LEGAL IMPLICATIONS OF THE USE OF THE BLOCKCHAIN TECHNOLOGY IN THE TRANSPORTATION INDUSTRY CONTEXT

Manuel Alba*

1. Introduction.

The blockchain technology has captured much attention during recent years, and its use has been gradually expanding from the field where it did originate (cryptocurrencies) to other applications, including the transportation industry. The blockchain has become popular for its alleged advantages as compared to preexisting technologies. As a relatively new technology (maybe not so much anymore), it has some features which previous practice is not necessarily familiar with. As soon as the activities that may benefit from the use of blockchain have legal implications, new features usually lead to new problems and uncertainties. The purpose of this paper is to briefly address the use of blockchain and its legal implications, including the legal ramifications that may be more interesting in the context of the transportation industry. To that end, we will first make an attempt to provide a basic description of the blockchain technology, and a glimpse of its differences as compared to previous solutions. We will then address the legal challenges that have been identified with regard to the use of the blockchain in general terms, as well as one of the most prominent tools that have been built upon it, the so-called smart contracts. Lastly, we will contextualize our discussion within the transportation and the logistics realm, in order to explore how the use of blockchain may change current practice and what the main legal concerns may be.

One idea should be stressed from the outset of this writing, however. Many people have been warning about the legal risks that the blockchain may entail. The risks attached to the use of any electronic communications technology depend on the use we make of it, rather than on the technology itself. This is also the case with blockchain-based solutions. As we will try to explain, many legal risks can be easily curbed by adjusting the features of the blockchain, but in some cases this will lead to the loss of part of the advantages that are normally attributed to this technology.

2. A brief description of the blockchain technology.

The blockchain is a technology whose main purpose and usefulness is to authenticate (to verify the authenticity of) information in the context of communications in the electronic or the digital medium[1]. One of the main risks in electronic communications relates to the need to verify the information exchanged,

* Associate Professor of Commercial Law at Carlos III University of Madrid. This paper has been drafted with the occasion of the FIATA Headquarters Session 2018. Although some references to specific technologies or solutions are made in this writing, nothing herein should be interpreted as a recommendation to use or not to use any of them. All statements are the sole responsibility of the author and are exclusively made with the intention to neutrally and objectively present or discuss the legal problems related to the use of digital means in the course of trade and business activities.

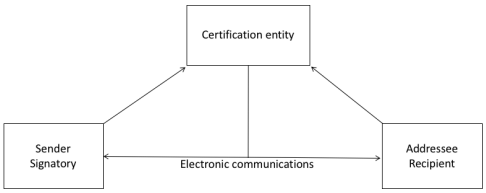
[1] In the sense that we will use it in this writing, information is authentic when it is in fact what it purports to be, i.e., when the person identified as the sender or in any electronic signature is in fact the sender or the signatory, and the information included in a communication, message or other document is in fact the information originally introduced, sent or stored (and has not been altered).

particularly where communications have a transactional purpose and provide the basis for decisions involving value (with the ensuing risk). Until recently, such electronically conducted, and thus information-dependent decisions or processes, did almost exclusively rely on the verification or authentication services provided by trusted third parties (trust services providers[2]). Trust service providers and their services may take different forms, but their intervention in all cases entails that the service provider intermediates in the communications process (between two or more parties) in order to verify the authenticity of the information exchanged or the communicated between them[3].

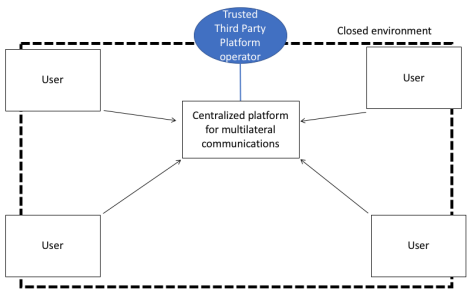
The third-party service-based approach, and the architecture that it is grounded upon, has found an alternative in the blockchain technology and the distributed ledger. The information exchange process in the distributed ledger, like third-party certification services, relies on the encryption of information and its verification by a decentralized network of multiple nodes on the basis of consensus. The information communicated through the network is shared by all nodes therein (the peers), which hence provide for the storage or record of such information as a distributed ledger. In its currently most

[2] See our comments in ALBA M., "Order out of Chaos: Technology, Intermediation, Trust and Reliability as the Basis for the Recognition of Legal Effects in Electronic Transactions", *Creigh. L. Rev.*, Vol. 47 (2014), p. 400-402.

[3] For instance, a certified electronic signature service provider (a certification entity) achieves this by issuing the user of the service (the signatory) an electronic signature certificate that is uniquely paired with its (previously verified) identity, and supplies the technology that enables the user to sign documents or communications and the addressees or any third party to verify the authenticity of the resulting signature (such services will allow verifying not only the identity of the signatory or the originator of the received information, but also in most cases the authenticity and the integrity of such information). This type of authentication services provided by certification entities do also extend to verification of the time of communications (time-stamp), the verification of the sending and the receipt of information, the certification of the authenticity of websites, or the contents or browsing of websites at a given time, or the certification of geolocation data.



This is the architecture also shown by the services of other trusted third parties, which on top of the foregoing provide also a centralized market or trading environment for business or transactional purposes. In these cases, the users would have access to a closed environment, in which all identities and the exchanged information would be authenticated or verified by the service provider.



common use (cryptocurrencies), the distributed ledger shows the previous history of transactions involving a certain specific asset (a cryptocoin). When communications have this particular purpose, each new transaction (the information in which it is registered) is broadcasted to the network (to the nodes), after which a competitive verification process (based on the resolution of a mathematical problem) takes place between them, in light of the recorded previous history (the so-called "mining", since the network rewards the fastest successful verification). The verification completed first by one of the nodes (as the "proof of work", in the Bitcoin network) is accepted by the rest of nodes on the basis of consensus (as long as it is not inconsistent with the information in the distributed ledger)[4]. A verified new transaction (the information in which it is reflected or recorded) is added to the chain of previous transactions as a new information block; the information in the distributed ledger, therefore, is structured as a chain of information blocks, which gives its name to this technology[5]. Every time a new transaction is concluded in relation to the same asset (the same coin), the process is repeated.

a. Distinctive features of the blockchain technology in its earliest use.

By reason of their decentralized architecture, the blockchain technology and the distributed ledger provide an alternative to the approach based on the intervention of a single trusted third party, thereby reducing the vulnerabilities frequently attributed to centralized communications[6]. Some other features have to be added to this, as they may be relevant to get an understanding of the legal problems feasibly involved in the use of blockchain for trading or business purposes. Thus, in the first place, in its earliest configuration and use (the blockchain at the service of the Bitcoin economy), this technology can be accessed and employed for free, and the exchange and verification of information can be achieved aside from any remunerated service (although different services have sprung up around cryptocurrencies trading). Second, the information in the distributed ledger can potentially be publicly accessed, which means that it is visible

[4] See a description of the process (for the Bitcoin as well as for other cryptocurrencies) in NAKAMOTO, S., "Bitcoin: a Peer-to-Peer Electronic Cash System", (available at https://bitcoin.org/bitcoin.pdf -last visit in January 2018), p. 3; FAIRFIELD, J. A.T., "Bitproperty", *S. Cal. L. Rev.,* Vol. 88 (2015), pp. 821-822; REYES, C. L., "Moving to Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: an Initial Proposal", *Vilanova L. Rev.*, Vol. 61 (2016), p. 197-198; ABRAMOWICZ, M., "Cryptocurrency-Based Law", GWU Legal Studies Research Paper No. 2015-9 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573788, las visit in February 2018), p. 22-23; GABISON, G., "Policy Considerations for the Blockchain Technology Public and Private Applications", *SMU Sci. & Tech. L. Rev.*, Vol. 19 (2016), p. 341; KIVIAT, T.I., "Beyond Bitcoin: Issues in Regulating Blockchain Transactions", *Duke L.J.,* Vol. 65 (2015), p. 578; SHACKELFORD, S.J. y MYERS, S., "Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace", *Yale J.L. & Tech.*, Vol. 19 (2017), p. 339.

[5] CHRISTENSEN, K., "Bitcoin, Blockchain and the Future of Financial Services", 134 (10) *Banking L. J.* 532 (2017), p. 532; FAIRFIELD, *cit. supra* note 4, p. 820; ABRAMOWICZ, *cit. supra* note 4, p. 13, 16-17.

[6] The consensus based approach entails that any attempt to hack or control communications in the distributed ledger would require control of at least 50% of the network, by reason of which in most cases such an action would simply be at a loss –ABRAMOWICZ, *cit. supra* note 4, p. 2; HYLAND, G.M. y DIGESTI, M.P., "New Nevada Legislation Recognizes Blockchain and Smart Contract Technologies", *Nevada Lawyer*, August 2017, p. 14; REYES, *cit. supra* note 4, p. 199; FAIRFIELD, *cit. supra* note 4, p. 806.

to any user in the network[7]. Thirdly, and by reason of the block structure and the verification system, the information exchanged, once verified and added to the blockchain in the distributed ledger, cannot be modified by any user in normal conditions, including the one introducing the information. This feature is commonly represented by referring to the "immutable" or "irreversible" character of the information[8], and it allows spotting the inconsistencies that, from a logical point of view (*i.e.*, in its contents), the information may show. Finally, the blockchain and the distributed ledger have been also described as a "trustless" system or technology, as it overcomes the need to rely on a single trusted third party for communications purposes. This last feature, however, should be further spelled out, as the blockchain and the distributed ledger, although based upon a decentralized open network, provide for an intermediated trust and communications scheme[9], in which trust by its users does actually play a crucial role. Users' trust is what determines the network's critical mass, and to that extent its reliability and its success.

By reason of all the foregoing features (and some others), the blockchain has been often deemed a cheaper and more efficient technology in terms of data verification and integrity. For the time being, the first and most prominent use of the blockchain has focused on the issuance and transfer of cryptocurrencies. The technology was therefore created and designed to support the representation, title allocation and transfer of digital (intangible) assets that may be recognized and administered as such on the basis of their permanent identification and their singularity[10]. The blockchain and the distributed ledger can be potentially applied with the same purposes to any intangible assets susceptible of being represented in digital information, including personal (contract-based) rights. This basically requires that the system reliably identifies the issuer and records any actions that may be needed to ensure the legal effectiveness of the issuance or creation of an identified asset (whether based on property law or on contract), that it does also identify the owner or holder of each asset or right and ensures that, once it has been transferred or disposed of, only the new owner may dispose of it (and the previous owner, transferor, can no longer do that); this is what has become to be termed as "tokenization", which necessarily must ensure that the "double spending" of an asset is prevented[11].

---

[7] See NAKAMOTO, *cit. supra* note 4, p. 6; REYES, *cit. supra* note 4, p. 191, 198-199; FAIRFIELD, *cit. supra* note 4, p. 820, 873-874; MARTIN CHRISTOPHER, C., "The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain", *Nev. L.J.,* Vol. 17 (2016), p. 149-150.

[8] SIBBITT, E., PATEL, B. y LERAU, J., "Blockchain and Financial Services: Hype or Herald", *Banking L. J.* Vol. 134, No. 4 (2017), p. 209; MARTIN CHRISTOPHER, *cit. supra* note 7, p. 175; GABISON, *cit. supra* note 4, p. 333.

[9] See comments by NAKAMOTO, *cit. supra* note 4, p. 1, 8; FAIRFIELD, *cit. supra* note 4, p. 813; MARTIN CHRISTOPHER, *cit. supra* note 7, 141-142, 155, 161; KIVIAT, *cit. supra* note 4, p. 574.

[10] In the Bitcoin blockchain, for instance, this is achieved by numbering each and every Bitcoin with a unique identifying code (see DOGUET, J.J., "The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System", *La. L. Rev.*, Vol. 73 (2013), p. 1125-1128; FAIRFIELD, *cit. supra* nota 4, p. 820, 857.

[11] See NAKAMOTO, *cit. supra* note 4, p. 2; ABRAMOWICZ, *cit. supra* note 4, p. 22-23; KIVIAT, *cit. supra* note 4, p. 578; FAIRFIELD, *cit. supra* note 4, p. 817, 820, 825-826, 830.

b. Blockchain, smart contracts and the internet of things.

All this being said, and to the extent that its main value lays on its greater reliability for verifying the authenticity of information and keeping its integrity, the uses of blockchain technology and the distributed ledger architecture are already expanding much beyond the ones just described. They can actually be used for any transactional or administrative purposes whatsoever, to the extent that they require or may be addressed through the exchange of information in electronic form; including those that may be more suitably undertaken by resorting to the tracking of events or circumstances relating to tangible (non-digital) assets (which, or whose ownership or related rights may be also electronically represented, as well as created, allocated/transferred or cancelled/terminated, *e.g.*, in accordance to a contract and/or contract law –think, for instance, of the logistical and the administrative route that commercial products have to go through from the place where they are produced or assembled until they reach their final destination or their final user).

These possibilities have to be assessed now by taking into account other technologies whose use may be combined with the operation of the blockchain and the distributed ledger; which have developed simultaneously to the blockchain based technologies or on top of and as a result of it.

The most significant example of the latter is the so called smart contracts. Smart contracts developed on the basis of the blockchain technology used in the Ethereum network[12]. Although the term "smart contract" suggests having legal connotations or a legal meaning, it was coined by technologists and is precisely used to refer to certain self-executed programs (software code) which are aimed at implementing or executing certain actions autonomously and in an automated sequence, feasibly as the result of the will of two or more transacting parties or upon their previous agreement (not necessarily under an otherwise formalized or executed contract, strictly speaking). Indeed, smart contracts in the first place are code, executable (informatics) programs. In at least the majority of cases, they have an internal logic structure that works upon a condition-action sequence[13], so that once a set condition has been met, a certain action is triggered without the possibility for the parties involved to alter the said course or otherwise prevent the pre-set operation of the code[14]. When executed, consequently, smart contracts may automatically trigger certain actions that will result in the exchange or transfer of value between the involved parties, particularly to the extent that such a thing may be achieved by the mere communication of information in electronic or digital form (*e.g.*, transferring a digital asset, such as a cryptocoin, from one party or entity's

[12] Ethereum is the network supporting a cryptocurrency called the ether or gas (see an explanation in "Vitalik Buterin reveals Ehtereum at Bitcoin Miami 2014", https://www.youtube.com/watch?v=l9dpjN3Mwps, last visit in March 2018).

[13] SAVELYEV, A., "Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law", *Basic Research Program Working Papers* (Series: Law), National Research University – Higher School of Economics, WP BRP 71/LAW/2016, p. 12, 14.

[14] FAIRFIELD, J., "Smart Contracts, Bitcoin Bots, and Consumer Protection", 71 *Wash. & Lee L. Rev. Online* 35 (2014), p. 38-39; SKLAROFF, Jeremy M., "Smart contracts and the cost of inflexibility", 166 *U. Pa. L. Rev.* 263 (2017), p. 291-292.

wallet to another's; or transferring money from one party's account to another party's account)[15].

As feasibly determined but uncertain facts, the satisfaction of conditions in smart contracts has to be verified by them (by the program), by seeking and verifying the needed information. The source of such information (as a missing element in the smart contract) may be "onchain" of "offchain". In the former case, the needed information will be logged somewhere in the blockchain or the distributed ledger of the network upon which the smart contract is actually executed, in which case the verification of information will be done without any feed from outside the network. In the latter case, on the contrary, the information will need to come from a source outside the network, which in the smart contract terminology has come to be called and oracle, and additional verification means will have to be resorted to[16]. Also, oracles themselves (at least in the current terminology) may actually be persons or entities (*e.g.*, when the needed information may have to be introduced manually by one person –let's say, an employee of the customs administration of a certain State) or digital sources, including smart devices or objects, which may provide automatically and on a permanent basis the information to be taken or verified (*e.g.*, where the evolution or the quotation of a certain price or asset has to be verified in a structured bond). A further step in sophistication is taken when a smart contract is provided with an algorithmic basis, as an algorithm superimposed to a smart contract may actually take decisions and trigger actions autonomously, rather than in the above-described mechanic way (condition-action), on the basis of complex mathematical reasoning and the algorithm's learning (including self-teaching) capabilities.

All the foregoing can additionally be combined with the use of smart objects (the population of the so-called internet of things). Such a combination would entail that actions triggered as a result of, let's say, a smart contract, will not be limited to the information onchain, or offchain but online; and will include physical or material actions performed by machines or devices, with multiple feasible consequences (e.g., the shipment of an item, with its previous picking and labelling; or the interruption in the access to, or the operation of a certain equipment).

c. Some specific uses of blockchain and distributed ledger networks.

Aside from the cryptocurrency economies and related services, different industries have shown interest in developing solutions based on blockchain, in light of its several advantages and the greater level of data security that at least for some purposes it shows for its proponents. Two different alternatives are worth highlighting here, as probably the most popular ones for the time being.

One of them, proposed some years ago, would consist of creating blockchains that would be interoperable with existing open blockchain networks, and particularly the Bitcoin network, but with their own different purpose (e.g., to create another cryptocurrency). This so-called "side-chains" would therefore be blockchains and would

[15] FAIRFIELD, *cit. supra* note 14, at 40; MIK, E., "Smart contracts: terminology, technical limitations and real world complexity", *Law, Innovation and Technology*, Vol. 9 (2017), No. 2 (available at https://doi.org/10.1080/17579961.2017.1378468, last visit in March 2018), p. 277.

[16] SKLAROFF, *cit. supra* note 13, at 271-272; MIK, cit. supra note 15, p. 296.

coexist with other blockchain systems in the distributed ledger of a given existing network[17], whose protocol might have to be designed or modified in order to give access to sidechains to the network, but thereby sparing the need for these blockchains to build and develop an entire network (in other words, they would benefit from an existing network and its critical mass, capillarity and level of decentralization). Other than that, in principle, this blockchains could show the same features as the ones previously described.

More recently, other case uses are basically focusing on the provision of services based on blockchain by creating "closed", "proprietary" or "private" blockchain networks[18]. Distributed ledger networks of this sort differ from the above-described ones in that, in the first place, they are operated by a given entity or a group or consortium of entities, who would therefore govern its operation. From an architectural point of view, the information and communications system would still show a certain level of decentralization, as it would rely on a networked nodes infrastructure, but in terms of governance of the network this would already imply a significantly different level of centralization. The disadvantages attached to these "private" blockchain networks and their (less) distributed ledger precisely relate to their (consequently) lower reliability as compared to public networks, and their potential dependence (in all feasible senses) on the entity or entities with authority to govern the network[19]. The feasible advantages that these entails, to the extent that the needs of users so advise, are those normally attached to centralized communications services with the intermediation of a single entity or party. Particularly when the network can be accessed by users upon the basis of a service relationship or under a contract, the terms of the relationship may well (and surely will) address the conditions for the use of the network. On this basis, access to the information in the network's blockchain or distributed ledger may be restricted (and granted under different levels of permission). Consequently, not all the information will be visible to users. Also, the information in the network's blockchain or distributed ledger may be susceptible of modification (presumably, in accordance to the conditions of the service or relevant contract), which means that the information won't be "immutable" or "irreversible". This of course should not undermine the verification capabilities of the service and the network, but it might be needed to attract users in some industries.

3. Legal issues early associated to the use of blockchain.

The expanding use of blockchain networks has naturally raised several concerns as to the legal implications that the technology and its features may raise. Many of those concerns are essentially linked to the use of cryptocurrencies, and not to the use of blockchain strictly speaking. Given the somehow murky activities where cryptocurrencies first found a place, as well as their later approximation to the "mainstream" economy, problems first related to the Bitcoin (or to cryptocurrencies)

---

[17] See FAIRFIELD, *cit. supra* note 4, p. 829; KIVIAT, *cit. supra* note 4, p. 604-605.

[18] GABISON, *cit. supra* note 4, p. 341; GATTESCHI, V., LAMBERTI, F., DEMARTINI, C., PRANTEDA, C. and SANTAMARÍA, V., "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?", Future Internet, Vol. 10, No. 2 (available at http://www.mdpi.com/1999-5903/10/2/20, last visit on April 2018), p. 5.

[19] GABISON, *cit. supra* note 4, p. 341, 345.

have spread from crime prevention (such as money laundering and know-your-client obligations) and taxation issues[20], to regulatory concerns with regard to shadow investment activities. These involve the discussion, for instance, of whether cryptocurrencies have to be in any way treated as financial instruments, whether entities providing services akin to intermediation or investment services related to cryptocurrencies must be treated as investment service providers or as multilateral trading platform, facilities or markets, or whether initial offerings of cryptocurrencies would (therefore) fall under the rules relating to IPOs of financial instruments (in brief, whether the rules on financial markets and instruments, and the corresponding powers of supervising authorities would catch the cryptocurrencies industry or would leave it beyond its perimeter, and thus whether this needs new regulations). One interesting question still to be clarified beyond such particular issues is what the very legal nature of cryptocurrencies is, since they do not fit into any legal category of tangible (movable or immovable goods) or intangible property within those currently recognized by the law[21] (property or title upon cryptocoins, and it's feasible value in transactions is based and stems from pure contracts and contract, not property law).

a. Legal concerns related to the use of blockchain based technologies

In an abstract approach to blockchain, beyond the use of cryptocurrencies, several problems have been also identified. They relate to the legal effects or the risks of the information registered in the blockchain or the distributed ledger, as well as its treatment or management under laws or regulations that, by reason of their scope and purpose, are clearly prone to find application in activities in the digital space. Going from the probably less to the most sophisticated concerns usually raised, we may discuss here:

a.1. *The legal validity or effects of written (or other) documents in the distributed ledger*. The legal validity and effectiveness of digital or electronic writings is recognized in laws and regulations in many countries since long ago. Signatures and written documents enjoy the same treatment as paper ones, both for private (e.g., contractual) or public purposes (*e.g.*, in the context of administrative processes or formalities). The approach to digital or electronic documents and signatures, however, and even though the purpose in all cases is not to discriminate the electronic media, clearly varies from region to region (or from country to country). In countries like the United Sates, for instance, electronic documents or signatures are recognized as equally valid and effective as paper ones for every purpose to the extent that the means used to generate, communicate or store the information are sufficiently reliable[22] (which in terms of evidence law, in a procedural context, seems to be also the principle applied to other means or documents). Under this approach (and without prejudice of specific laws or regulations anyhow qualifying this rule), any existing or new technology may potentially be used in any transactional or

[20] See, *e.g.*, KIVIAT, *cit. supra* note 4, p. 590

[21] And the doubt would reach not only the private law field, but also public law areas, such as taxation law (where this is also currently discussed).

[22] See, for instance, Electronic Signatures in National and Global Commerce Act, 15 U.S.C. 7001-7006; Uniform Electronic Transactions Act 1999 (National Conference of Commissioners of Uniform States Law).

administrative processes to generate, exchange or submit documents or information in electronic form.

In other cases, and sometimes for purposes involving public administrations, the approach to electronic documents or signatures can very different. In particular, regulations may require the use of a certain specific technology for administrative formalities or procedures, or in general for access to documents or information, or communications with the public administration (*e.g.*, in Spain these require the use of a certain certified electronic signature for identification and signing purposes). Such a prescriptive policy may hinder the effectiveness of documents or information in the blockchain or the distributed ledger, and their legal (other than feasibly the technological) interoperability with any administrative processes based thereupon. The expansion of the use of blockchain technologies to commercial activities, however, will probably force public administrations to take all this into account and (where needed) to gradually open room for its use with administrative purposes too.

In some regions, such as the European Union, the state of the law as regards e-documents and signatures may be a problem as well in the sense herein discussed. Current regulations on trust services are not only clearly based on the central trusted third-party architecture, but also reliant on the accreditation (qualification) of certification service providers (and their technology) by public authorities[23]. Under this scheme, documents or signatures based on a qualified certificate (as issued by a qualified service provider) is presumed to be authentic, while other documents are not, and their authenticity may have to be proved (*e.g.*, for enforcing a contract in court proceedings)[24]. It is easy to see how this also puts blockchain based technologies at a competitive disadvantage, at least at a formal level. This rule, however and as between the parties involved, may be modified by contract.

a.2. *IP rights in the distributed ledger*. Another source of concern with regard to the use of blockchain based technologies relates to the communication of information that is subject to intellectual property rights. This has been a concern since the internet became of massive use, as information can be easily and cheaply copied or replicated in the digital medium; and in particular since the raise of the internet 2.0, as many services' added value began to rely on the possibility for users to upload their content onto the information systems put at their disposal by service providers, thereby creating a liability risk for intermediaries and service providers themselves as well[25]. Potential sources of IP infringement and liability risks have been identified also in the use of blockchain based technologies. These are akin to the ones already attached to preexisting technologies for digital communications,

[23] Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[24] Arts. 25.2, 35.2, 41.2, 43.2, 46 Regulation 910/2014.

[25] Intermediaries liability in this context has received special attention in European legislation and jurisprudence (see Arts. 12 to 15 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; see also the European Court of Justice decisions in cases C-236/08 to 238/08, 23 March 2010, and C-324/09, 12 July 2011).

but somehow linked to the particular features of blockchain networks in their initial look. First, from the point of view of users, it is said that the distributed ledger, the public accessibility of information and the fact that, once in the ledger, it cannot be modified, entails a greater risk of continued infringement of IP rights, as, even if the information is identified as potentially risky, the user cannot do much to avoid its quick spread or to eliminate or modify it[26]. Second, from the point of view of the network peers, the fact that the information flows through, or is lodged in their nodes with no control in principle, and (again) with no chance to modify or eliminate it, may likewise entail a liability risk, much like the one of other intermediaries in the digital space. Finally, for IP rights holders, blockchain or distributed ledger networks may entail greater difficulties to spot infringements or, even when so spotted, to enforce their rights. Besides the delocalization element that the internet already entails, in this regard we have to take into account that the distributed nature of the ledger entails that any potentially infringing information is likewise distributed, which is likely to make any enforcement efforts less effective[27].

This is an ongoing debate, and all these views have actually been put in question, as it is said that blockchain technologies may precisely provide a solution to the IP rights problem. This would be so to the extent that the information in the distributed ledger cannot be copied or duplicated[28]. We must remember that all these risks depend on how we use this and any other technologies. As regards users of blockchain-based technologies, an important element to asses is which purpose they are used for, what kind of information will be introduced in the ledger, and whether and how such information may be held under control of the user or the person/entity introducing or making any use of it (particularly where such technology is accessed on the basis of a service relationship, as it may be increasingly the case in the future). The same goes for the operators of the network or its nodes in relation to any intermediary liability risk. Without prejudice of the disadvantages that they may entail in different ways, the so-called private or permissioned blockchain networks, and their feasible submission to (wholly or partly) centralized governance schemes may certainly curb these risks, it is a question of how the technology is used and devised.

a.3. *Privacy and data protection*. Another field where the use of blockchain technologies and the distributed ledger is giving raise to increasing concern is privacy and personal data protection. The said issues are the subject in several regions of the world to strict regulations, where the risks of administrative liability are considerable. Problems related to personal data protection in this context are somehow close to the ones assessed in relation to IP rights, since the issues encountered here do also refer to how information is obtained or introduced in the blockchain or the distributed ledger, and how it is managed thereafter. For instance, in Europe, personal data protection rules have followed a scheme whose scope and logical structure relies on a definition of personal data, addresses how personal data may be collected, which rights the holder of such data mandatorily has, and finally

[26] GABISON, *cit. supra* note 4, p. 335.

[27] GABISON, *cit. supra* note 4, p. 340.

[28] FAIRFIELD, *cit. supra* note 4, p. 841.

how personal data must be used, managed or processed, including cases where the custody of personal data is outsourced or entrusted to a third-party entity[29]. Again, this and similar regulations seem to have been devised on the basis of the existing common architectures used in the internet (mostly reliant of websites held and operated by a single entity or by a service provider on its behalf, including those where users may upload content, but where information is stored and administered or managed under a centralized authority scheme), without taking into account the distributed and decentralized structured of blockchain networks, with all the aforementioned features (and their distributed architecture in terms of management of the information, as well as their decentralized structure in terms of governance)[30].

Compliance with regulations relating to personal data protection will certainly require that the technology used, also where it is supported on blockchain or a distributed ledger, allows managing the information in a given way; which, again, is a question of design of the technology[31]. From the point of view of the data recipients, controllers or processors this should be a crucial question also when accessing the technology under a service relationship with a third-party provider.

b. Questions related to the use of smart contracts.

Legal issues relating to smart contracts are also worth discussing, since probably (among other things, but most importantly) smart contracts will lead to the automation of many processes in commercial activities, in very different fields. Those industries that are prone to such automation of information-based processes (even where they may entail physical or material actions, such as the movement or handling of goods) are likely to start using smart contracts in the near future (and reality is already showing that among those we must certainly include the supply chain, logistics services and strategies or transportation).

A recurring debate in the smart contract legal literature is whether they may be considered as contracts in a legal sense. According to their current use, where a smart contract is implemented or put in motion, there is a previous agreement of the parties involved which may well qualify as a contract (the legal requirements as set in the law should be met, for this purpose)[32]. We would have to distinguish here different hypotheses; but an important question, as usual in contractual relationships, is whether the parties involved are aware of the nature of a device such as a smart contract and its feasible implications or consequences in the legal field, and whether they consequently have a rational and reasonable strategy in this regard too. Rather than giving an opinion

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[30] GABISON, *cit. supra* note 4, p. 330-331.

[31] See remarks by GATTESCHI, LAMBERTI, DEMARTINI, PRANTEDA and SANTAMARÍA, *cit. supra* note 18, p. 5.

[32] O'SHIELDS, R., "Smart Contracts: Legal Agreements for the Blockchain", *N.C. Banking Inst.*, Vol. 21 (2017), p. 189.

on the advisability of the varying options, it is probably more useful to understand the consequences to be expected in each of them.

First, in some cases a smart contract will be not only result of the will of the involved parties as submitted to their contractual agreement, but also the memorialization of the contract itself[33]. In these hypotheses we can conclude that there is a contract between the involved parties (all conditions being met), but we would have to approach a smart contract from two different angles: the smart contract as the formal reflection of the will of the parties (form), and the smart contract as self-executable code leading to certain actions, in accordance to the agreement of the parties, as a result of the dynamic character of software (performance). As a formal instrument based in a certain language, a smart contract in the first place entails certain interpretation challenges, for part (not all) of which existing rules may be of some help[34]. Contract law on interpretation of contracts, and particularly where there is a written document in which the contract has been memorialized, are based on the assumption that the parties have used written natural language and, although identifying the actual will of the parties as the relevant element and goal of interpretive efforts, take the literal usual meaning of the words or terms employed as a starting point[35]. Some progresses are being made in the field of informatics to replace code with natural language for these and other purposes, but for the time being code is used, which means that part of the existing legal rules seem not to be fit for these sorts of contracts.

In light of this, we may resort to other interpretation tools that contract law provides, which may be of some use in this setting. For instance, coded language may be given a certain natural meaning in accordance to an interpretive usage (such as those existing in commercial contract law and jurisprudence), provided a consolidated and recurring meaning is given to code in the trace (and under certain circumstances)[36]. Alternatively, we may resort to the actions that the execution of the code leads to, as a relevant element to ascertain the will of the parties as reflected in the (smart) contract (and as a result thereof)[37].

In a second hypothesis, the parties using a smart contract may write the code (or have it drafted) in accordance (and as a result) of their previous agreement, which may have been formalized in one or more written documents or not. In this case we would

---

[33] See CLACK, C.D., BAKSHI, V.A. and BRAINE, L., "Smart Contract Templates: foundations, design aspects and research directions" (available at https://arxiv.org/abs/1608.00771, last visit on March 2018), referring to these smart contracts (or to smart contracts in this hypothesis) as "smart legal contracts"; MIK, *cit. supra* note 15, p. 287.

[34] SAVELYEV, *cit. supra* note 13, p. 14.

[35] See, for instance, Art. 4.1 UNIDROIT Principles on International Commercial Contracts 2016 (hereinafter UNIDROIT Principles).

[36] See Art. 4.3 (e) UNIDROIT Principles.

[37] Provided a smart contract is tamper-proof and error-free, it might not make much sense to distinguish, as we have done above, between the smart contract as the formal reflection or memorialization of the agreements of the parties, and the actions or the result of the execution of the code that the smart contract is reflected in, as the latter will necessarily be the result of the former. However, practice has already shown that this might not be necessarily the case, and such an approach, at least theoretically, makes easier to identify legal rules that may be useful in this context in the current state of the law. See for instance Art. 4.2 UNIDROIT Principles.

have to consider a smart contract (its drafting already) as part of the performance of the contract between the parties[38]. In terms of strategy, the parties would be advised to make this explicit in their written agreement; but one way of the other, where such an intention by the parties can be established, a written agreement would take precedence in the interpretation of the will of the parties, and the contents of a smart contract implemented thereunder would have to be approached on that basis. So, for instance, where only one of the parties is assigned the task to draft the corresponding smart contract, any departure in its contents or consequences from the previous contractual agreement (including coding errors) may be considered a breach of contract. Alternatively, the contents of the smart contract, to the extent that it adds to, or departs from the contract, may be used as an interpretation source to complement the latter's content, or to prove the will of the parties to modify the contract's original terms[39].

Once again, this discussion already assumes that when a smart contract is used between two or more parties for the purpose to conduct their relations, there will be a contract, of which the smart contract may be both formal reflection and performance or, alternatively, only performance of the contract. This means that contract law rules will apply to at least several aspects of the situation, but that precisely for that reason the parties will enjoy a wide discretion in disciplining their relationship under the principle of freedom of contract. Interpretation difficulties aside, at least some of the features that we see in smart contracts or the problems that we can imagine thereunder can be fitted in existing contract law rules, and the uncertainties sometimes linked to them can have a solution in legal rules or otherwise subject to contract law notions and principles.

Thus, for instance, the use of oracles in the mechanics that characterize smart contracts can be approached as yet another type of open terms in contracts; open terms that in this case would actually foresee a mechanism for determination of the parties' rights and obligations as per their agreement[40]. Following up with one of the ideas earlier expressed, smart contracts are likely to be used in long term cooperation relationships where automation contributes to the increase of value. In such cases smart contracts may be modified or adjusted gradually, or algorithms may be used to allow the digital infrastructure to adjust to a changing reality, whereas feasibly previous existing written contracts will not be changed. Such circumstances may be framed in the rules addressing the so-called evolving terms in commercial contracts[41].

By the same token, when using smart contracts account must be taken of their feasible limitations as contracts from a legal point of view, their submission to previous agreements and rules, as well as all the consequences of the application of contract law. Sometimes smart contracts, given their autonomy and independence from any subsequent human intervention, and their corresponding usefulness for disciplining

---

[38] See again CLACK, BAKSHI and BRAINE, *loc. cit. supra* note 33, referring to smart contracts in this hypotheses as "smart contract code".

[39] Art. 4.3 (c) UNIDROIT Principles.

[40] See, for instance, Arts. 2.1.14 and 4.8 UNIDROIT Principles; see also MIK, *cit. supra* note 15, p. 296, arguing that the need to rely on off-chain sources as oracles prevents a smart contract to operate in a fully self-sufficient manner.

[41] See again Arts. 4.2 and 4.3 UNIDROIT Principles.

contractual relationships, are presented as "self-enforceable" contracts[42]. Smart contracts do indeed provide for the automated performance of contractual obligations. They may even foresee the application of corrective measures or other remedies, such as a reduction of price, the rejection, restitution and replacement of goods or merchandise, their repair, the payment of penalty clauses, or even the suspension or the termination of the supply of goods or services. Automated implementation of these types of measures or contractual remedies does indeed sidestep the need of litigation that their enforcement normally requires. They may even provide for automated dispute resolution mechanism, to the extent that the resolution of controversies may be submitted to formulaic language, implemented through code and, therefore, likewise automated.

Without prejudice of their advantages, we must again take into account that a smart contract, and its execution, may lead to a breach of contract where it is inconsistent with the agreements of the parties (regardless of the way in which we may ascertain their will), or may be contrary to legal rules. Likewise, we should distinguish between performance of a contract (or contract obligations, including the ones stemming from or characterized as contractual remedies), on the one hand, and enforcement of rights stemming from a contract, on the other. Quick and precise performance may be achieved through smart contracts, to the extent that code is capable to fully reflect and implement all the relevant agreements of the parties. However, and to the extent that enforcement relates to the right of each of the parties to seek recourse to executory remedies in order to have their contractual rights satisfied (again, including the ones characterized as remedies), it seems extremely doubtful that smart contracts may by themselves exhaust the consequences of a contract and be completely self-sufficient. To the extent that contract law rules apply to smart contracts too, parties will always have the possibility to enforce their rights in any way as foreseen in the law, not necessarily in a smart contract where used, subject to control by courts[43].

4. Use cases of blockchain based technologies in transportation and related industries.

As briefly stated at the outset, blockchain and the distributed ledger, cryptocurrencies aside, are generating an amount of discussion, noise and expectations that is probably larger than the volume of actual consolidated use cases that rely on blockchain. Many startups and projects based on the benefits of blockchain to generate value are nowadays constantly blossoming, but no leading actors can still be clearly identified. Those sectors or industries where blockchain/distributed ledger-based technologies are attracting greater attention are those where the logical structure of the blockchain seems to provide an added usefulness, and these prominently include the financial industry, on the one hand, and the supply chain, logistics and transportation industries, on the other.

Transportation and logistics activities and services, like the supply chain, can be described as processes whose main purpose is the movement and management or handling of goods or merchandise; but which are essentially dependent since long ago

[42] See comments by MIK, *cit. supra* note 15, p. 280-281, 284-287; SAVELYEV, *cit. supra* note 13, p. 19.

[43] See comments by CLACK, BAKSHI and BRAINE, *cit. supra* note 33, p. 4.

on information streams. Information systems and flows in these activities have always been devised with the purpose to (to the extent possible) track goods, as well as the events and milestones that may be relevant for the purpose to move them from one place to another from the administrative, the transactional and the strategical angle. This can be said of the different practices followed in trade at each point in time, from the old paper bill of lading and related documents, to the latest visibility solutions provided by third-party logistic service providers. Of course, their usefulness has gradually increased as their sophistication, reach, versatility and effectiveness has also grown. In particular, the ability of digital solutions to gather a greater amount of information, to multiply accessibility thereto, as well as to filter and systematize it in varying ways, has reinforced the usefulness of available data and allowed rationalizing its benefits and feasible applications. The logical structure of the blockchain (a chain of sequenced and interlinked events or actions reflected as a chain of information blocks) fits well into this rationale. An immediate and quite obvious application of the blockchain and the distributed ledger, in the first place, is the representation and allocation of title upon rights or other intangibles (*e.g.*, bills of lading, monetary claims) for transactional purposes (since they were precisely created for that purpose).

As opposed to the open and publicly accessible networks that support many of the existing cryptocurrencies, the solutions that are being forecasted in the aforementioned industries are likely to be offered as services. Therefore, they are structured as private and permissioned service-based networks, with all the ensuing consequences. The probably most prominent use case within these industries is the IBM/Maersk *Global Trade Digitization* platform[44]. The information on this project is still limited, but as it is being presented by its promoters, the offered solution is aimed at providing an information environment targeted to different actors in the supply chain ecosystem, focused on the tracking and traceability of goods and events or actions related to their movement within the supply and the logistic chain. The complete expected usefulness of the solution is still partly known, but the main purposes that the service is intended to serve are the reinforcement of transparency in supply chain relations, the faster and more reliable management of information and tracking of goods and events regarding administrative (customs, export and import) or transactional (contract or ownership related) milestones, and a more efficient aggregation and systematization of data with strategical value[45]. In particular for logistical and transportation purposes, it is aimed at providing a "single source of truth" with regard to all relevant events in the carriage of goods. It has been also announced that the solution will incorporate the possibility to

---

[44] Information on this project can be found at https://www.ibm.com/blockchain/industries/supply-chain (last visit on March 2018), and https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/ (last visit in March 2018).

[45] LUBOWE, B. and McDERMOTT, D., "Trtust in Trade. Towards Stronger Supply Chains" (available at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03771USEN&cm_mmc=OSocial_Blog-_-Blockchain+and+Watson+Financial+Services_Blockchain-_-WW_WW-_-Meet+Alex+Tapscott+Learn+about+the+Blockchain+Revolution+In+Text+Trust+in+trade&cm_mmca1=000020YK&cm_mmca2=10005803&&&cm_mmc=OSocial_Blog-_-Blockchain_Blockchain-_-WW_WW-_-BLOG+In+Body+Text+for+Trust+in+Trade+the+modern+supply+chain&cm_mmca1=000020YK&cm_mmca2=10005803&, last visit in March 2018).

use smart contracts with the purpose to automatize administrative and contractual processes[46], which takes us back to the problems discussed in relation thereto.

This solution, like any other solution with a similar approach in the context of the different possibilities that the use of blockchain networks allows, raises some questions as to its architecture, its "private" character, as well as to its business disruptive effects. As to the architecture and the infrastructure of the network, the solution seems to be based on the involvement of the interested stakeholders (exporters/suppliers, importers, distributors, banks or financial entities, ports or port authorities, export or import authorities, customs or taxation authorities) both as users and as network peers, thereby ensuring a certain level of decentralization. However, its private (privately operated) character and its permissioned accessibility is likely to entail certain consequences. On the one hand, its permissioned character will allow combining the possibility to share information between users, and at the same time to protect such information for interested users (with no hindrance for the information verification process). In terms of governance, this and other aspects of its operation will be nevertheless subject to the authority of the entity or group of entities operating the service, which shows an important difference as compared to fully decentralized networks, where governance is also based on consensus[47]. In this specific aspect, blockchain based services like this one are closer to the central trusted-third party model than to the fully decentralized and distributed network model. Of course, this may raise questions as to the neutrality of the operator of the service and in general its obligations as against users, given that different stakeholders or users may have conflicting interests. This is likely to be carefully managed as part of the added value of the service itself.

Finally, the change and the level of disruption that this type of services may bring about in the logistics or the transportation industry is quite uncertain but worth discussing as well. This is specially so in terms of intermediaries, as changes in information-based processes resulting from emerging digital services very often touch upon intermediation schemes in the first place (in the so-called "reintermediation" that the Internet has brought about). Thus, for instance, as part of the message conveyed in the promotion of the IBM/Maersk project, it is made clear that the service will spare the need to resort to certification authorities or central trusted third parties for verification of the exchanged information. For the purposes of our discussion, we can say that transport intermediaries (such as freight forwarders or agents) undertake in three types of intermediation (or their intermediation may cover three different aspects): the physical or material intermediation (pure receipt and dispatch of goods for the account of their clients, under different contractual relationships -handling, storage and delivery), market intermediation in the provision of transportation services (normally acting as non-vessel operating carriers, and contributing to market transparency, integration of carriage services and intermodality or transportation networks'

[46] See "IBM ad Maersk Demo: Cross-Border Supply Chain Solution on Blockchain", https://www.youtube.com/watch?time_continue=208&v=dcddYatMCGQ (last visit on June 2018).

[47] ABRAMOWICZ, *cit. supra* note 4, p. 16. See comments in CASEY J.M. and WONG, P., "Global Supply Chains Are About to Get Better, Thanks to Block Chain", *Harvard Business Review*, March 13 2017 (available at https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain, last visit in March 2018).

interoperability), and, finally, what we may call "information" intermediation (basically, documentary formalities with public administrations or authorities for export/import purposes). We call this latter aspect information intermediation because formalities and administrative procedures are essentially structured as information processes, where documents (or information in general) have to be submitted to the competent authorities in order to facilitate their supervising or control functions, as the basis of their executory jurisdiction, within the context of the movement of goods or merchandise.

The activities of transport intermediaries very often seek providing value through integration of services, and these will include, to a varying extent, all types of intermediation referred to. In this setting, therefore, changes in the information flows intermediation may affect the whole business of transportation intermediaries. Be as it may, processes relating to the paperwork or the documentary formalities to be fulfilled with bodies or authorities *in situ* (at the ports, airports, terminal points or borders) may no longer need a local intermediary if authorities can be accessed through an electronic communications system[48]. This may force intermediaries to think how other intermediation activities may be affected, how they may still provide added value in a future scenario, or how they may precisely take advantage of the new emerging services (through partnerships or alliances). All this provided that blockchain services like these succeed.

[48] Such a system does not need to rely on blockchain or a distributed ledger network. Preexisting technologies could also provide for such functionality, including those based on trusted third-party service providers. This, however, requires the involvement of public administrations or authorities, which might be eased by the expansion of the blockchain (and the hype it is somehow generating).