency of the transactions. There is a higher probability of the accuracy of information transmitted given its decentralized nature. However, their alleged reputation succumbs to opportunistic incentives that make it possible to copy the information from another node and receive the compensation in exchange.[105]

The provider of the input (human or not) can rely on the most common and useful mechanism of information in cryptos: CoinMarketCap,[106] which mirrors online databases that provide dissemination of information and disclosure of companies that raise money from the public.[107] The function of CoinMarketCap, besides sharing information about crypto enterprises, is to provide the trusted websites where the ICO takes place.[108]

b) Notaries

Another example of oracle enterprise are notaries. In civil law countries, long before the auditor, the *latin notary* accomplished the function of public officer and certifier. This type of legal intermediary has long provided reliability between contractual parties and encouraged multiparty transactions. Different from the auditor's role, this intermediary operates on behalf of both parties. Its superior role and reputation is monitored by a centralized body (in Italy the Consiglio Nazionale del Notariato) providing guidance in conflict of interest issues and a sanctioning apparatus that oversees the notary labor nationwide.[109]

In Italy, and in most civil law countries, the *latin notary* figure fulfils, at the

[105] N. Attico, n 98 above, 178-179.

[106] This website is a data provider with reliable and verified information regarding the current state of cryptocurrencies. Recently CoinMarketCap announced the launch of two cryptocurrency benchmark indices on Nasdaq Global Index Data Service, Bloomberg Terminal, Thomson Reuters Eikon. CMC Crypto 200 (CMC200) – cryptocurrencies under influence of Bitcoin –, and CMC Crypto 200 ex BTC (CMC200EX). CoinMarketCap Blog, 'CoinMarketCap cryptocurrency benchmark indices to launch on NASDAQ, Bloomberg and Thomson Reuters today' available at https://perma.cc/X5BQ-A5E3 (last visited 30 December 2019).

[107] Such as the SEC company filings EDGAR (Electronic Data Gathering, Analysis, and Retrieval system) available at https://perma.cc/64ED-66WP (last visited 30 December 2019), or the document section of the Borsa Italiana website, available at https://perma.cc/RCL6-BYMR (last visited 30 December 2019).

[108] The listing criteria for cryptocurrencies must be publicly and actively traded on at least two exchanges, supported by CoinMarketCap, and meet the definition of cryptocurrency as stated in Wikipedia. Those are the minimum requirements needed for cryptocurrencies' submission for consideration. The success of a submission for addition on CoinMarketCap further depends on community interest, trading volume, uniqueness, age of project. See, CoinMarketCap, 'Methology: Listing Criteria' available at https://perma.cc/8GMA-4BU8 (last visited 30 December 2019).

[109] The CNN enacts the code of professional responsibility/deontological rules binding for all notaries in Italy while the deputy body that guaranties rules compliance is the *Consigli Notarili Distrettuali*.

same time, the duties of a public officer and the performances of a private practitioner in the legal field.[110] Different from public officers, the notary's fees do not derive from the State but from private parties – as it is in the case of lawyers. Furthermore, notaries' reputation and independence is preserved by the lack of fixed clients – as repeat players that may condition the notary decision process –; the competition, which is limited due to the high bar to entrance through the notary exam and often the bar exam; the fixed taxes and state fees that they must carry on behalf of the State; plus civil and criminal liabilities, arising from the exercise of their role.[111]

Following this approach *Provable*[112] (previously known as *Oraclize*, an oracle company) provides the external data with a double authenticity proof. Provable is a smart contract that uses the TLS Notary technology, which ensures the truthfulness of the information acquired from an internet website in a specific moment, giving it firm date. The transaction master key is split between the auditee (Provable), the auditor (an open-source Amazon Machine Image) and the server.[113]

To summarize, in the case of oracles the transaction is not fully self-enforced since it is required to segregate funds until the condition in the contract is met and the person has not raised a complaint. In the case of dissatisfaction, the dispute is resolved by the oracle (the machine as in Provable), or a human acting as a third-party arbitrator, which would render a decision and release the escrowed accounts.

3. Certifiers

New types of technical blockchain auditing firms[114] have emerged to give confidence in the project and attract investors. Following this path, the crypto currency certification consortium (C4) is an online organization devoted to establishing cryptocurrency standards, namely minimum requisites of code compliance.[115] High profile current and past members include the inventor of

[110] A. Anselmi, n 70 above, 24.

[111] Hence, placing their activity within the general contracts for intellectual services (Art 2230 Italian civil code) for the safeguard of public trust. M. Di Fabio, 'Il notaio pubblico ufficiale e libero professionista, Notaio (diritto vigente)' *Enciclopedia del Diritto* (Milano: Giuffré, 1978), XXVIII.

[112] One of their main services is the certified processes. 'While authenticity proofs give transparency to the execution of our processes, external audits verify that our code does what it should do. We cover the entire audit trail - everything is being monitored from inception to execution'. Provable, 'Top Features: Certified Processes' available at https://perma.cc/JR44-ZMKB (last visited 30 December 2019).

[113] Provable, 'Authenticity Proofs Types: TLSNotary proof' available at https://perma.cc/CRA4-KYCZ (last visited 30 December 2019).

[114] ADBK Consultancy available at https://perma.cc/8DZH-E9EP (last visited 30 December 2019) and also available at https://perma.cc/C5WE-J97J (last visited 30 December 2019).

[115] As emphasized in their Mission 'The CryptoCurrency Certification Consortium (C4) establishes cryptocurrency standards that help ensure a balance of openness & privacy, security & usability, and trust & decentralization'. CrytoCurrency Certification Consortium, 'Mission' available at https://perma.cc/K73L-5W7R (last visited 30 December 2019).

Ethereum (Vitalik Buterin) who is on the Board of Directors, and the Chief Scientist at Provable (Piotr Piasecki) who was an advisor. C4 provides training and releases certifications such as the Certified Ethereum Developer (CED), which has a contract learning section in the second unit based on Solidity.

In this scenario, the trust reposed in the intermediary (enhanced by the technology) descends from the professional responsibility to which they are subject. Certifiers, as required by the C4, must follow a code of ethics. The status of certifier must be both earned (the courses last two years) and maintained. Compliance with these rules makes C4 one of the first examples of a self-regulatory organization in this area.[116]

The US context has developed its own self-regulatory organization for virtual commodities, the 'Virtual Commodities Association', (VCA), which sets forth industry standards in virtual commodity marketplaces, and best practices for SROs, potentially issuing reports. VCA was established by Gemini Trust Company (LLC) and is regulated under New York banking law. Gemini is, at the same time, the greatest US exchange and custodial services for cryptocurrencies (XBT, ETH, LTC, ZEC).[117] VCA's scope remains uncertain. Vain were the efforts of the Winklevoss brothers, founders of Gemini, to introduce bitcoin ETF on a regulated exchange – the proposal was rejected twice by the SEC.[118] However, the SEC's caution does not equate to a definitive rejection but allows the agency more time to consider its approach to cryptoassets.[119]

4. Dispute Resolution Systems

Dispute resolution systems, in blockchain, place themselves as intermediaries in the ex ante phase of design of the smart contracts. One of these examples is Aragon (Ticker: ANT).[120] Parties that use this platform for smart contracts submit

[116] Greater degree of expertise, innovatory possibilities, and information costs are benefits that self-regulatory organizations provide. A. Ogus, 'Rethinking Self-Regulation' 15 *Oxford Journal of Legal Studies*, 97-108 (1995). Indeed, those advantages are measured with the fact that there are not legally sanctioned rules imposed but social norms or 'reactive measures' ('*misure di reazione*'). See M. Ramajoli, 'Self regulation, soft regulation e hard regulation nei mercati finanziari' *Rivista della Regolazione dei Mercati*, 53 (2016).

[117] Only Bitcoin (XBT) was traded as futures in both the Chicago Board Option Exchange (CBOE) and the Chicago Mercantile Exchange (CME), but now put on hold – restraining any issuance. At the current moment there are no Bitcoin futures contracts; the last one listed expired last June. A. Osipovich, 'Cboe Abandons Bitcoin Futures' *Wall Street Journal*, available at https://perma.cc/JTK2-SABT (last visited 30 December 2019).

[118] K. Rooney and B. Pisani, 'Winklevoss twins bitcoin ETF rejected by SEC' *CNBC*, available at https://perma.cc/JQB2-MJH6 (last visited 30 December 2019).

[119] SEC, File no SR-CboeBZX-2019-004, Release no 34-85475, 'Notice of Designation of a Longer Period for Commission Action' 29 March 2019, and Release no 34-85896, 'Order Instituting Proceedings to Determine Whether to Approve or Disapprove a Proposed Rule Change to List and Trade Shares of the VanEck SolidX Bitcoin Trust' 20 May 2019.

[120] Aragon Network, 'White Paper' (2018), available at https://perma.cc/A8LA-VT9Z (last visited 30 December 2019).

their controversies to this specific jurisdiction posting a bond, using collateralized agreements. Aragon is similar to an arbitration court. However, instead of having arbiters or qualified persons in the decision making process, controversies are solved by jurors, namely, members of the network. They receive the appointment as jurors as long as they earn reputation by resisting bribery attacks.

The automatization in the response to a future event rests in the nature of the smart contract. In this scenario, contractual parties can settle in advance the scheme for the audit that could possibly reduce the need for dispute resolution (through the aggregation of information).[121] However, as in the DAO, the automatization via the smart contract does not guarantee the remedial effects of the legal contract.[122]

Another example in the blockchain scenario is Augur,[123] a smart contract based on predictive markets.[124] Augur's token REP stands for reputation. By predicting future events, this altcoin helps people in the blockchain community ferret out possible frauds and report on existing state of art in the blockchain. The probability of the outcome of the events relies on logarithmic market scoring rules.[125] The cost of its creation is relative and varies upon the amount of information aggregated in order to predict the outcome, regardless of the frequency or number of participants that give information. Oracles in smart contracts by giving the input of (human) information assess the honesty of the information by mathematical models.[126]

Augur can assume the role of an alternative arbitration court or alternative juries.[127] These new technologies are already in use in research,[128] and some argue that they can also work as decentralized courts, or better said juries, because the importance is not to have a proper juror, especially in private litigation, but

[121] C. Catalini et al, n 55 above, 7.

[122] K. Werbach, 'Trust, But Verify: Why the Blockchain Needs the Law' 33 *Berkeley Technology Law Journal*, 489, 545 (2018).

[123] Ticker: REP.

[124] It works by creating an event tied to the acquisition of the outcome token (two or more depending on the event outcomes) – which reflects posting a bond –, and the squared token distribution. So that the payment of the winner token occurs through the amount received by the loser token (N. Attico, n 85 above, 131).

[125] Different from Augur is the Gnosis, (Ticker: GNO) https://perma.cc/KV6Z-FLDS (last visited 30 December 2019), a different type of Ethereum based prediction market that operates on the futarchy theory, the ability to create laws employing solely market predictive forces in the aggregation of information. At the same time, it disregards any external input on the modality to reach a particular objective, the event that triggers a particular decision to reach that objective is fully market based. Essentially, employing the measurement of welfare by a cost benefit analysis it is possible, for example, to remove managers. R. Hanson, 'Votes, Values, but bet beliefs' (2013) available at https://perma.cc/7WE7-RBT3 (last visited 30 December 2019).

[126] R. Hanson, 'Logarithmic Market Scoring Rules for Modular Combinatorial Information Aggregation' 1 *Journal of Prediction Markets*, 2-3 (May 2003).

[127] See K. Werbach, n 122 above, 549 and P. De Filippi and A. Wright, n 2 above, 75.

[128] A.Z. Robertson & A.H. Yoon, 'You Can Get What You Pay For: An Empirical Examination of the Use of MTurk in Legal Scholarship' 72 *Vanderbilt Law Review*, 1633 (2019).

to deliver the ruling, a task that is not necessarily better performed by in-person jurors.

V. Conclusion

'(T)ales of fortunes made and dreamed to be made' characterize the ICO market.[129] ICOs push 'financial disruption' and the entry of new investors driven by 'passion for cryptoassets, blockchain, altcoins, and distributed ledger technology'.[130] And the underlying smart contracts promise a new decentralized world of consensus that makes traditional intermediaries obsolete.

The broadening of the ICO investor population to investors who are not code-literate, however, has put pressure on the market. Without advocating the replication of old financial structures, this article identifies areas of continuing need for some intermediation. In explaining this scenario of ICOs, we tried to highlight the necessity of bridging information from the code, the white paper and other human readable information, and the offline world.

The activities of the new ICO intermediary can be understood as falling into three categories: translation, reconciliation, and verification. First, there is a need for a third-party intermediary to translate code. A code reader and translator could inform investors of the important encoded terms of the ICO. The second role for a new ICO intermediary is to reconcile the code with other promises. It would look at both the code and the other materials directed at investors to determine whether they correspond. It would determine to what extent the code reflects the promises advertised and disseminated through the means of information that induced investors to take part in the venture – the white papers, websites, podcasts, social media, etc. Finally, the ultimate ICO gatekeeper's task is to verify the offline/offchain information from the real world relevant for its impact on the ICO. All three functions of a new ICO intermediary would support confidence in the market.

[129] US Securities and Exchange Commission (US SEC), n 7 above.
[130] See, Flippening available at https://perma.cc/64RK-ZU65 (last visited 30 December 2019).