

Chapter

Artificial Intelligence and Blockchain: Debate around Legal Challenges

Antonio Merchán Murillo

Abstract

The rapid technological change and its development have led to an era of technology and applications that are leading us to transversal changes, based on the data that feed the Internet. This change is taking place through the Internet of Things (IoT), machine-to-machine (m2m) communications, robotics, big data, blockchain, and artificial intelligence (AI). In this context, it can be seen how artificial intelligence and blockchain are opening up, posing specific legal challenges to those imposed by technologies. Recent developments in AI are the result of increased processing power. The emergence of new traceability and authentication as blockchain can allow recording assets, participant transactions, which can provide valuable information on the origin and history. These facts should lead to study and to make regulatory proposals and to study the existing legal framework.

Keywords: artificial intelligence, ethics, legal framework, blockchain, trust

1. Introduction

Recent discussions have revolved around the need to regulate the AI sphere itself and set limits, to prevent the so-called artificial general intelligence from developing. On the other hand, blockchain is becoming popular, and its continuous attempts to implement it have curiously given confidence to the digital society of the future, although it does pose serious challenges.

Although it must be kept in mind that artificial intelligence (AI) is going to pose challenges in its application, we must not lose sight of the blockchain, which, although it focuses on validation, permanence, and achieving higher levels of certainty, control, and trust, is going to pose the challenge of acting together with AI; that is, blockchain has the mission of generating trust, transparency, and acting as a mediator. So you are going to have the challenge of making it possible for AIs to act and connect with each other.

However, we cannot forget the commercialized cloud (computing) services either. The cloud has become the perfect scenario for AI, and also for blockchain, since, for the development of these applications, not only is a significant calculation capacity necessary during learning

2. Artificial intelligence: aspects to consider

AI-based systems can simply consist of software (e.g., voice assistants, image analysis programs, search engines, voice and facial recognition systems), but AI can also be embedded in devices hardware (e.g., advanced robots, self-driving cars, drones, or Internet of Things applications).

AI is used daily, for example, to translate from one language to another, generate subtitles in videos, or block unsolicited email (spam). Far from being science fiction, AI is already part of our lives, in the use of a personal assistant to organize our workday, in the movement in a self-driving vehicle or in the songs or restaurants suggested by our phones.

AI is about developing systems capable of solving problems and performing tasks by simulating intellectual processes. The AI can be taught to solve a problem, but it can also study the problem and learn how to solve it itself without human intervention. Different systems can achieve different levels of autonomy and can act independently. In this sense, its operation and its results are unpredictable, since these systems function as “black boxes” [1].

Today, there are various definitions of artificial intelligence [2]. However, none of them has been universally accepted [3], a fact that leads us to the first challenge, making a timeless, general, and at the same time, robust definition of AI, especially when one thinks of AI and its normative regulation.

A certain issue cannot be regulated without establishing a solid definition of what is regulated. Therefore, it is essential to establish a generally accepted definition of AI that is common and flexible and does not hinder innovation, considering that AI is becoming more and more sophisticated.

The principles enunciated by UNCITRAL when establishing in their Model Laws on Electronic Commerce or on Electronic Signature the procedures and basic principles, as well as fundamental, to facilitate the use of modern techniques can serve as a starting point of communication, in order to record and communicate information in various types of circumstances, such as: nondiscrimination, neutrality with respect to technical means, and functional equivalence. These principles are widely recognized as fundamental elements of electronic commerce [4]. At the same time, they are reflected in the enunciation of the requirements that electronic communications must meet.

In this way, a common European definition must be established [5], including the definitions of its subcategories, considering the following characteristics:

- a. the ability to acquire autonomy through sensors and/or through the exchange of data with its environment (interconnectivity) and the analysis of the said data;
- b. the ability to learn through experience and interaction;
- c. the form of the physical support of the robot;
- d. the ability to adapt their behavior and actions to the environment.

2.1 Debate of regulations

In our opinion, we must consider a series of methodological and substantive questions regarding the regulation of technology in general and robotics and AI in

particular. In the first place, it is worth asking whether sufficient arguments can be identified to accommodate these new technologies and therefore justify a change in the existing legal framework, that is, are existing laws sufficient to meet the regulatory challenges of the technology, and if not, should some laws be adapted to include the new technology, generally by making the language of the law more technology-neutral or rather should they be *sui generis* laws? With the existing administrative regulations, the lack of interoperability is guaranteed [6].

As we know, interoperability is a very important issue. When we talk about this, we mean that the processes, technologies, and protocols required to ensure the integrity of the data and the identity of the citizen, when they are transferred from one system to another, must entail, by definition, a correct interconnection of the systems and data exchange. However, this is not always carried out, let's think about the right of access.

At the technical level, although standards abound, the lack of common basic standards for some technologies must be highlighted. At the legal level, the laws that prescribe a specific predominant technology are pointed out as factors that impede progress, the difficulty of those responsible in understanding their respective frameworks of mutual trust and even in the areas of liability and compensation [7]. An example of the problem of interoperability is, and sometimes continues to be, the situation that is present in Spain at a regional level and in the EU: State authorities throughout Europe offer electronic access, focusing, above all, on the needs and national media, which has generated a complex system with different solutions, which has given rise to new obstacles to cross-border exchanges, which hamper the functioning of the single market for companies and citizens.

Second, it is necessary to clarify the direct and indirect role that ethics can play in the regulation of technology [8]. The impact of AI is cross-border. The EU is realizing this, trying to regulate its sphere and establish limits. The debates point to 11 areas: ethics, security, privacy, transparency, and accountability, work, education and capacity development, inequality and inclusion, legislation, and regulation; governance and democracy, war, and superintelligence.

These debates are justified and should be taken into account. However, they are part of a larger problem, related to the insufficient conception of artificial intelligence that society has, which makes trust difficult, and to the current laws, which have not yet recognized the specific characteristics of artificial intelligence [3]. In this way, the need arises to analyze and deepen an ethical framework so that both citizens and companies can trust the technology with which they interact, have a predictable legal environment, and have the effective guarantee that they will protect themselves and their fundamental rights and freedoms.

Let us think that technologies based on artificial intelligence influence aspects such as health, safety, productivity, or leisure, and in the medium term, they will have a great impact on energy, transport, education, and domestic activities. Regarding education, it is essential to find new models and methodologies that integrate ethical concerns in relation to the impact of artificial intelligence on humanity, especially in everything related to security, freedom, privacy, integrity, and dignity; self-determination and nondiscrimination, and the protection of personal data [9].

The complexity of AI entails the need to create an ethical and efficient framework, for which the principle of transparency must be based on, which consists of the fact that it must always be possible to justify any decision that has been adopted with the help of artificial intelligence and that can have a significant impact on the life of one or more people. On the other hand, it should always be possible to reduce the calculations of the AI system to a form understandable to humans.

3. Blockchain

Blockchain is a distributed information processing technique on which different treatments and business models can be implemented. The blockchain is a large database that is distributed among various nodes that participate in the chain. This functions as an immutable logbook that contains the complete history of all transactions that have been executed on the network⁵. These nodes are connected in a decentralized network, without a main computer, and they are networks called P2P (network of peers, network between equals) that communicate with each other using the same language that they transmit a message, called a token. The P2P network is a computer network in which all or some aspects work without fixed clients or servers, but rather a series of nodes that behave as equals to each other. They act simultaneously as clients and servers with respect to the other nodes of the network, allowing the direct exchange of information in any format between the interconnected computers. Usually, this type of networks is implemented as overlay networks built in the application layer of public networks as in the case of the Internet. A token (symbol, signal, or token) is a representation of the information that the network contains [10]. The information travels encrypted, due to this, it is distributed without revealing its content, as the number of transactions grows, the chain of blocks grows, and each block has its own digital footprint. Its scope is immense, and Ethereum could replace basically any intermediary, substituting products and services that depend on third parties to be totally decentralized.

3.1 Types

Depending on the permissions required to be part of a blockchain, three categories can be distinguished:

- A. Public: Where anyone can download the necessary programs on their computer and set up a node and participate in the consensus process, anyone who is a party can send transactions through the Internet, which will be included in the blockchain.
- B. Federated or consortium: In this class, they do not allow anyone to configure a node on their PC and participate in the transaction validation process since access permission is needed, which is usually granted to members of a certain group, for example: the group of financial entities.
- C. Private: In these blockchains, the authorizations to carry out transactions are conceived by private organizations that will determine the conditions under which they will allow the reading of the transactions carried out.

3.2 Features

- A. Immutable. Nobody can alter or delete the data in the registry or add new content without any validation. When a transaction occurs, all nodes on the network will have to say that it is valid, or it will not be added to the record.
- B. Decentralization. There is no single person or governing authority that reviews the framework.

- C. Origin: All nodes can verify the moment in which a certain asset has been registered in the block chain, who was its first owner, and all the subsequent changes of ownership that have occurred up to that moment.
- D. Security. All registry data are strongly encrypted, using cryptography, which is one of the most complex mathematical algorithms in existence.
- E. Each block has a unique hash ID (fingerprint) and changing it is impossible.
- F. To carry out a transaction in the blockchain, the use of public and private keys is necessary.
- G. Register distributed. Due to the nature of the technology, all nodes maintain the registry and therefore, the computational power is distributed among them, and the nodes act as verifiers.
- H. Consensus. It is a determining factor. Without consensus, the system does not work. For the information contained in a block to be considered valid, all participants must agree. The network developer needs to implement some kind of consensus algorithm.
- I. Speed. It offers a faster result. For example, a transaction might take a few minutes to complete.

4. Artificial intelligence and blockchain: the need for a joint study

Recent developments in AI are the result of increased processing power, improvements in algorithms, and exponential growth in the volume and variety of digital data. Many AI applications have begun to enter our daily lives, from machine translations to image recognition to music generation, and are increasingly being implemented in industry, government, and commerce. Connected and autonomous vehicles and AI-supported medical diagnostics are soon-to-be-common application areas.

Now, for the other to happen, there must be a communication between the machines that must be validation and with a high level of certainty and control. For this reason, we consider that joint action, if it is not obvious that it must take place, will be important. In fact, it is an issue that is being debated more and more globally.

In this context, a question of trust, transparency, reliability, speed, and effectiveness in automatic electronic transactions arises.

The emergence of new traceability and authentication systems, such as blockchain, can make it possible to record assets, transactions, and participants, which can provide valuable information about origin and history.

In this way, solutions based on blockchain can enable the rapid detection of possible illicit or defective actions within the system itself, products to illicit markets. In this way, it is evident that the deployment of digital technologies, such as blockchain, is key to the development of AI.

In this context, Regulation (EU) 2018/1807 of the European Parliament and of the Council, of November 14, 2018, regarding a framework for the free circulation of non-personal data in the European Union, arises from the need to establish administrative

cooperation, based on the review of the European Interoperability Framework; however, with this standard we only intend to make you see that development is a reality.

Now, it should be borne in mind that the current regulations have not yet recognized the specific characteristics of the contracts that may arise, and neither blockchain technology nor artificial intelligence, it is true that in the cloud environment (computing), things have been developed in UNCITRAL.

For example, in the absence of direct legal regulation of AI, article 12 of the United Nations Convention on the Use of Electronic Communications in International Contracts, which establishes that a person (either a natural or legal person) on whose behalf a programmed computer was used should be responsible for any messages generated by the machine. However, in the explanatory note, UNCITRAL makes it clear that this article is an enabling provision and should not be misunderstood as transforming an automated message system or a computer into a subject of rights and duties. Electronic communications that are generated automatically by a computer or messaging system without human intervention should be interpreted as “coming from” the legal entity on behalf of which the computer or messaging system operates. The issues relating to the subject of the action that could arise in this context must be settled in accordance with rules outside the Convention, which returns us to the previous point. In any case, in our opinion, it is of vital importance to establish a legal framework, especially in an international context, in which its real applicability is included [11].

To give security to the transaction to be carried out, blockchain arises, as a decentralized technology, which entails some legal uncertainties, such as the legal nature of blockchains and shared digital records, which includes problems of judicial jurisdiction and applicable law; thus, each network node may be located in a different place as there is no “central party” responsible for the digital registry, whose nationality could serve for regulation.

As we say, as the Internet becomes part of everyday life, the need arises to study the adaptation of private international law systems to the new demands [12]. For this reason, our intention is to analyze, deepen the debate, and respond to the problems, succinctly raised, in order to contribute, as far as possible, to give certainty to the responsibility, due diligence, contracts on intelligence systems artificial, as well as the condition of artificial intelligence and the attribution of its acts of legal significance and the use of blockchain technology in the formation of smart contracts, to mention some pertinent issues, as we say, from a private international law perspective.

4.1 The existing international law

The agreements attributing jurisdiction included in the underlying contract are relevant to the extent that they are effective in accordance with the rules of our private international law system (in principle, in accordance with the provisions of Regulation 1215/2012 – Brussels Reg. I bis), which significantly restricts its operability in transactions with consumers.

Aside from these transactions, it will be necessary to observe the eventual incidence of special rules such as that of article 25.2 Brussels I bis Regulation with respect to the written form in electronic contracting, presupposition of the effectiveness of the agreements attributing jurisdiction. Likewise, the situations in which the special jurisdiction of article 7.1 Regulation 1215/2012 becomes applicable must be observed, and it may be controversial to what extent the automation of certain benefits

conditions the determination of the place of fulfillment of the obligation for the purposes of that rule.

In relation to the applicable Law, we are going to bear in mind issues that have to do with the meaning of the automated fulfillment of certain commitments and its interaction with the underlying relationship between the parties. The basic criterion is that the provisions of the Rome I Regulation (including its specific consumer protection regime and the application of rules transposing the Directives on consumers) must be followed in principle in relation to the underlying transaction between the parties, without ignoring that the application of certain provisions may be a source of controversy—for example, its art. 14.2 and the specification in this framework of the place of compliance—as well as that other regulatory instruments may also be relevant.

For example, the origin criterion of the Directive on electronic commerce in relation to the contractual aspects included in the coordinated scope of the Directive when it is applicable. It will also be necessary to take into account the existence of issues subject to autonomous connection, among others, the ability to contract and, very especially, everything related to the applicable regime in terms of personal data protection, in which it will be necessary to comply with the provisions in article 3 RGD regarding the need to comply with its provisions in the situations included within its scope of territorial application.

However, notwithstanding the foregoing, the evidentiary effectiveness to accredit transactions or other circumstances within the framework of judicial proceedings will in principle be determined, as a procedural matter, by the *lex fori*.

In the context of the EU, Regulation 910/2014, regarding electronic identification and trust services for electronic transactions in the internal market and which repeals Directive 1999/93/EC, is of particular relevance for these purposes.

4.2 Problems associated with AI, blockchain

All this in accordance with the principle of preexistence of existing law. Now, in the underlying contractual relationship we are going to find cases in which the technology can be given a non-nationality, as we have seen before, and we may encounter problems in the connection criteria, cross-border insolvencies that blockchain detects, etc., are problems that, if not now, they will be over time, when artificial intelligence advances and also companies evolve to the cloud.

Why?

The blockchain poses different risks because of the technology and the way of operations: One of the main problems that will affect the blockchain is the inability to control and stop its operation. In addition, the lack of control over the operation can lead to the lack of responsibility of the company that manages the platform. Let us think that, in its simplest form, blockchain is a decentralized technology or a distributed ledger in which transactions are recorded anonymously. This means that the transaction ledger is simultaneously maintained on a network of unrelated computers or servers.

Therefore, the allocation and attribution of risk and responsibility in relation to a blockchain service that is not working properly will have to be carefully analyzed, not only at the provider-customer level, but also around all the participants in the system.

It should be noted, regarding the process, that blockchain has the ability to cross-jurisdictional boundaries since the nodes in a blockchain can be located anywhere in the world.

This can pose a series of complex problems that require careful consideration in relation to citizen-State, company-State, company-company, citizen-company, company-administration, citizen-Administration relations of the same State, and of different ones. In this regard, it should be noted that, in a decentralized environment, it may be difficult to identify the appropriate set of rules to apply. Estonia does.

And it does so by proposing electronic identity as a connection criterion, since it is related to residence, in this case electronic [13], insofar as the need to link information and its management, solely, with the person who issues it, becomes essential for numerous different interactions: an organizational infrastructure (identity management) and a technical infrastructure (identity management systems), to develop, define, designate, manage, and specify authorization levels, assigning roles and identity attributes related to specific groups of people, such as company directors, employees, or customers.

The evolution of technology is creating large electronic files, with it, large commercial and state databases. A national identifier, contained in an identity card, allows capturing information about a person, which is found in different databases, so that they can be easily linked and analyzed through certain data analysis techniques. At the same time, ID cards are also getting smarter. The generation of data also has the potential to be offered in a medium where they can be directly processed. In this way, files that can be crossed and structured, as well as transferred, are created. For this reason, you have to pay special attention to any identity management system and see who are where people are.

At its simplest level, each transaction could fall within the jurisdiction of the location of each node in the network. With this, it should be noted that in an online environment, authenticating the identity of the remote party is more important than ever. It plays a key role in the fight against identity fraud and is also essential to establish the necessary trust that facilitates any type of electronic transaction.

At this point, it should be taken into account that the relationship between Law and IT goes beyond what has been seen so far [14]. That is why one of the main issues that arise, with respect to cross-border services, is the security and confidentiality of information transmitted over the Internet, which should lead us to guarantee the protection of personal data that lead to the identification of its owner.

By this, we mean that the electronic identity is an identity that is made up of information stored and transmitted to the different users of it. Let us think that the identity is a fundamental element, which links the information to its owner, located in some State, giving rise to its location, and therefore, to the effective and safe handling of the specific data that enter the cloud.

We must keep in mind that all electronic identity schemes depend on two processes: first, identity authentication and, later, identity verification. When authenticated, the identity is registered in the system and can then be used for transactions. Identity is verified at the time of each transaction, from within the cloud itself. From the information registered at that moment, the identification information arises or that will identify the person, as if it were the signature, which will be used, later, to link an individual in an inseparable way.

We observe that within the cloud, there will be two elements that will come together to facilitate the identity of the person who intends to access the cloud. These two fundamental elements are the identity fixed to the individual and another fixed to the transaction that is carried out [15]. The first will be the one that identifies the parties and, therefore, will have a direct effect on the formation and enforceability of the contract, thus determining its capacity to be contractually bound, by including

elements such as the name of the legal person, its form legal, its registration number in the registry (if applicable), its registered office or address of the business center, together with the mention of its founding documents. The second would be the largest body of transaction information, and it is continually updated, based on the transactions you make in the cloud.

If the above is not enough, it will be necessary to assess the specific contract and the specific links, of the said contract, with the different countries attending, as indicated by the CJEU, in its Judgment of October 23, 2014, case C-305/13, to the “overall assessment of all the objective elements that characterize the contractual relationship and assess the element or elements that, in his opinion, are more significant” and “in the event that it is alleged that a contract has closer ties with a country” other than the country whose law is designated by virtue of the presumption established in said section, the national court must compare the ties between the contract and the country whose law is designated by virtue of the presumption, on the one hand, and between the contract and the other country in question, on the other. The national judge must consider all the circumstances that concur, including the existence of other contracts related to the contract in question [16].

In this way, issues related to identity management must be regulated by the different legal systems that discipline the multiple activities of the specialized operators that carry out the identification tasks and the functional operators. In this context, it must be considered that the eIDAS Regulation does not impose the creation of national electronic identification schemes as such, but rather aims to guarantee their interoperability by applying the principle of mutual recognition.

Let us think that the identity is a fundamental element, which links the information to its owner, located in some State, giving rise to its location and, therefore, to the effective and safe handling of the specific data that enter the cloud. We must keep in mind that all electronic identity schemes depend on two processes: first, identity authentication and, later, identity verification. When authenticated, the identity is registered in the system and can then be used for transactions. Identity is verified at the time of each transaction, from within the cloud itself. From the information registered at that moment, the identification information arises or that will identify the person, as if it were the signature, which will be used, later, to link an individual in an inseparable way.

On the other hand, we could find ourselves in situations in which the parties intervene in unequal conditions, the applicable laws on contracts usually establish that the contract in question is a contract of adhesion. Service providers are often familiar with a limited number of local laws, and especially local laws governing contracts and the right to privacy. For that reason, they will proceed to choose an applicable law that establishes the requirements related to the protection of information that the service provider in question can or is willing to comply with, which offers rules for the elaboration of contracts that are predictable and acceptable to their purposes.

These issues may force the client company to assume certain responsibilities toward its end users in relation to the determination of the applicable type Law, which may be abusive.

Given this, as indicated by the Judgment of the CJEU, dated July 28, 2018, case C-191/15, when appreciating the abusive nature of a certain contractual clause in the framework of an action for injunction, of article 6, section 2, of the Rome I Regulation, it turns out that the choice of the applicable law is made without prejudice to the application of the mandatory provisions provided for by the law of the country in which the consumers whose interests are defended by means of that action reside.

Such provisions may include those transposing Directive 93/13, provided that they guarantee a higher level of protection for the consumer. At this point, the main legal risk that arises for the client company is not being able to fully assess the risks linked to the contract, for example, ignorance of the weak points inherent in the technology that is being used; missing or inadequate security features; economic risks linked to the loss of data or breaches of the agreement, etc.

5. Conclusion

The need arises to analyze and deepen an adequate legal framework, so that both citizens and companies can trust the technology with which they interact, have a predictable legal environment, and have the effective guarantee that their rights will be protected and freedom.

For this reason, we propose the need to review certain criteria to prevent liability from being diluted with respect to the operations carried out by service providers, if the criteria for the applicability of the legislation are not sufficiently clear.

Additional information/notes/thanks/other declarations

The information in this chapter is based on the work published, by the author, in 2019 in the *Administrative Law Review*, 2019 (50). Being, therefore, an update, evolution, and revision of the conclusions reached.

Author details

Antonio Merchán Murillo
Pablo Olavide University, Spain

*Address all correspondence to: amermur@gmail.com

IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] UNCITRAL. Legal issues related to identity management and trust services. New York Times. 2017
- [2] Čerka P, Grigienė J, Sirbikytė G. Is it possible to grant legal personality to artificial intelligence software systems? *Computer Law & Security Review*. 2017; **33**:685
- [3] UNCITRAL. A/CN.9/960 – Work Programme of the Commission – Legal Aspects of Smart Contracts and Artificial Intelligence: Submission by the Czechia. New York: United Nations; 2018
- [4] Illescas R. Law of Electronic Contracting. 2nd ed. Madrid: Civitas; 2019. p. 508
- [5] European Commission. Artificial Intelligence for Europe {SWD(2018) 137 final}, Brussels, 25.4.2018 COM(2018) 237 final. 2018
- [6] López de Mantarás R. Ethics in artificial intelligence. *Research and Science*. 2017; **48**:49
- [7] Gurkaynak G, Yilmaza I, Hakseve G. Stifling artificial intelligence: Human perils. *Computer Law & Security Review*. 2016; **32**:758
- [8] Čerka P, Grigienė J, Sirbikytė G. Liability for damages caused by artificial intelligence. *Computer Law & Security Review*. 2015; **31**:376-389
- [9] European Commission. Proposal for a Regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final} Brussels, 21.4.2021. COM(2021) 206 final. 2021/0106(COD). 2021
- [10] De Filippi P, Wright A. Decentralized blockchain technology and the rise of lex cryptographia. 2015. Available from: https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRNid2580664.pdf
- [11] UNICTRAL. Text—Explanatory Note United Nations Commission on International Trade Law. New York: United Nations; 2007
- [12] BURDEN K. EU update. *Computer Law & Security Review*. 2018; **34**:418
- [13] Diago, M^aP. La residencia digital como nuevo factor de vinculación en el Derecho Internacional Privado del Ciberespacio ¿posible conexión de futuro? *Diario LA LEY*. 2014; **8432**(2):2-8
- [14] Viguera Revuelta R. The computer contracts. *Revista de la Contratación Electrónica*. 2008; **97**:61
- [15] Cuthbertson A. Estonia First Country to Offer E-Residency Digital. *International Business Times*. 2014. Available from: <https://www.ibtimes.co.uk/estonia-first-country-offer-e-residency-digital-citizenship-1468766>
- [16] UNCITRAL. A/CN.9/WG.IV/WP.162 - Draft Provisions on the Use and Cross border Recognition of Identity Management and Trust Services. New York: United Nations; 2020