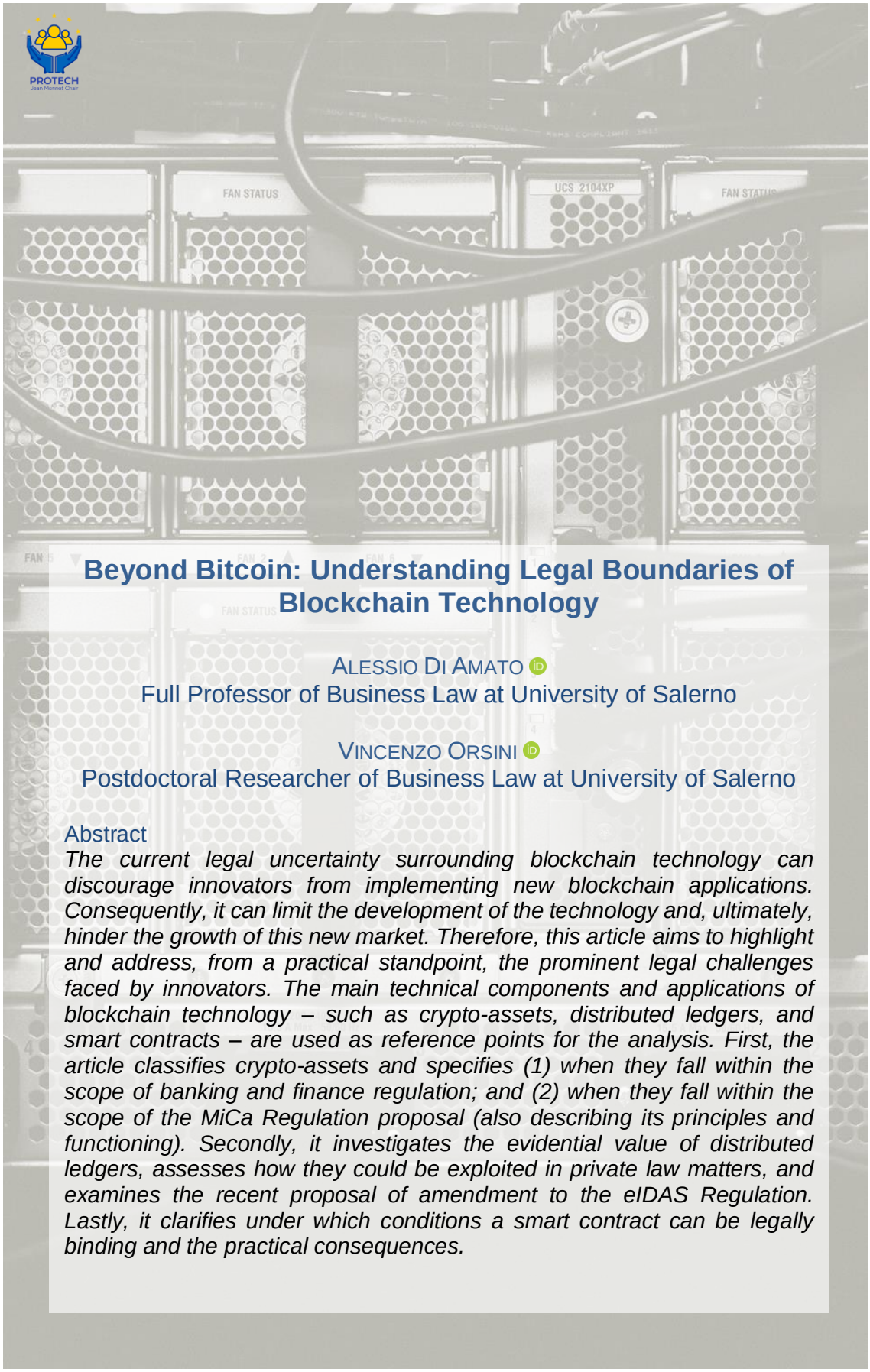
Di Amato A, Orsini V, 'Beyond Bitcoin: Understanding Legal Boundaries of Blockchain Technology ' (2022) 1 EJPLT, 110-131.
DOI: https://doi.org/10.57230/EJPLT221ADAVO

EJPLT
ISSN 2704-8012



Beyond Bitcoin: Understanding Legal Boundaries of Blockchain Technology

ALESSIO DI AMATO
Full Professor of Business Law at University of Salerno

VINCENZO ORSINI
Postdoctoral Researcher of Business Law at University of Salerno

Abstract

The current legal uncertainty surrounding blockchain technology can discourage innovators from implementing new blockchain applications. Consequently, it can limit the development of the technology and, ultimately, hinder the growth of this new market. Therefore, this article aims to highlight and address, from a practical standpoint, the prominent legal challenges faced by innovators. The main technical components and applications of blockchain technology – such as crypto-assets, distributed ledgers, and smart contracts – are used as reference points for the analysis. First, the article classifies crypto-assets and specifies (1) when they fall within the scope of banking and finance regulation; and (2) when they fall within the scope of the MiCa Regulation proposal (also describing its principles and functioning). Secondly, it investigates the evidential value of distributed ledgers, assesses how they could be exploited in private law matters, and examines the recent proposal of amendment to the eIDAS Regulation. Lastly, it clarifies under which conditions a smart contract can be legally binding and the practical consequences.

Keywords: blockchain law, crypto-assets; MiCa Regulation; distributed ledgers; eIDAS; smart contracts.

Introduction.[1]

Scholars started investigating bitcoin, blockchain and related technologies in 2014, no later than five years after the launch of the bitcoin protocol.[2] Ever since then, the literature in the field has rapidly increased due to the capability of blockchain technology of ensuring security and transparency in no-trust environments. Even though the general public focused mainly on cryptocurrencies, computer scientists, entrepreneurs, and academics, realized that blockchain technology could have had many more applications. The base assumption is that, at its core, blockchain is 'a specific type of database that uses certain cryptographic functions to achieve the requirements of data integrity and identity authentication'.[3] Therefore, blockchain technology shall primarily be intended as a technical tool to ensure the reliability of the information contained in a database, a tool that could have multiple applications in several industries other than banking and finance.[4]

While traditional centralised databases for registering and transferring assets tend to be expensive and inflexible – since they need to be controlled or supervised – the blockchain could significantly reduce infrastructure costs by adopting a ledger distributed among a peer-to-peer network. However, blockchain technology in its purest form (e.g., bitcoin) ignores external legal requirements, and shall be integrated with new features to become compliant with the law.[5] Moreover, the legal system itself is not prepared for a paradigm shift from centralised to distributed systems.[6] Hence, developers and organizations

[1] This paper is the result of the joint work of Prof. Alessio Di Amato and Dr. Vincenzo Orsini, that defined together its aim, structure, and content. The drafting effort, however, was divided between Prof. Di Amato, that wrote the introduction, and Dr. Orsini, that wrote the following paragraphs.

[2] For a systematic review of blockchain research in the business literature, see J Frizzo-Barker and others, 'Blockchain As A Disruptive Technology For Business: A Systematic Review' (2020) 51 International Journal of Information Management, 2.

[3] J Bacon and others, 'Blockchain Demystified: A Technical And Legal Introduction To Distributed And Centralised Ledgers' [2018] Richmond Journal of Law & Technology, 5-6.

[4] UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Block chain' (2016), 4.

[5] C Reed and others, 'Beyond Bitcoin—Legal Impurities And Off-Chain Assets' (2018) 26 International Journal of Law and Information Technology, 160-162.

[6] The decentralised nature of blockchain technology makes it difficult not only to apply the existing regulation, but also to understand how the blockchain can be regulated in an effective way. See, G P La Sala, 'Intermediazione, Disintermediazione, Nuova Intermediazione: I Problemi Regolatori', *Diritto del Fintech* (CEDAM 2020), 7-8. Nonetheless, authors generally believe that the blockchain will follow the same regulatory curse of the Internet since also the latter was difficult to regulate at the beginning. Meanwhile, it seems that the blockchain is governed by the private and technical set of rules generated by smart contracts and decentralized organization, that seems to constitute a new 'lex cryptographia'.
See, A Wright and P De Filippi, 'Decentralized Blockchain Technology And The Rise Of Lex Cryptographia' [2015] SSRN Electronic Journal, 51-56; P Hacker and others, *Regulating Blockchain: Techno-Social And Legal Challenges* (Oxford University Press 2019), 16-19; K Becker, 'Blockchain *Matters*—Lex Cryptographia And The Displacement Of Legal Symbolics And Imaginaries' (2022) 33 Law and Critique, 118-122.

could find it extremely difficult and expensive to comply with legal and regulatory requirements. Here stands the main obstacle for innovators: those willing to embrace blockchain technology and implement new solutions for their businesses may have hard times understanding the legal boundaries and, ultimately, may disregard the idea completely.

Thus, this article aims to provide a framework for better understanding those legal and regulatory requirements and navigate the legal system. The analysis will be structured using the main technical components and applications of blockchain technology (such as tokens, distributed ledgers, and smart contracts), as reference points. First, the article will classify crypto-assets, clarify when they fall within the scope of banking and finance regulation and try to specify if other laws could find application. Secondly, it will investigate the evidential value of the distributed ledger for registering and transferring assets and highlight the current obstacles to the adoption of blockchain for assets that exist outside the blockchain itself (off-chain assets). Lastly, it will analyse the legal value of smart contracts and their interaction with traditional contracts. Considering that smart contracts are, essentially, computer programs that run on a blockchain, it is necessary to define under which conditions they can be legally binding and how can they be enforced.

1. Brief Notes on Regulated Crypto-assets.

Blockchain technology allows to create, in a digital environment, rival goods (i.e., goods that may only be possessed by a single user at a time).[7] Those goods are named crypto-assets and, in their purest form, are nothing more than 'a chain of digital signatures' and were meant to be used as a payment system.[8] Notwithstanding, tokens are not all the same, being primarily the developer that defines function and features of a token or a set of tokens. The market is continuously evolving and counts a wide variety of applications and cases.[9] In fact, since the introduction of the bitcoin protocol, many types of crypto-assets have been developed, ranging from stable coins, that are crypto-assets whose value refers to fiat currencies or other assets, to non-fungible tokens (NFTs), that are being used to commodify digital assets, like images or even tweets.[10]

[7] Most goods in economics are rival because they cannot be used by different people at the same time (e.g., a hammer), whereas data (e.g., a digital image) can normally be used by any number of people simultaneously, without being diminished. This is the reason why, before the emergence of blockchain technology, digital goods were considered necessarily non-rival goods. See, C I Jones and C Tonetti, 'Nonrivalry And The Economics Of Data' (2020) 110 American Economic Review, 2819-2820.

[8] The purpose of the bitcoin protocol emerges from the title of the white paper itself, that suggests the idea of a new electronic payment system. See, S Nakamoto, 'Bitcoin: A Peer-To-Peer Electronic Cash System' (2009) <https://bitcoin.org/bitcoin.pdf> accessed 1 July 2018, 2.

[9] For a taxonomic deconstruction of blockchain-based technologies, see P Tasca and C J Tessone, 'A Taxonomy Of Blockchain Technologies: Principles Of Identification And Classification' (2019) 4 Ledger, 8.

[10] A non-fungible token is a crypto-asset that represents an intangible and unique digital item like a particular piece of digital art, music, video, etc. Differently from other crypto-assets, that are standardized, NFTs are unique and not fungible. The market for NFTs recently boomed [The EU Blockchain Observatory & Forum, 'Demystifying Non-Fungible Tokens' (2021) 13] raising several questions among legal scholars. See, G Frezza, *Arte E Diritto Fra Autenticazione E Accertamento* (Edizioni scientifiche italiane 2019); T M Evans, 'Cryptokitties, Cryptography, and Copyright' (2019) 47 AIPLA Q J, 219; I E Okonkwo, 'NFT, Copyright And Intellectual Property Commercialization' (2021) 29 International Journal of Law and Information Technology; A Guadamuz, 'The Treachery Of Images: Non-Fungible Tokens And Copyright' (2021) 16 Journal of

Because of the variety of crypto-assets, there may be a lack of clarity as to the legal and regulatory framework that finds application in each different case. On one hand, 'there is not a "one size fits all" solution when it comes to legal qualification'.[11] Depending on function and features of a certain crypto-asset, its legal qualification may be different and, consequently, the applicable legal regime. On the other hand, many crypto-assets are still unregulated in the EU. Even though some Member States developed bespoke laws for crypto-assets, and the EU is currently working on a legal framework in the areas of tokenisation and smart contracts, the only European law that applies transversally to any kind of token is the fifth anti-money laundering Directive (hereinafter, AMLD5).[12] It is possible, nevertheless, to identify certain types of crypto-assets that are, already at this stage, regulated; and to try to anticipate the outlines of the European legal framework on crypto-assets.

Preliminarily, it is important to highlight is that the terms 'token', 'cryptocurrency', 'virtual currency' and 'crypto-asset' are often used improperly as synonyms. The word 'token' has mainly a technical meaning and does not have any legal connotation. It can be used to describe the entire family of technical instruments issuable via the blockchain (cryptocurrencies, for instance, are only a species of tokens).[13] Conversely, virtual currencies have been explicitly defined by the fifth anti-money laundering Directive as a 'digital representation of value […] which can be transferred, stored and traded electronically' [art. 3(18)] – a broader definition that disregard completely the adoption of blockchain technology. In other words, virtual currencies are not necessarily issued in the technical form of tokens, and the notion does not encompass every type of token. For this reason, here it will be preferred the term 'crypto-asset', a term that has been recently adopted in the EU Regulation proposal on Markets in Crypto-assets (hereinafter, MiCa) to identify any type of token, issued using blockchain technology, that is representative of value or rights [art. 3(1)(2)].

Moreover, it is worth mentioning that while some blockchains, like bitcoin, are constituted solely of crypto-assets that have been mined (i.e., produced validating transactions), some others offer part of them for sale. In the first case, every crypto-asset is previously produced via mining and, only after, sold on a secondary market such as an exchange platform. In the latter case, the developers of a blockchain presale some crypto-assets to promote their network and fund their project:[14] this procedure is called Initial Coin Offering, or ICO.[15] A

Intellectual Property Law & Practice; J A T Fairfield, 'Tokenized: The Law Of Non-Fungible Tokens And Unique Digital Property,' (2022) 97 Indiana Law Journal; S Hecker and M Vanzetti, 'L'«Originale» Nell'arte Come Concetto Mutevole Nel Tempo E Nell'ambito Della Sua Attuale Tutela' [2022] Arte e Diritto; C Trevisi, R M Visconti and A Cesaretti, 'Non-Fungible Tokens (NFT): Business Models, Legal Aspects, And Market Valuation' [2022] Media Laws.

[11] ESMA, 'Advice On Initial Coin Offerings And Crypto-Assets' (2019), 4.

[12] European Union Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43.

[13] 'Crypto Basics' (*Coinbase*, 2022) <https://www.coinbase.com/it/learn/crypto-basics/what-is-a-token> accessed 5 September 2022.

[14] In other words, the developer of a project issue tokens that offers in exchange for other cryptocurrencies like BTC or ETH. For an outline of ICOs, see: European Parliamentary Research Service, 'Understanding Initial Coin Offerings. A New Means Of Raising Funds Based On Blockchain' (2021).

[15] The legal challenges of ICOs have been addressed by many authors. Among others, see: I M Barsan, 'Legal Challenges Of Initial Coin Offerings (ICO)' (2017) 3 Revue Trimestrielle de Droit Financier; J Enyi and

programmer, for instance, could decide to finance the development of a software project by offering for sale some of the coins that, in the future, he will accept as payment. In this way, he will be able to directly profit from the issuance of crypto-assets and employ those resources in the project.

The sharp rise of ICOs imposed financial supervisory authorities from all around the globe to clarify if, and when, securities laws find application. The first investigation in the matter dates back to 2017, when the U.S. Securities and Exchange Commission (hereinafter, SEC) published its report about the Decentralized Autonomous Organization, or DAO, which represents a cornerstone in the brief ICO history.[16] The SEC stated, for the first time, that certain crypto-assets can fall within the scope of US securities laws and regulations if they pass the 'Howey test', thereby qualifying as 'investment contracts'.[17] In order to pass the test, a crypto-asset should represent '[1] an investment of money in a common enterprise [2] with a reasonable expectation of profits [3] to be derived from the entrepreneurial or managerial efforts of others'.[18] As a consequence, those who offer and sell 'security-like' crypto-assets must comply with the laws regarding public offerings, and those who engage in the activities of an exchange must register as national securities exchanges.[19]

Since the test should be undertaken on a case-by-case basis, its correct interpretation become crucial for understanding the nature of any crypto-asset. Consequently, the SEC decided to release a public statement containing a 'Framework for "Investment Contract" Analysis of Digital Assets' in which it

---

Y Le Ngoc Dang, 'Regulating Initial Coin Offerings ("Cryptocrowdfunding")' [2017] Butterworths Journal of International Banking and Financial Law; P Hacker and C Thomale, 'Crypto-Securities Regulation: Icos, Token Sales And Cryptocurrencies Under EU Financial Law' (2018) 15 European Company and Financial Law Review; D Boreiko, G Ferrarini and P Giudici, 'Blockchain Startups And Prospectus Regulation' (2019) 20 European Business Organization Law Review; D A Zetzsche and others, 'The ICO Gold Rush: It's A Scam, It's A Bubble, It's A Super Challenge For Regulators' (2019) 60 Harvard International Law Journal; F Annunziata, 'Speak, If You Can: What Are You? An Alternative Approach To The Qualification Of Tokens And Initial Coin Offerings' (2020) 17 European Company and Financial Law Review; P Maume, 'Initial Coin Offerings And EU Prospectus Disclosure' (2020) 31 European Business Law Review.

[16] In brief, the DAO was meant to be a virtual investment fund executed on a blockchain. To raise funds among investors, its promoters sold "DAO Tokens", crypto-assets that would have granted voting power in the DAO and given access to future earnings. Unfortunately, before the DAO could start operating, a hacker used a flaw in the DAO software to steal part of the funds previously raised (valued approximately $150 millions) and led the SEC to start an investigation to determine why so many people were allowed to invest in something that so closely resembled a company. Since Ethereum was forced to restore DAO investors, the SEC decided not to prosecute the promoters of the DAO - Securities Exchange Commission, 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO', Release n. 81207 of 25th July 2017.

[17] *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

[18] *Ibid.*

[19] Cryptocurrency laws and regulations, at this stage, vary state by state. Some state governments have adopted a favourable approach to crypto-related activities, exempting crypto-assets from state securities laws or banking laws, while others adopted a more restrictive approach, requiring some sort of authorization (e.g., 'BitLicense' in New York). For an overview, see: 'Cryptocurrency Laws And Regulations By State' (*Bloomberg law*, 2022) <https://pro.bloomberglaw.com/brief/cryptocurrency-laws-and-regulations-by-state/> accessed 29 June 2022. At the Federal level, up until now, initiatives have been relegated to administrative levels (SEC, CFTC, IRS, OCC, FinCen). Different bills, however, have been proposed but still have not passed: (i) the 'Token Taxonomy Act', that specifies that digital tokens, such as those used in virtual currencies, are not securities for regulatory purposes and provides for the tax treatment of virtual currencies; (ii) the 'Consumer Safety Technology Act', which requires various agencies to explore the use of emerging technologies in the context of consumer products and safety; and lately (iii) the 'Lummis-Gillibrand Responsible Financial Innovation Act', whose ambitious aim is to define guidelines for the crypto-assets space, providing also a taxonomy and specific rules for stable-coins.

explained the elements of the test.[20] It specified, first, that the definition of 'money invested' is broad and includes any type of consideration (including cryptocurrencies); secondly, that both dividends, periodic payments and capital gains can be considered as 'profit'; and thirdly, that the 'reliance on the effort of others' should assessed through an objective inquiry. This inquiry should focus on the 'reasonableness' of the expectation of the investor, and on the 'essentiality' of the managerial effort of promoters, sponsors or third parties (to be essential, it should affect the success or failure of the initiative). Ultimately, the SEC clarified that 'price appreciation resulting solely from external market forces (such as general inflationary trends or the economy) impacting the supply and demand for an underlying asset generally is not considered "profit" under the Howey test'.

In the meantime, the European Securities and Markets Authority (ESMA) warned that 'where the coins or tokens qualify as financial instruments it is likely that the firms involved in ICOs conduct regulated investment activities'. [21] Besides, it highlighted that it is duty of the firms to consider if some EU rules – such as the Prospectus Directive[22], the Markets in Financial Instruments Directive II (hereinafter, MiFID II)[23], the Alternative Investment Fund Managers Directive (AIFMD)[24], or the Fourth Anti-Money Laundering Directive (AMLD4)[25] – may apply. Nonetheless, it did not clarify when a crypto asset qualifies as a security under the EU law.

The issue was faced more recently by the ESMA when it released an 'Advice on Initial Coin Offerings and Crypto-Assets'.[26] There, it confirmed the applicability of the EU financial rules to crypto-assets that qualify as 'transferable securities' or other types of MiFID financial instruments. As known, the EU law does not provide a distinctive definition of 'financial instrument' but, instead, lists those who fall into the category at Section C of Annex I of the MiFID II: 'transferable securities', 'money market instruments', 'units in collective investment undertakings', and several derivative instruments. Consequently, those who are involved in ICOs should pay close attention to the list and, particularly, to the interpretation of 'transferable securities'.[27]

---

[20] Securities and Exchange Commission, 'Framework For "Investment Contract" Analysis' (2019).

[21] The Supervisory Authority issued two different warnings: one on the risks of ICOs for investors and another one on the rules applicable to firms involved in ICOs - European Securities and Markets Authority, 'Esma Highlights ICO Risks For Investors And Firms' (2017) <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms> accessed 8 June 2022.

[22] European Council Directive 2003/71/EC of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC [2002] OJ L 345/64.

[23] European Union Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L 173/349.

[24] European Union Directive 2011/61/EU of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 [2011] OJ L 174/1.

[25] European Union Directive 2015/849/EU 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 648/2012 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 L 141/73.

[26] ESMA, 'Advice On Initial Coin Offerings' (11).

[27] The qualification of crypto-assets as transferable securities is a highly debated topic. See, I M Barsan, 'Legal Challenges' (15); P Hacker and C Thomale, 'Crypto-Securities Regulation'(15); D Boreiko, G Ferrarini and P Giudici, 'Blockchain Startups' (15); F Annunziata, 'Speak, If You Can' (15); P Carriére, 'Le "Criptovalute" Sotto La Luce Delle Nostrane Categorie Giuridiche Di "Strumenti Finanziari", "Valori Mobiliari"

As noted by some authors, the definition of 'transferable security' given by Article 4(1)(44) of MiFID II follows formal and substantive criteria.[28] Formally, it includes 'those classes of securities which are negotiable on the capital market'. Hence, it requires the crypto asset to be standardized, transferable and negotiable. Substantially, it exemplifies transferable securities with traditional assets such as shares, bonds, and some derivatives. Thus, even though some authors disagree[29], it is commonly accepted that crypto-assets should resemble the examples provided by the law in order to be considered as transferable securities. However, it is worth noticing that a survey among financial supervisory authorities revealed that the actual classification of crypto-assets as transferable securities can differ among Member States because of the different implementation of the EU law at national level.[30]

What is clear is that, depending on how they are structured, crypto-assets may fall outside of the scope of the existing rules and hence outside of the regulated space. Crypto-assets that do not qualify as financial instruments, at this stage, are only partially regulated in the EU. Although some Member States, such as Malta and France, established bespoke regimes both for issuers and third-party service providers (e.g., exchanges or custodians), the EU law only focuses on anti-money laundering measures. [31] In fact, the AMLD5 brings exchange platforms and wallet providers under the control of the national competent authorities and imposes on them Customer Due Diligence obligations.[32] They must, therefore, identify customers and monitor their business relationships in order to report any suspicious activity so that competent authorities can intervene.

For this reason, many started to classify crypto-assets in such a way as to

E "Prodotti Finanziari"; Tra Tradizione E Innovazione' [2019] Rivista di Diritto Bancario; K Langenbucher, 'Building A Capital Market – The Final Report Of The High Level Forum On The EU Capital Market Union' (2020) 17 European Company and Financial Law Review; A Minto, 'The Legal Characterization Of Crypto-Exchange Platforms' (2021) 22 Global Jurist. Some authors argue that cryptocurrencies should be considered as money or intangible goods: C Pernice, *Digital Currency E Obbligazioni Pecuniarie* (Edizioni scientifiche italiane 2018); T de Graaf, 'The Qualification Of Bitcoins As Documentary Intangibles' (2019) 27 European Review of Private Law; M Cian, 'La Criptovaluta Alle Radici Dell'Idea Giuridica Di Denaro Attraverso La Tecnologia: Spunti Preliminari' (2019) 72 Banca borsa tit. cred.; V Orsini, 'Della Natura Giuridica Delle Criptovalute' [2021] Diritto del mercato assicurativo e finanziario.

[28] P Hacker and C Thomale, 'Crypto-Securities Regulation'(15), 645-696.

[29] D Boreiko, G Ferrarini and P Giudici, 'Blockchain Startups' (15), 678-680.

[30] ESMA, 'Advice On Initial Coin Offerings' (11).

[31] Outside the EU, Liechtenstein has also adopted a bespoke regime for crypto-assets (the Token and Trusted Technology Service Provider Act).

[32] The early intervention in the anti-money laundering space was determined by a case that gained the attention of the Financial Action Task Force (FATF): on Tuesday 1st October 2013, the US authorities closed 'Silk Road', the most famous online black-market in the world. It sold any kind of illegal goods, such as drugs and weapons, and was famous for being completely anonymous. Silk Road was situated in the dark web and guaranteed non-traceability of the users by allowing payments only via Bitcoin. For the full story, see: J Bearman, 'The Rise And Fall Of Silk Road, Part I' [April 2015] Wired <https://www.wired.com/2015/04/silk-road-1/> and, 'The Rise And Fall Of Silk Road, Part II' [May 2015] Wired <https://www.wired.com/2015/05/silk-road-2/> both accessed 28 June 2022. The event alerted the FATF that, in 2014, published a report where it warned of the risk posed by virtual currencies and, in 2015, published its guidance for a risk-based approach to virtual currencies: Financial Action Task Force, 'Guidance For A Risk-Based Approach to Virtual Currencies' (FATF 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 28 June 2022. The EU took action immediately afterwards, starting the process that led to the AMLD5: EU Commission, 'Communication COM (2016) 50 to the Council and the Parliament on an Action Plan to further step up the fight against the financing of terrorism' (2 February 2016).

distinguish ‘security like tokens’ from ‘currency like tokens’ (like Bitcoin).[33] Nonetheless, the most adopted classification[34] is probably the one developed by FINMA, the Swiss financial market supervisory authority.[35] It identified three categories of crypto-assets by economic function: cryptocurrencies, security tokens and utility tokens. Cryptocurrencies are tokens that ‘have no further functions or links to other development projects [and may] become accepted as a means of payment’.[36] Their scarce supply should help them retain value and, consequently, make them employable as electronical payment instruments (hence the name cryptocurrencies) but their volatility often prevents them to achieve this function.[37] Security tokens are those that resemble traditional financial instruments (like shares, bonds or derivatives) and, as such, fall within the scope of securities laws.[38] The category of utility tokens, instead, is residual and includes every crypto-asset that does not fall within the first two categories.[39]

2. The MiCA Regulation Proposal.

Risks and opportunities of this unregulated space, that includes both cryptocurrencies and utility tokens, led the EU Commission to adopt, in 2020, a ‘digital finance package’ composed of both a strategy and legislative proposals on crypto-assets and digital resilience.[40] On one side, the Commission recognized that the lack of regulation, combined with the market expansion, poses significant risks on the holders of crypto-assets in terms of investor protection, market integrity and financial stability.[41] Furthermore, bespoke national laws on crypto-assets could determine market fragmentation, hinder the

[33] The distinction was identified by I M Barsan, 'Legal Challenges’ (15), 56-59.
[34] Because of the expansion of the crypto-assets market, many other classifications have been developed through the years as to consider also ‘stable-coins’, ‘central bank digital currencies’ and ‘non-fungible tokens’. The British Financial Conduct Authority, for instance, identifies: (i) exchange tokens; (ii) utility tokens; (iii) security tokens; (iv) e-money tokens. See, FCA, 'Guidance On Cryptoassets' (2019) PS19/22. The Bank of Italy, instead, classifies: (i) virtual currencies; (ii) payment tokens, that include (a) stable-coins, (b) central bank digital currencies, and (c) non-convertible digital coins; (iii) security tokens; (iv) utility tokens. See, C Gola and A Caponera, 'Aspetti Economici E Regolamentari Delle «Cripto-Attività»' (2019) 484 Questioni di Economia e Finanza.
[35] FINMA, 'Guidelines For Enquiries Regarding The Regulatory Framework For Initial Coin Offerings (ICO)' (2018).
[36] FINMA, 'FINMA Publishes ICO Guidelines (Press Release)' (2018) 2.
[37] ECB Crypto-Assets Task Force, 'Crypto-Assets: Implications For Financial Stability, Monetary Policy, And Payments And Market Infrastructures' (2019) ECB Occasional Paper Series No 223, 9.
[38] FINMA, 'Guidelines’ (35) 5-6; ESMA, ‘Advice On Initial Coin Offerings’ (11) 18-21.
[39] FINMA, 'Guidelines’ (35) 5.
[40] Even though the MiCa Regulation is still not effective, some authors have already commented the proposal: D A Zetzsche and others, 'The Markets In Crypto-Assets Regulation (MICA) And The EU Digital Finance Strategy' [2020] SSRN Electronic Journal; F Annunziata, 'Verso Una Disciplina Europea Delle Cripto-Attività. Riflessioni A Margine Della Recente Proposta Della Commissione UE' [2020] Diritto bancario. Approfondimenti; V P Carrière, 'Crypto-Assets: Le Proposte Di Regolamentazione Della Commissione UE. Opportunità E Sfide Per Il Mercato Italiano' [2020] Diritto bancario. Approfondimenti; R Lener and L Furnari, 'Cripto-Attività: Prime Riflessioni Sulla Proposta Della Commissione Europea. Nasce Una Nuova Disciplina Dei Servizi Finanziari “Crittografati”?' [2020] Diritto bancario. Approfondimenti; M Lucchesi, 'Crypto-Assets: The Draft "MICA" Regulation Aims For A New EU Regulation' (2021) 179 International Business Law Journal.
[41] EU Commission, ‘Communication COM/2020/591 final to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions on an Action Plan on a Digital Finance Strategy for the EU’ (24 September 2020) §4.4.

development of a digital single market, and limit the possibilities for businesses to scale up at a European level.[42] On the other side, the EU saw the opportunity to create a safe and friendly environment for blockchain start-ups by removing legal uncertainty, reducing operating costs and boost investors' confidence in the market.[43]

The digital finance package is aimed at regulating those crypto-assets which are not already governed by EU legislation and at proposing a pilot regime for market infrastructures that are considering the idea of adopting blockchain technology to clear and settle transactions.[44] The package, therefore, comprises different legislative proposals:

- Regulation on Markets in Crypto-assets (hereinafter, MiCa)[45];
- Directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341[46] – as to include crypto-assets;
- Regulation on a pilot regime for market infrastructures based on distributed ledger technology[47];
- Regulation on digital operational resilience for the financial sector (DORA)[48].

Security-like crypto-assets will still be governed by financial laws (in the clarified version), while the others will be regulated by the MiCa Regulation. On one side, to clarify the existing legal framework, the proposed Directive specifies that the category of 'financial instruments' defined by the MiFID II includes such instruments 'issued by means of distributed ledger technology' [art. 6 (1)]. On the other side, the MiCa Regulation excludes from its material scope those financial instruments [art. 2 (2)(a)] and requires firms to produce a legal opinion stating that their crypto-assets cannot be qualified as such [art. 16 (2)(d)]. Furthermore, the MiCa Regulation excludes from its scope crypto-assets issued by central banks acting in their monetary authority capacity [art. 2 (3)(a)].

The MiCa Regulation is mainly focused on stable coins, that recently emerged as a peculiar type of crypto-assets which seek to solve the volatile nature of cryptocurrencies.[49] Facebook and many players of the financial industry, for instance, started developing a stable coin pegged to several fiat currencies and

---

[42] *Ibid.* §4.1.
[43] *Ibid.* §4.2.
[44] *Ibid.*
[45] Proposal for a European Union Regulation COM/2020/593 final of 24 September 2020 on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [2020].
[46] Proposal for a European Union Directive COM/2020/596 final of 24 September 2020 amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341[2020].
[47] Proposal for a European Union Regulation COM/2020/594 final of 24 September 2020 on a pilot regime for market infrastructures based on distributed ledger technology [2020].
[48] Proposal for a European Union Regulation COM/2020/595 final of 24 September 2020 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 [2020].
[49] For an introduction to the topic, see: A Delivorias, 'Stablecoins. Private-Sector Quest For Cryptostability' [2022] European Parliamentary Research Service. On the legal issues posed by stable-coins, see: D W Arner, R Auer and J Frost, 'Stablecoins: Risks, Potential And Regulation' (2020) 905 BIS Working Papers; M Dell'Erba, 'Stablecoins In Cryptoeconomics. From Initial Coin Offerings (Icos) To Central Bank Digital Currencies (CBDC)' (2020) 22 New York University Journal of Legislation and Public Policy; J Cheng, 'How To Build A Stablecoin: Certainty, Finality, And Stability Through Commercial Law Principles' [2020] Berkeley Business Law Journal.

usable across the internet via social media platforms.[50] The mechanics of stable coins are not uniform: some are pegged to one or more fiat currencies or commodities (off-chain collateralized), some are pegged to other cryptocurrencies (on-chain collateralized), some implement algorithmic tools that adapt the supply to the market price (non-collateralized), and some others use hybrid or alternative mechanisms.[51] By incorporating features designed to stabilise their value over time, stable coins may reach wider adoption as payment instruments and, ultimately, pose a serious threat to financial stability.[52] The idea that the Euro, as payment system, may be eventually challenged by one or more stable coins led the EU to take action and regulate this space.

For this reason, the MiCa Regulation proposal essentially establishes two different regimes, a general one and another one specifically tailored on stable coins. Crypto-assets, in general, are defined as 'a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology' [art. 3 (1)(2)]. A definition that should be interpreted 'as widely as possible' in order to encompass every unregulated crypto asset (Recital 8). Two specific subcategories of stable coins are then defined and regulated separately: (1) 'asset-referenced tokens', which are stable coins pegged to 'several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets'; and (2) 'e-money tokens' which are stable coins pegged to a single fiat currency.[53] Algorithmic stable coins, that automatically adjust the supply according to the demand, should not be considered as asset-referenced tokens (Recital 26).

The main aim of the general regime is to ensure that issuers of crypto-assets act fairly and professionally, that crypto-assets services providers are reliable and resilient, and that market abuses are deterred and sanctioned.

The first set of rules regards issuers. To provide enough transparency and adequate assurances to purchasers, issuers of crypto-assets willing to start a public offering or to be admitted on an exchange platform should be, first of all, legal entities [art. 4 (1)(a)]. Secondly, issuers should draft a white paper, notify it to the supervisory authorities and publish it on their website [art. 4 (1)(b-d)]. Thirdly, marketing communications should be fair, clear and not misleading, and be communicated to the same authorities [art. 6-7]. Fourthly, funds received by the issuer during a public offering that is limited in time should be kept in escrow

[50] D A Zetsche, R P Buckley and D W Arner, 'Regulating LIBRA: The Transformative Potential Of Facebook'S Cryptocurrency And Possible Regulatory Responses' (2019) 44 European Banking Institute Working Paper Series.

[51] M Dell'Erba, 'Stablecoins In Cryptoeconomics' (49), 10-15.

[52] G7 Working Group on Stablecoins, 'Investigating The Impact Of Global Stablecoins' (2019) 12-14.

[53] The proposal establishes a different and stricter regime for 'asset-referenced tokens' (ARTs) and 'e-money tokens' (EMTs) due to their potential to become widely accepted as payment instruments (Recital 25). Issuers of ARTs, for instance, before launching a public offering or being admitted on a trading platform, should be authorized by the supervisory authority and their white papers should be approved prior to publication. Furthermore, at the crossroads of the regulation stand several rules regarding the stabilisation mechanism and the reserve assets backing the value of such crypto-assets. Issuers of EMTs, instead, should be either authorized as credit institutions or electronic money institutions and holders of EMTs should have a redemption right, at par value, of the fiat currency which the EMT is pegged to. Additional requirements and supervisory rules are then provided for 'significant' ARTs and EMTs, that are those exceeding certain thresholds defined by the EBA (e.g., market cap) that pose greater risks to financial stability.

by a credit institution or an authorised crypto asset service provider [art. 9]. Fifthly, those who purchase a crypto asset directly from the issuer should be provided with a right to withdrawal for a limited period of time [art. 12]. Lastly, issuers should act honestly, fairly and professionally, avoid conflicts of interests, and follow the most appropriate standards of security [art. 13].

A cornerstone of the legal regime is certainly the provision of a white paper, whose purpose is to inform prospective purchasers about functions, characteristics and risks of the crypto asset offering.[54] Even though the business practice makes blockchain start-ups already draft white papers, the MiCa Regulation proposal requires their notification to the supervisory authorities (but not their approval), provides explicit liability rules, and standardizes their content.[55] In fact, every white paper should contain information about the issuer, about the project, about the offering of crypto-assets or their admission to exchange platforms, about the rights and obligations attached to the crypto asset, about the technology employed and about the risks faced by purchasers [art. 5]. Furthermore, every marketing communication should be consistent with the content of the white paper [art. 6 (c)]. It is worth noting that cryptocurrencies like bitcoin and Non-Fungible-Tokens (NFTs) are exempt from the obligation to draft a white paper [art. 4 (2)].[56]

The second set of rules involves crypto asset service providers. Often, crypto-asset holders are threatened by cybersecurity incidents involving exchange platforms[57], incidents that may cost millions of Euros in losses, undermine market confidence and, eventually, hinder financial stability.[58] Since the extent of those issues or risks is partially determined by the inexistent regulatory framework[59], the MiCa Regulation proposal attempts to mitigate them by creating a bespoke regime for crypto asset service providers. The proposal enlists, at art. 3 (1)(9), eight types of services that can be provided by such operators. The services can be grouped in two categories (Recital 12): the first one identifies the activities of trading platforms, exchanges, and wallet providers; the second one includes placing crypto-assets, receiving and transmitting orders, executing those orders and providing advice on crypto-assets. In order to provide those services on a professional basis, crypto asset service providers should be legal entities and should be authorized from the national supervisory authority. The ESMA updates

[54] P P Pirani, 'Gli Strumenti Della Finanza Disintermediata: «Initial Coin Offering» E «Blockchain»' [2019] Analisi Giuridica dell'Economia, 332-337.

[55] D A Zetzsche and others, 'The Markets In Crypto-Assets Regulation' (40), 11-13.

[56] There are some notable exemptions from the obligation to draft a white paper: the most traditional ones regard private offerings (addressed to fewer than 150 people or solely to qualified investors) and offerings under the threshold of 1 million (over 12 months), and resemble those provided by the Prospectus Regulation; the most innovative ones, instead, regard crypto-assets that are offered for free, crypto-assets automatically created through mining, and crypto-assets that are unique and not fungible. Consequently, cryptocurrencies like bitcoin and Non-Fungible-Tokens (NFTs) will not be entirely governed by the MiCa Regulation proposal but only by title V, on crypto asset service providers, and by title VI, on the prevention of market abuses. Such exemptions seem to be justified by the fact that, in those cases, a proper offering does not take place because crypto-assets are either given for free, produced or individually negotiated and, therefore, their acquisition does not pose the same risk of information asymmetry.

[57] A Alkhalifah and others, 'A Taxonomy Of Blockchain Threats And Vulnerabilities', *Blockchain for Cybersecurity and Privacy* (2022).

[58] Financial Stability Board, 'Crypto-Asset Markets. Potential Channels For Future Financial Stability Implications' (2018), 8-12.

[59] MiCa Regulation Proposal, 4-5. See also OICV-IOSCO, 'Issues, Risks And Regulatory Considerations Relating To Crypto-Asset Trading Platforms' (2020), 3-5.

a register of crypto asset service providers.

The MiCa Regulation proposal requires crypto asset service providers to 'act honestly, fairly and professionally in accordance with the best interests of their clients' [art. 59 (1)] and, in particular, to warn their clients about risks and not to provide misleading information. Members of the management and those who own, directly or indirectly, a relevant stake in the business should have the necessary good repute and competence and should take all reasonable steps to ensure continuity and regularity in the performance of their crypto-asset services, both from an organizational and technical standpoint [art. 61]. Any crypto asset service provider should have in place prudential safeguards, in form of funds or an insurance policy, of an amount equal to the highest between the minimum capital requirements specified by annex IV per type of service (ranging from EUR 50.000 to 150.000) and one quarter of the fixed overheads of the preceding year [art. 60]. Moreover, providers should safekeep crypto-assets, passwords to access those crypto-assets, and any other fund belonging to their clients while avoiding their use without express consent. Finally, the proposal entails specific obligations for the provision of certain services related to crypto-assets.

The last – but not less important – set of rules concerns market abuses. In fact, certain behaviours could destabilize crypto asset prices, cause huge losses to their holders, and jeopardize users' confidence in markets of crypto-assets (Recital 64). Hence, the MiCa Regulation proposal – considering that many crypto-assets fall outside the scope of the Market abuse Regulation[60] and that its entire application could be disproportionate – lays down specific rules to deter abuses. First, issuers should disclose inside information concerning the public in a 'complete, correct, and timely manner' unless it remains confidential, or may prejudice or mislead the public [art. 77]. Secondly, nobody in possession of inside information should use such information to deal with crypto-assets or to make recommendations to others [art. 78] and, thirdly, any conduct that may constitute market manipulation is prohibited [art. 80].

3. The Evidential Value of Distributed Ledgers.

Having already examined the legal framework of crypto-assets, it is now time to point the attention towards another central element of blockchain technology, the distributed ledger. As it is known, the distributed ledger is a core component of the blockchain because it ensures that the information stored in the blockchain remains untampered. In fact, by sharing encrypted copies of the ledger across multiple nodes, the blockchain safeguards its integrity against external attacks.[61]

A distributed ledger (more in general, a blockchain) plays mainly an evidential role since it provides and safeguards information.[62] The bitcoin protocol, for instance, uses the distributed ledger to record any bitcoin transaction and,

[60] European Union Regulation No 596/2014 of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC [2014] OJ L 173/1.

[61] J Bacon and others, 'Blockchain Demystified' (3), 12-13.

[62] E Mik, 'Blockchains As Transacting Platforms?', *'Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 169; M Finck, *Blockchain Regulation And Governance In Europe* (Cambridge University Press 2019) 1.

consequently, to keep trace of bitcoins' entitlement history, making sure that it does not get hacked.[63] A distributed ledger, however, could custody any kind of information (even a document or an image). It works as a traditional database but, being distributed across multiple nodes, ensures the integrity of the data concerning that information. Hence, businesses could employ blockchain technology to record and preserve any kind of information (e.g., to keep track of their inventories or to safeguard important documents), developing the features that best suit their needs.[64]

The evidence that can be provided by the distributed ledger falls within two broad categories: evidence about entitlement and evidence about attributes.[65] In the first case, the distributed ledger serves the purpose of recording any transaction of a certain asset intercurred between participants of the blockchain. It, therefore, should give evidence about the person entitled to dispose of a certain asset: as a traditional land register records the ownership history of real estate, a distributed ledger can record the entitlement history of tokens, like with the bitcoin protocol.[66] In the latter case, the distributed ledger records additional information – such as the characteristics of an asset or a person – and its modifications. Documents, images, health data, and so forth, fall all within this category of evidence. Obviously, the two categories of evidence can be offered simultaneously. Blockchains that store non-fungible tokens, for instance, produce both evidence of entitlement and evidence of attributes of those specific tokens (representative of digital assets like images or texts).[67]

The evidential features of the blockchain largely depend on the information stored by the distributed ledger. Whether the information refers to something that exists only on the blockchain (on-chain assets), the blockchain can be said to be 'pure'. [68] The bitcoin protocol, for instance, can be considered as a 'technologically "pure" system' because its electronic coins are intangible and exist only as digital entities. Moreover, any right over bitcoins is solely entitled by the distributed ledger itself and they would cease to exist if every copy of the ledger is erased. Conversely, whether the information refers to something or someone existing in the real world (off-chain assets), the blockchain can be said to be 'impure'. Off-chain assets exist outside the blockchain and can have either tangible form, like real estate or cars, or intangible form, like intellectual property rights or shares of a company. Both tangible and intangible off-chain assets can survive the peril of the blockchain because they have a legal existence in the real world. Rights in such assets are determined by the law and the blockchain is not the only evidence about those assets.

Off-chain assets pose a relevant issue to those willing to implement a blockchain. Since rights in such assets are determined by the law and not by the system itself, any modification not included in the distributed ledger could lead to

[63] S Nakamoto, 'A Peer-to-Peer Electronic Cash System' (8), 1.
[64] An early overview of the possibilities offered by blockchain technology was given by the bestselling book D Tapscott and A Tapscott, *Blockchain Revolution* (Penguin 2018).
[65] C Reed and others, 'Beyond Bitcoin' (5), 165.
[66] *Ibid.*
[67] A brief introduction to NFTs has been provided *supra* [10].
[68] C Reed and others, 'Beyond Bitcoin' (5), 161-164.

a mismatch between the reality of facts and that depicted by the blockchain.[69] A judgement, for example, could impact on the ownership of an off-chain asset. In such a case, because of the technical safeguards of blockchain technology, it would be very difficult – if not impossible – to rectify the distributed ledger. Therefore, the blockchain should be implemented in such a way as to give someone the authority to modify the information stored in the distributed ledger.[70] Otherwise, nobody would have the power to technically reverse any transaction because that power would be necessarily distributed among the nodes of the network.

Assuming nonetheless that distributed ledgers can preserve data integrity and perform an evidential function from a technical standpoint, their significance remains to be investigated from a legal standpoint in the European framework. The legal significance of distributed ledgers may not be a relevant problem to 'pure' blockchain systems because on-chain assets are created by the system, and it is the system itself that provides technical rights in such assets. Neither would be a relevant problem if the distributed ledger is adopted, within a single organization, just to ensure integrity of data collected for internal purposes (e.g., to track the inventory) because the ledger does not serve an evidential function outside the organization. However, the problem gains utmost importance if off-chain assets and third parties are involved. In fact, despite the technical safeguards provided by blockchain technology, the legal system may not recognize any value to the information stored in the distributed ledger and it would not provide any evidence in a legal sense.[71]

Hence, it is time to investigate under which conditions distributed ledgers can truly play an evidential role for off-chain assets. As a general premise, it is necessary to highlight that not every activity that has legal effects can be freely executed by private individuals. Many activities are of exclusive competence of the State and can be performed only by governmental bodies or qualified professionals using predetermined technical instruments. It is the case, for example, of real estate transactions: in every European Member State registering ownership of and charges on land involve qualified professionals and land registers held by governmental bodies.[72] This kind of activities falls, at least partially, under the scope of public law and implementing distributed ledgers in such matters would certainly require law amendments and tailored technical solutions to provide any legal effect.

The evidential function of distributed ledgers could be more easily exploited in

[69] J Bacon and others, 'Blockchain Demystified' (3), 32-33; E Mik, 'Smart Contracts: Terminology, Technical Limitations And Real World Complexity' (2017) 9 Law, Innovation and Technology, 11.

[70] In terms of structure, blockchains can show great differences, the main one being probably between public (permissionless) and private (permissioned) blockchains. Public blockchains allow everyone to obtain a copy of the distributed ledger and participate in the consensus mechanism employed to update the distributed ledger. Governance, therefore, is distributed democratically among the users of the network. Private blockchains, instead, adopt an access control layer (ACL) that requires users to be authorized in order to access the network. Since developers preserve some form of governance, the blockchain loses its complete decentralization and resembles more traditional software applications. See, M Finck, *Blockchain Regulation* (62) 195-198; ESMA, 'Advice On Initial Coin Offerings' (11), 10-11.

[71] It has already been advocated that information stored on a distributed ledger may not constitute property. See, L Sagar, *The Digital Estate* (Sweet & Maxwell 2018) chapter 4.

[72] European University Institute, 'Real Property Law And Procedure In The European Union' (2005).

private law matters because of the principle of freedom of contract.[73] As it is known, individuals are free to decide whether and with whom they want to enter into a contract and, more importantly, its content (within the boundaries of the law). Parties, therefore, are capable of determining the terms of their agreement and its legal effects. In these matters, they can also decide to adopt a technical instrument like blockchain technology and its distributed ledger. In substance, the distributed ledger could be employed either to record the contract, as to preserve its content, or be recalled by the contract itself as a source of information (to measure the performance agreed, the occurrence of some conditions, etc.). The parties, for instance, could rely on the information stored on the distributed ledger to determine the price to be paid in exchange of some goods or services offered.

Those interested in implementing a blockchain, however, should pay attention to the form required by the law to conclude the contract. As it is known, contracts can be both concluded – implicitly – by conduct, or – expressly – by word of mouth or in writing. The general rule is that contracts can be concluded informally, as the parties prefer. However, specific rules, depending on the matter and on the country, impose the written form either as evidence or as a validity requirement.[74] When the law requires the written form, distributed ledgers could not produce any legal effect unless they are able to satisfy the legal requirement of the written form. Therefore, it is necessary to assess whether a distributed ledger, in abstract, can satisfy this requirement.

To solve the problem, it is necessary to give a bit of context. From an historical standpoint, the legal requirement of the written form was developed around paper documents. In fact, paper documents – either manuscript or simply signed – have two main features: (1) through the signature, they can provide evidence about the identity of the signatory and about its intention to adopt the content of the document; and (2) they are difficult to counterfeit because, in most cases, experts can verify both handwriting and modifications on those documents. Conversely, many electronic documents are modifiable without leaving traces, and cannot be uniquely attributed to one person. This is the reason why, facing the emergence of e-commerce and the transition from paper documents to electronic documents, the European legal system had to find tailored solutions to identify parties and ensure integrity of electronic documents.[75]

The main piece of legislation in this regard is the eIDAS Regulation[76] that, succeeding Directive 1999/93/EC, is modelled around electronic signatures and trust services. On one side, electronic signatures are utilised to preserve data integrity due to their technical capability to cipher electronic documents. On the other side, 'trust service providers' (Certification Authorities and Registration Authorities) are appointed responsible for verifying identities and issuing ownership certificates of electronic signatures. In other words, flaws of electronic documents are solved by using electronic signatures in combination with trust service providers both to authenticate parties and to secure electronic

[73] Some authors investigated aspects of contract and property laws as to determine whether digital assets are capable of acquiring *erga omnes* status. See, R Kulms, 'Blockchains: Private Law Matters' [2020] Singapore Journal of Legal Studies, 63-89.
[74] E McKendrick, *Goode On Commercial Law* (Penguin 2010) 80.
[75] C Reed, 'What Is A Signature?' (2000) 3 Journal of Information Law & Technology.
[76] European Union Regulation No 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 L 257/73.

documents.

The eIDAS Regulation states also the principle whereby ‘an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form’ [Art. 46]. However, not all electronic documents are considered equal by the Regulation because it takes a tiered approach to legal value. In fact, the evidential strength changes according to the electronic signature attached to the document: the higher the guarantees offered by the signature, the stronger the evidential value will be. The simplest ‘electronic signature’ is any data ‘used by the signatory to sign’, such as plain text or an image of the signature [art. 3(10)]. An ‘advanced electronic signature’ is uniquely linked to the signatory and to the data signed therewith ‘in such a way that any subsequent change in the data is detectable’ [art. 26(1)(d)]. A ‘qualified electronic signature’ is an advanced electronic signature issued by a qualified trust service provider that meets the technical requirements laid down by the eIDAS Regulation. Being the safest, the qualified electronic signature produces ‘the equivalent legal effect of a handwritten signature’ [art. 25(2)]. Consequently, electronic documents signed with this kind of signature are the only ones that meet the requirement of the written form. Other electronic documents will produce legal effects only if the written form is not a validity requirement.

Since ‘electronic documents’ are defined by the eIDAS Regulation as ‘any content stored in electronic form, in particular text or sound, visual or audiovisual recording’ [art. 3(35)], distributed ledgers could well be considered as such.[77] Hence, they would be admissible as evidence in legal proceedings as any other electronic document and, likewise, their evidential strength would rely on electronic signatures. Therefore, the implementation of electronic signatures in distributed ledgers needs to be analysed further.

As it is known, blockchains already employ public-key cryptography, that is the same technology adopted by many advanced and qualified electronic signatures. The system works by generating for each user a pair of linked keys (constituting a digital signature): the private key can be used to sign, while the public key can be used to authenticate the signatory and verify the integrity of the data. The difference is that, whereas e-signatures are uniquely attributed to a real-life person by a trust service provider, blockchains only need to authenticate users on a technical level (to identify users allowed to interact with the distributed ledger).

Nonetheless, blockchains do not operate all in the same way, and a distinction should be drawn between permissionless and permissioned ledgers.[78] In permissionless ledgers everyone can join the network, and every user remains anonymous. In the bitcoin protocol, for instance, everyone is allowed to anonymously set up a wallet and create the keys required to send and receive bitcoins. Thus, the set of keys would never be capable of identifying users and the distributed ledger would have a weak evidential value.

---

[77] F Sarzana di S. Ippolito and M Nicotra, *Diritto Della Blockchain, Intelligenza Artificiale E Iot* (IPSOA 2018) 51.

[78] *Supra* [70]. Moreover, H Eenmaa-Dimitrieva and M J Schmidt-Kessen, 'Regulation Through Code As A Safeguard For Implementing Smart Contracts In No-Trust Environments' (2017) 13 EUI Working Papers, 10-16.

In permissioned ledgers, instead, access is restricted solely to the members that have been approved by some form of centralized authority. This access control layer, hence, could be designed as to require user identification.[79] In this case, users would be uniquely linked to the signature required to interact with the distributed ledger as with an advanced electronic signature. An organization willing to implement its own distributed ledger, for instance, could assign a pair of keys to each customer after the upload and live verification of his identification document. In this case, any piece of information stored in the distributed ledger by the customer, such as a purchase order, would have a strong evidential value. However, in order to meet the legal requirement of the written form, the organization would have to rely on qualified trust service providers (or register itself as such) and attribute qualified electronic signatures to its users.

However, adapting the rules designed for e-signatures for blockchain applications, is not an easy task. For this reason, the EU Commission has recently proposed an amendment to the eIDAS Regulation that attempts to cope with distributed ledgers.[80] An 'electronic ledger' (to use the proposal's words) is there recognized to combine 'time stamping of data and their sequencing with certainty about the data originator similar to e-signing with the additional benefit of enabling a more decentralized governance that is suitable for multi-party cooperation', and to 'help companies saving costs by making multiparty coordination more efficient, safer and [to facilitate] regulatory supervision'. The regulation of electronic ledgers, thus, becomes of 'paramount' importance to give legal effect to the transactions contained within the ledger itself.[81]

The proposal distinguishes between simple 'electronic ledgers', that are tamper proof records of data, and 'qualified electronic ledgers', that are also created by a qualified trust service provider by implementing technologies that ensure the requirements set forth in the Regulation. Hence, it first recognizes the legal value of all electronic ledgers and, secondly, states that 'a qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger [art. 45(h)]. As a consequence, the certification as qualified trust service providers should provide that legal certainty needed for use cases where the distributed ledger needs to meet the requirement of the written form. Using the words of the European legislator, a qualified electronic ledger 'creates a reliable audit trail for the provenance of commodities in cross-border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative public services' (Recital 34).

---

[79] The adoption of permissioned ledgers in the financial system to solve the issue of digital identification and representation is analysed taking as an example Diem, the stable-coin sponsored by Meta by G A Jafari and M C Gruber, 'The Case Of Diem: A Distributed Ledger Technology-Based Alternative Financial Infrastructure Built By A Centralised Multisided Platform' (2021) 4 Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 324-326.

[80] Proposal for a European Union Regulation COM(2021) 281 final of 3 June 2021 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity [2021].

[81] C Sorge and M Leicht, 'Blockchain-Based Electronic Time Stamps And The Eidas Regulation: The Best Of Both Worlds' (2022) 19 SCRIPT-ed; R Garavaglia, 'Cambia Il Regolamento Eidas E Nascono I Gestori Qualificati Di Registri Distribuiti' (*Pagamenti Digitali*, 2021) <https://www.pagamentidigitali.it/payment-regulation/eidas/> accessed 8 June 2022.

4. Giving Smart Contracts a Legal Framework.

The most famous application of blockchain technology is almost certainly that of smart contracts, whose name and possible implementations have sparked an intense debate among legal scholars.[82] In fact, smart contracts aspire to be contracts written in programming language that enable computers to autonomously execute them.[83] In other words, self-performing contracts. However, the reality is that they are just computer programs that run on a blockchain. Therefore, it is necessary to analyse their legal value and their relationship with traditional contracts and, more specifically, to define under which conditions they can be legally binding and how can they be enforced.[84]

The idea of autonomous (smart) contracts is not new. Nick Szabo coined the term in 1997 by giving an example: as a vending machine takes coins and dispense product and change fairly, so could computers engage in any exchange of valuables controlled by digital means.[85] The basic idea was to embed contractual clauses in hardware and software as to make breach of contract expensive. In this way, once the parties define the terms of the contract, those are converted into a computer program that automatically checks if some conditions are met and provides the expected performance. At this point, the contract could autonomously enforce itself without any intervention (hence becoming 'smart').

The difference between traditional contracts and smart 'contracts' stands in the fact that a smart contract would not only be concluded, but also performed, electronically. In traditional contracts, conclusion and performance are two very different moments. First, the parties agree to be bounded and, only afterwards, they execute the contract. If one of the parties is not willing to perform, the process can be very inefficient and consuming: the other party has to institute legal action for breach of contract and demand, before the Court, its enforcement. In smart contracts, conversely, the breach of contract would be impossible. Since

---

[82] Among many others, P Cuccuru, 'Beyond Bitcoin: An Early Overview On Smart Contracts' (2017) 25 International Journal of Law and Information Technology, 188; P Cuccuru, 'Blockchain Ed Automazione Contrattuale. Riflessioni Sugli Smart Contracts' [2017] Nuova giur. civ. comm., 107; D Di Sabato, 'Gli Smart Contracts: Robot Che Gestiscono Il Rischio Contrattuale' [2017] Contr. impr., 386; C Clack, V A Bakshi and L Braine, 'Smart Contract Templates: Foundations, Design Landscape And Research Directions' [2017] arXiv:1608.00771v3; K E C Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts And The Social Workings Of Law' (2017) 3 Engaging Science, Technology, and Society, 1; E Mik, 'Smart Contracts: Terminology, Technical Limitations And Real World Complexity' (2017) 9 Law, Innovation and Technology, 269; R De Caria, 'The Legal Meaning Of Smart Contracts' (2018) 26 European Review of Private Law, 731; M Giuliano, 'La Blockchain E Gli Smart Contracts Nell'innovazione Del Diritto Del Terzo Millennio' [2018] Diritto dell'informazione e dell'informatica, 989; M Durovic and F Lech, 'The Enforceability Of Smart Contracts' (2019) 5 The italian law journal, 493; C Miraglia and V Orsini, 'Gli Smart Contract Tra Falsi Miti E Teoria Generale', *Temi di diritto civile* (Brasil Multicultural 2019), 119; P De Filippi, C Wray and G Sileno, 'Smart Contracts' (2021) 10 Internet Policy Review, 2. An extensive study has been recently published by UK Law Commission, 'Smart Legal Contracts Advice To Government' (2021).

[83] E Mik, 'Smart Contracts' (82), 3-5.

[84] Some authors argue that smart contracts 'should be considered as self-sufficient legally-binding agreements' because they 'do clearly create obligations which stand independently from the digital code'. See, R De Caria, 'The Legal Meaning Of Smart Contracts' (82), 746-749.

[85] N Szabo, 'Smart Contracts: Building Blocks For Digital Markets' (Fon.hum.uva.nl, 1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 8 June 2022.

smart contracts are self-performing, there would not be (at least theoretically) any necessity for public enforcement.[86] One party, for instance, could never deliberately fail to pay, because the programming code would autonomously provide for it.

In recent years, contracts started to show an increasing degree of automation.[87] It might be enough to recall how Uber determines the price of a ride and automatically pays the driver, or how streaming platforms like Netflix allow users to access their content only under payment. Nonetheless, it was not until the launch of the Ethereum platform in 2014 that the expression 'smart contracts' was evoked again and became popular. In fact, as it is known, the Ethereum platform was conceived in a Turing-complete programming language as to allow anyone to deploy decentralized applications called 'smart contracts' and to receive payments in its native cryptocurrency, 'ether'.[88]

The dual spirit of cryptocurrency scheme and software development platform was the key for the revival of the idea of smart contract. On one side, the implementation of smart contracts in a blockchain framework helps to prevent unilateral changes to the contractual scheme and is particularly helpful in no-trust environments. On the other side, the possibility to arrange payments in cryptocurrency avoid interferences of banking intermediaries in the execution of the smart contract (payment orders, for instance, cannot be revoked).

The expression 'smart contracts' could be misleading because it might induce to think that they are the digital equivalent for traditional contracts.[89] It is oversimplistic to think that any contractual clause could be expressed as an algorithm and that, consequently, any contract could be traduced into a computer program.[90] Even though code and contract can – at least theoretically – overlap, it is very difficult to establish whether a software can be considered as a legally binding contract. Therefore, it is of paramount importance to clarify the fundamental elements that qualify, from a legal standpoint, a contract and verify whether, and to what extent, they can be represented in programming code.[91] The code governing the smart contract could well be unable to meet the requirements imposed by the law and, consequently, result only in a piece of code that automates a performance. 'The technology of smart contracts does not constitute a new contract law; instead, the interpretation and validity of smart contracts has to be assessed against the backdrop of existing contract law'.[92]

A contract is 'an agreement between private parties creating mutual obligations enforceable by law'.[93] It is a legally binding agreement because

[86] P Cuccuru, 'Beyond Bitcoin' (82), 186-188.
[87] Contractual implications of the automation of contracts are analysed in detail by M D'Ambrosio, *Arbitraggio E Determinazione Algoritmica Dell'oggetto* (Edizioni scientifiche italiane 2020).
[88] See, 'What Is Ethereum?' (*ethereum.org*) <https://ethereum.org/en/what-is-ethereum/> accessed 6 July 2022.
[89] G Finocchiaro, 'Il Contratto Nell'era Dell'intellingenza Artificiale' [2018] Rivista trimestrale di diritto e procedura civile, 441-460.
[90] Some authors even claim that 'smart contracts fail to take the social complexities of contracting into account' and that 'contracts operate as social resources, through and against which people manage their relationships, and within which legal obligations and social expectations are intricately interwoven and mutually constitutive'. See, K E C Levy, 'Book-Smart, Not Street-Smart' (82), 10.
[91] M Giuliano, 'La Blockchain E Gli Smart Contracts' (82) ,1027.
[92] J Oster, 'Code Is Code And Law Is Law—The Law Of Digitalization And The Digitalization Of Law' (2021) 29 International Journal of Law and Information Technology, 14.
[93] E Peel and G H Treitel, *Treitel On The Law Of Contract* (Sweet & Maxwell/Thomson Reuters 2020).

parties can rely on the law and its agents to enforce it. In case of breach, the Court can put the innocent party in the position he would have been in had the contract been properly performed.[94] The agreement, however, shall meet the requirements set by the applicable law.[95] Requirements vary across legal systems and countries but, in principle, the fundamentals are mutual assent, adequate consideration, capacity, and legality. In some cases (like financial transactions), formalities like the written form can also be required. Hence, the smart contract should not infringe the law (for instance, by selling access to hacked software), involve adequate consideration, and – more importantly – be stipulated with mutual assent. Parties should agree to be legally bound through an offer and an acceptance: either via digital means (e-mails, click-wrap agreements, etc.) or implicitly (one party makes available the smart contract and the other consciously executes it).

For the sake of clarity, it might be helpful to divide smart contracts in 'smart contract code' and 'smart legal contracts'.[96] A smart contract can be considered as 'smart contract code' when it is only a software that automates a performance and requires a separate contract to set the terms (for instance, a computer program that automates an insurance contract). In this case, the use of the word 'contract' is inappropriate and does not bring any legal implication since the contractual terms will have to be found elsewhere (contract and code are separated). A smart contract can be considered, instead, as a 'smart legal contract' when the software is, autonomously, a legally binding contract (contract and code overlap). The contract here is not only performed but also represented by programming code because the legal requirements are satisfied.

A smart contract code, requiring parties to separately stipulate a traditional contract, falls under the 'external model' of smart contract.[97] In fact, the contractual terms that are legally binding are external to the smart contract itself: the parties first stipulate the contract (orally, in writing, or digitally) and then execute the smart contract code as to automate the performances. Conversely, in a smart legal contract, parties enter into an agreement by simply using the program (for instance, sending a certain amount of cryptocurrency to the wallet of the smart contract). Therefore, it can be said described as an 'internal model' of smart contract: the contractual terms are the algorithms constituting the smart contract itself. The whole contractual scheme is represented by algorithms. Fictionally, one party makes an offer by making available the smart contract while the other accepts by activating it. Using the computer program, the party agrees to its rules and accept its outcomes.

The internal model is not suitable for all contracts because the contractual

[94] Robinson v Harman [1848] 18LJ Ex 202.

[95] UK Law Commission, 'Smart Legal Contracts' (82), 39-73, for instance, outlines the requirements for a legally binding contract under the law of England and Wales and discuss how these requirements might be satisfied in the context of smart legal contracts.

[96] Distinction proposed by Josh Stark *in* 'Making Sense Of Blockchain Smart Contracts' (*CoinDesk*) <https://www.coindesk.com/making-sense-smart-contracts/> accessed 1 July 2022. Later, it has been adopted by C Clack, V A Bakshi and L Braine, 'Smart Contract Templates' (82), 6. Recently, it has been used as the foundation of UK Law Commission, 'Smart Legal Contracts' (82).

[97] The idea that smart contracts may fall either within the internal model of smart contract or the external one has been laid out by ISDA Linklaters, 'Smart Contracts And Distributed Ledger – A Legal Perspective' (ISDA Linklaters 2017) <https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf> accessed 8 June 2022.

scheme needs to be easily understandable. The smart contract should be able to show the necessary information which is material to an acceptee for making an informed assessment, just like a vending machine displays both the product and the price. Since the party makes an offer by making available the smart contract, the offer must include all the key terms of the contract. Otherwise, as it is known, it will classify as an advertisement. However, the programming code is not always inspectable and is not comprehensible by everyone.[98] Thus, the offer should be simple enough as to be acceptable by tacit or implicit consent. Complex contractual schemes could be binding only if additional information is provided and, consequently, need to adopt the external model of smart contract.

Moreover, every clause of the contract should be susceptible of being translated into programming language. First, not everything that has legal relevance can be executable by computer programs because they cannot 'encode references to general standards or general clauses' (like the principle of good faith).[99] Even though AI technology would enable it, traditional software is not capable of interpreting or guessing.[100] Nonetheless, AI would introduce a margin of error that is unacceptable for blockchains. Secondly, only operational aspects of a contract (those regarding some sort of action, like a cryptocurrency transfer) can be automated. Consequently, an internal model of smart contract would be draftable only with unambiguous terms and operational aspects.[101]

Nonetheless, the external model of smart contract presents some disadvantages due to the fact that the contractual scheme and the smart contract code are detached. Once activated, the smart contract executes the performance autonomously and cannot be interrupted. This means that any contractual issue (e.g., null and void contract) has no consequences on the execution of the software. The performance, in this case, would be legally invalid but computationally correct.[102] Consequently, it would not be rectifiable unless an opposite transaction is recorded on the blockchain, or the blockchain itself is designed as to allow rectification in specific cases. In fact, 'the alteration would invalidate the hash of the block containing the record, and also the hashes of all subsequent blocks'[103]. This means that, in case of breach, the Court would not have the power to directly interfere with the smart contract but would have to use other remedies such as damages. The internal model of smart contract, however, would suffer of the same issue in case of programming errors.

[98] P Cuccuru, 'Beyond Bitcoin' (82), 188-189.
[99] *Ibid*., 189-190.
[100] Some authors advocate that '[p]redictive capabilities created by big data and artificial intelligence increasingly allow parties to draft contracts that fill their own gaps and interpret their own standards without adjudication' - A J Casey and A Niblett, 'Self-Driving Contracts' [2017] SSRN Electronic Journal, 1.
[101] C Clack, V A Bakshi and L Braine, 'Smart Contract Templates' (82) 5-11.
[102] It is even argued that 'smart legal contracts may actually increase instances of defective performance, given the scope for the code to perform in ways the parties did not expect or intend'. See, UK Law Commission, 'Smart Legal Contracts' (82) 102-155, that extensively analyses the remedies applicable (also in practice) by British Courts.
[103] C Reed and others, 'Beyond Bitcoin' (5) 22.