# Legal Challenges of Block chain for e Government Application

**Andrea Peláez-Repiso[1], Pablo Sánchez-Núñez[2], Francisco E. Cabrera[3] and Luis Ayuso[4]**

[1]Facultad de Derecho, Universidad de Málaga (Spain)

[2]Programa de Doctorado en Comunicación por la Universidad de Cádiz; la Universidad de Huelva; la Universidad de Málaga y la Universidad de Sevilla (Spain)

[3]Departamento de Lenguajes y Ciencias de la Computación, Escuela Técnica Superior de Ingeniería Informática, Universidad de Málaga (Spain)

[4]Departamento de Derecho del Estado y Sociología, Facultad de Ciencias Económicas y Empresariales, Universidad de Málaga (Spain)

## Abstract.

In the last year, the concept of distributed ledgers has entered mainstream company and policy agendas. Between different types of ledgers, it can be said that blockchain is the most notable. Different studies have shown that blockchain technology can reduce bureaucracy, increase the level of trust in public recordkeeping. In order to make further progress in its implementation in the different areas, it is necessary first of all that technological and ecosystem maturity of distributed ledgers have to increase in order to unlock the transformative power of blockchain; and in second instance the Policy agenda should focus on non-technological barriers, and create new administrative processes that can be re-engineered for blockchain. But, this new context, faces new legal challenges: personal data, free circulation of data..., which must to be analysed. The main objective of this paper is to analyse the new legal challenges from technical and methodological points of view.

**Keywords:** Blockchain, eGovernment, Personal Data, Legal, Transparency.

## 1. Introduction

We currently live in the Information Society, where new technologies have become protagonists, becoming part of a multitude of sectors of our society. One of the sectors that has gained special importance its introduction, is in the public sector, giving place to the concept of eGovernment (Lee, Tan, & Trimi, 2005).

The eGovernment consists of the implementation of new technologies to serve the functioning of the State. It is a model that is based on transferring to the digital world the operations of the government, such as government connections with the citizen, companies or other governments, bureaucratic procedures, or the administration and management of

documents under the responsibility of the State (Harrison et al., 2012; Napoli & Karaganis, 2010). These efforts are made with the goal of increasing transparency, preventing fraud, increasing the participation of citizens in controlling the actions of the administration, as well as achieving greater efficiency in Public Administration, streamlining processes and reducing costs (Wallace, 2018).

In order to make this possible, it is necessary to have a support for its application, based on computer architectures. One of the most novel and revolutionary architectures that currently responds to these needs is Blockchain technology, also known as chain of blocks (Ølnes, Ubacht, & Janssen, 2017).

The Blockchain technology provides a database formed by a decentralized and distributed network, it is like a book of records, in which thousands of users are connected through their computers, which have access to the registered information and have an unalterable copy of that record (Alexopoulos, Charalabidis, Androutsopoulou, Loutsaris, & Lachana, 2019). It is also a network that allows numerous transactions to be carried out without the need for intermediaries or any higher authority (Tasatanattakool & Techapanupreeda, 2018).

But as with any new technology, it must comply with regulations in order to protect the rights of citizens. This presents a problem as Blockchain is very recent and, to the best of the authors knowledge, there is no regulation has been made with this technology in mind, therefore it must adapt to existing regulations (Franciscon et al., 2019; Niranjanamurthy, Nithya, & Jagannatha, 2019).

The blockchain technology implies that information is decentralized, and many people have access to it, causing legal consequences in terms of data protection, which must be studied in order to work on possible solutions (M. Finck, 2018).

The objective of this work is to analyse the legal aspects that Blockchain must comply with, and some which are not mandatory, in its implementation as part of an eGovernment application, with regards to the legal aspects of private information protection. To this end, the work has been organized as follows: in the second section a background is presented, and the uses of blockchain for Digital Government are introduced, as well as the legal framework of application in this topic. In this work, we are going to consider the Legal Framework of the European Union as it is one of the most advanced, and subsequently the Spanish regulation is applied, as an example of the concretion of a legal framework. In the third section a legal analysis is carried out, and the work ends with the conclusions.

## 2. Background

### 2.1 Blockchain for Digital Government

Blockchain is one of the most interesting information technologies at present and has been highlighted by the World Economic Forum as one of the main emerging technologies. Etymologically speaking, Blockchain is an English term derived from the concept of "chain of blocks" that it employs for the storage of information, which is a rather unconventional approach for data storage designed to make the society more transparent and more truthful.

The Blockchain model was defined in 2008 by Satoshi Nakamoto and this revolutionary system was rapidly applied in the crypto currency, in his paper entitled "Bitcoin, A peer to peer Electronic Cash system", it was described it as a peer-to-peer system, through which crypto currencies could be executed safely. Since then, the applications of this new technology have evolved, and today it is considered one of the most innovative, and its application to numerous sectors of society is the object of study (Legerén-Molina, 2019).

Through this system we can store information and carry out transactions without intermediaries, all thanks to the characteristics it presents:

1. It is a decentralized network. The transactions made are automatically recorded a copy in each node in each device of the user connected to the network. Therefore, a multitude of people will have access to this information, being able to verify that it has been carried out and checking that there is no attempt of alteration. This feature provides security, as it makes hacking almost impossible and impractical, as it would require thousands of computers and would spend a lot of energy and money trying to eliminate the copy of each user. So, you would spend more than you could get by hacking the system. In addition, this feature would also provide transparency, as users know in real time, every transaction or information entered into the system (Rizal Batubara, Ubacht, & Janssen, 2019). However, in the legal field, this feature has consequences with respect to data protection regulations (Porxas & Conejero, 2018).
2. Immutability. The information you enter cannot be deleted or modified. Only information can be added. On the one hand this feature prevents fraud, prevents any manipulation. If an attempt is made to modify data contained in an already validated block, it would cause the Hash to be changed and consequently that of the following blocks as a domino effect. This would be detected by the participating nodes or users and the string would be invalidated. On the other hand, the immutability of the entered information, in combination with the its ease of access by everyone, generates more legal consequences with respect to the Personal Data Protection legislation (Legerén-Molina, 2019).
3. Absence of intermediaries. The certification and security of documents are not given by a notary or a superior institution, they are given by the users. From this characteristic a greater flexibility in the system is acquired, reducing costs and time in procedures.

The users that can be found in the network are of two types, on the one hand, there are the users, who want to use the network, make transactions and exchange information, and on the other, there are the miners, who create the blocks where the information is stored. The latter create the blocks from mathematical operations and then add them to the chain where users validate, and if it is correct begins to replicate in all nodes. In this way the miners charge for their services (Dolader Retamal, Bel Roig, & Muñoz Tapia, 2017).

Regarding the functions that can be performed, in addition to its registration function, by storing information, also allows us:

- The exchange between your users of money, securities, rights... through tokens. Tokens are the creation of digitized assets. And in the Blockchain system they function as means of exchange.
- It allows the creation of Smart contracts. These contracts allow token transactions to be made through the Blockchain network. Besides, its execution is linked to a pre-programmed condition, so that when that condition is met, the contract will be executed by itself. These also have legal consequences regarding their modality as a contract and their validity (Legerén-Molina, 2014).

It is worth mentioning that the original technology has evolved giving rise to different types of blockchain, depending on who has access to the information, so when implementing a blockchain solution there are three possible technologies (Lin & Liao, 2017):

- The first access policy is the Public blockchain, which are characterized by the fact that anyone can participate in the network and every participant has access to the information contained in the blockchain. As it is an open network participant do not need permissions to access and their identity can be anonymous. This type of chain is best suited to the use of intelligent contracts. Notable examples of this type are Bitcoin and Ethereum.
- Secondly, the Private blockchain does not grant access to everyone, instead you need permission from the creator. The identities are known by the creator or managing organization where the permissions are centralized. The number of users is limited as well as the actions they can perform. These chains would lose the characteristic of transparency of the information presented by the public as their autonomy focuses on a single organization. They are mostly used by companies with the goal of maintaining greater privacy. Examples of this type are Hyperledger or Multichain.
- Lastly, we find the federated or consortium. In this case the autonomy does not have a single organization, but several that unite to decide the conditions of the network with a group leader coordinating this interaction. These are partially decentralized systems which are mostly more used in the financial sector. One example of this usage by a financial institution can be found in R3(Banks) (Legerén-Molina, 2019).

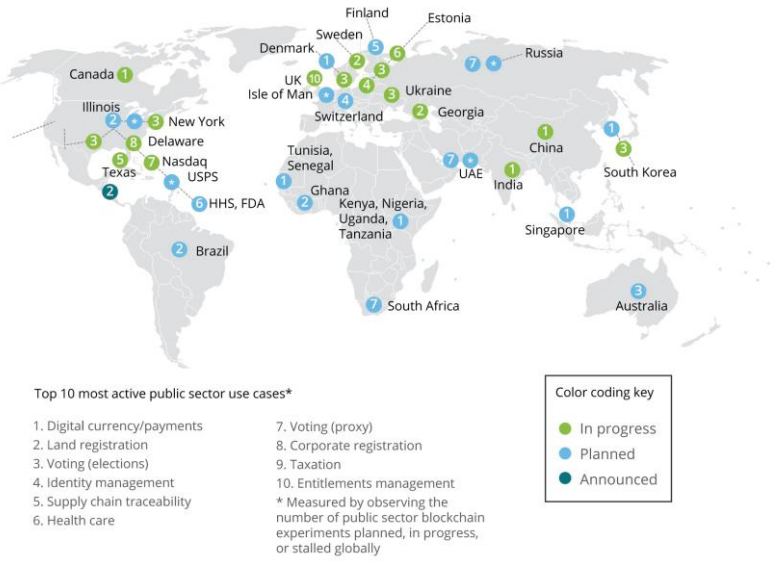
In short, Blockchain is a technology that we must consider in the government framework because it would bring us numerous benefits such as:

- Reduced economic costs, time and complexity of government information exchange processes. It would increase the connections between government and citizens and between public administrations. For example, public institutions could exchange information about taxes or crime quickly and cheaply.
- Reduction of bureaucracy, discretionary power and corruption, using distributed accounting books and the use of intelligent contracts.
- Increases of automation, transparency and accountability of information in government records for the benefit of citizens.

- Increased confidence of citizens and businesses in government processes and records as they are not under the sole control of government (Allessie, Sobolewski, & Vaccari, 2019).

Given the strong points of blockchain technology, it is no surprise that many more companies, countries and international organizations (Figure 1) are adopting it for their capabilities of providing transparency, participation, traceability and security.

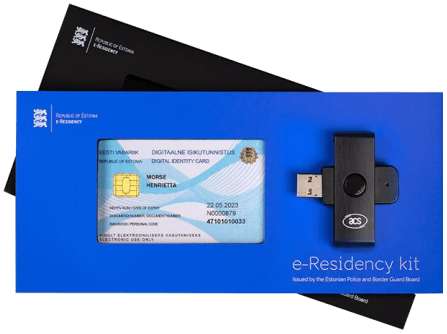
*Figure 1: Blockchain in the Public Sector, as of March 2017. Blockchain experiments in the public sector are accelerating globally, with a concentration in the US and Europe.*




*Source: Deloitte Analysis in conjunction with the Fletcher School at Tufts University. Deloitte University Press.*

An example of the implementation of this system is the Estonia's government, that in the 90' began to build the foundations for today's e-services. The country created a population database, which included an individual's name, ID code, date of birth and place of residence ("Blockchain — e-Estonia," n.d.). The country developed an online identity system and digital signatures that enables citizens to easily verify themselves when performing online tasks such as banking and voting. They are also the creators of the first international e-Residency programme (Figure 2) that enables digital entrepreneurs to start and manage an EU-based company online.

*Figure 2: Estonia e-Residency kit.*




*Source: https://e-resident.gov.ee/welcome/.*

### 2.2 Legal Framework

Blockchain is a new technology that does not yet have a specific regulation. That is why it must be adjusted to the current legislation. However, due to its characteristics, it conflicts with data protection regulations.

The legislation in which we will base ourselves to know the limits of this technology is the following one:

- Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016, on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Organic Law 3/2018 of 5 December on the Protection of Personal Data and the guarantee of digital rights

Also we will make a mention on one of the functionalities that contain Blockchain, the one to realize intelligent contracts, the same ones will have to adjust to the general principles of the contracting, to the rights and obligations gathered in the country of execution, in our case to the Spanish Civil Code.

## 3. Legal Review

The technology advances in a fast way with respect to the legislation, and for that reason, it is necessary to evaluate the legal aspects that affect the Blockchain technology, so that it allows us to continue advancing.

First, before going into the aspects that produce legal consequences in Blockchain, we must know why the data protection regulations apply. The Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016, on the protection of natural persons about the processing of personal data and on the free movement of such data, protects the personal data of natural persons of European citizens. Therefore, the data of legal entities spilled in Blockchain will not have this protection. On the other hand, in spite of the fact that the Blockchain data are encrypted by cryptographic techniques, such as the so-called Hash,

the Regulation will also be applicable and so the European Data Protection Authorities in the Working Group, Article 29, clarify that they include as personal data any encrypted data, including through the use of Hash, algorithms in the block strings. Also, the jurisprudence of the TJUE, of the Second Chamber of the TJUE, in its sentence 582/14 of October 19, 2016, establishes that when the pseudonyms combined with other data allow to identify the person, these data will have personal character.

Therefore, all the data poured in blockchain, of personal character, whether encrypted by cryptographic techniques or pseudonyms, and always within the European framework, the Data Protection Regulation of the European Union will be applicable to them.

Furthermore, in countries such as Spain, its Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights, we must bear in mind that it also extends the protection of the data of deceased persons, in its Article 3.

Once we know that the European Data Protection Regulation applies and is complied with, we move on to analyse what aspects influence it. On the one hand, this system complies with some of the essential elements protected by the regulation, such as consent requirements. The proof of this is recorded in the system's transaction history, which shows that users always validate and verify the information that enters the chain. On the other hand, it complies with design privacy with pseudonyms and hash algorithms, users' information regarding personal data is encrypted.

However, there are other points that conflict, due to their decentralized and immutable nature, and they are the following:

- Right to rectification. The immutable character, implies that once the block is closed the information cannot be modified, which is incompatible with the right to rectification contained in Article 16 of the Data Protection Regulation of the European Union, which must allow the data subject to rectify data that are inaccurate. By means of the Blockchain system it will only be possible to add information but never to modify it.
- Right to erasure (‘right to be forgotten’). With the immutable character, it also implies that the information cannot be deleted. Once information is added to the chain and validated, it is impossible to remove it. This is incompatible with the right to erasure, contained in Article 17 of the Data Protection Regulation of the European Union, since the interested party has the right to have his personal data deleted if he so requests.
- Principles relating to processing of personal data. As we do not know the period of conservation of the information in Blockchain, it is incompatible with Article 5 of the Regulation, about the principles relating to processing, since it provides for the limited conservation of information.
- Data controller. Regulated in the chapter IV of the Regulation. At Blockchain there is no Data Controller. Due to the decentralized nature of Blockchain, each participant in the network is placed on an equal footing with the others regarding the transactions, each one validates and verifies its own information and that which includes the others. So, there is no single figure to whom to turn in order to be able

> to exercise the rights in the regulations, or who determines the data and purposes of the processing, or in short who controls that the obligations established by the regulations are fulfilled. In this way, there is also no third party responsible, such as the data protection delegate, if the large-scale data requirements are met (EUBlockchain, 2018).

Currently in Europe there are no case law pronouncements regarding Blockchain and Data Protection. However, we highlight the report of the European Parliament: "Blockchain and General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?" On the possibility that these digital books can be brought into line with European data protection regulations. It sets out what is needed to bring regulations into line, and that is through regulatory guidance, support for codes of conduct and certification mechanisms to provide greater legal certainty and also funding for research, as it considers that solutions could be found through interdisciplinary research, the development of technical and governance solutions and experiments with block chain protocols (Michele Finck, 2019).

It should be noted that there are already companies working on possible solutions for blockchain and its adaptation to certain elements of the Regulation. For example, work is being done to incorporate an "editable blockchain", by means of which the information entered can be modified or deleted (Legerén-Molina, 2019).

With respect to Blockchain's functionalities, such as Smart Contracts, with respect to its legal aspects, these contracts will be valid if they respect the requirements of the Civil Code and the specific legislation depending on the object of the contract (Legerén-Molina, 2014).

## 4. Conclusion

Society has undergone a process of transformation in the way it works, leaving behind traditional forms of organization and becoming a Globalized Society.

Furthermore, with the arrival of the Information Society, where technologies have come to stay, adapt and provide benefits, they demand from the State a process of modernization and implementation of new technologies for the development of their management and organization.

Through eGovernment, this implementation of new technologies is made possible. And it is that more and more information is stored and managed, which makes more difficult and costly the administrative tasks of governments. A new technology appears for it, the Blockchain technology which brings us numerous benefits that until today we had not seen.

Through this technology there are many initiatives that could be carried out, speed up the processes of Public Administrations, increase the transparency of information, gain trust with citizens by increasing their connection with the State, prevent fraud or develop Smart Contracts, and all from its distributed database.

The problem is that the technology progresses in an unstoppable and fast way, this causes the regulations that regulate it to become obsolete, not adapting to the new technological challenges. Therefore, it will be necessary to carry out legislative work that, considering the

characteristics of the technology, adapts to its use, without forgetting the protection of citizens' rights.

For that reason, in Blockchain and its possible use in the eGovernment, in which it contributes us numerous benefits, it will be necessary to consider the aspects that limit us its use, in this case in front of the regulation of Personal Data Protection. With the purpose of solving it by means of a compromising and innovative legislative work. In such a way that the regulations never suppose us an impediment in the technological evolution of our society.

## References

Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Loutsaris, M. A., & Lachana, Z. (2019). Benefits and Obstacles of Blockchain Applications in e-Government. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 3377–3386). https://doi.org/10.24251/HICSS.2019.408

Allessie, D., Sobolewski, M., & Vaccari, F. (2019). *Blockchain for digital government*. https://doi.org/10.2760/93808

Blockchain — e-Estonia. (n.d.). Retrieved January 21, 2020, from https://e-estonia.com/tag/blockchain/

Dolader Retamal, C., Bel Roig, J., & Muñoz Tapia, J. (2017). La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía Industrial*, (405), 33–40.

EUBlockchain. (2018). Blockchain and the GDPR, 4–31. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, *4*(1), 17–35. https://doi.org/10.21552/edpl/2018/1/6

Finck, Michele. (2019). Blockchain and the General Data Protecion Regulation: Can distributed ledgers be squared with European data protection law?, (July). https://doi.org/10.2861/535

Franciscon, E. A., Nascimento, M. P., Granatyr, J., Weffort, M. R., Lessing, O. R., & Scalabrin, E. E. (2019). A Systematic Literature Review of Blockchain Architectures Applied to Public Services. In *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 33–38). IEEE. https://doi.org/10.1109/CSCWD.2019.8791888

Harrison, T. M., Guerrero, S., Burke, G. B., Cook, M., Cresswell, A., Helbig, N., … Pardo, T. (2012). Open government and e-government: Democratic challenges from a public value perspective. *Information Polity*, *17*(2), 83–97. https://doi.org/10.3233/IP-2012-0269

Lee, S. M., Tan, X., & Trimi, S. (2005). Current practices of leading e-government countries. *Communications of the ACM*, *48*(10), 99–104. https://doi.org/10.1145/1089107.1089112

Legerén-Molina, A. (2014). Revista de derecho civil. *Revista de Derecho Civil*, *5*(2), 193–

241. Retrieved from http://www.nreg.es/ojs/index.php/RDC/article/view/320

Legerén-Molina, A. (2019). Retos Jurídicos Que Plantea La Tecnología De La Cadena De Bloques. Aspectos Legales De Blockchain. *Revista de Derecho Civil*, *VI*(1/2019 (enero-marzo)), 177–237. Retrieved from http://nreg.es/ojs/index.php/RDC

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, *19*(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01

Napoli, P. M., & Karaganis, J. (2010). On making public policy with publicly available data: The case of U.S. communications policymaking. *Government Information Quarterly*, *27*(4), 384–391. https://doi.org/10.1016/j.giq.2010.06.005

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, *22*(S6), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Porxas, N., & Conejero, M. (2018). Tecnología blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados. *Actualidad Juridica (1578-956X)*, (48), 24–36. Retrieved from http://mendeley.csuc.cat/fitxers/03215a0f4b323221f47f7f5adf377d9a

Rizal Batubara, F., Ubacht, J., & Janssen, M. (2019). Unraveling Transparency and Accountability in Blockchain. In *20th Annual International Conference on Digital Government Research on - dg.o 2019* (pp. 204–213). New York, New York, USA: ACM Press. https://doi.org/10.1145/3325112.3325262

Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. *International Conference on Information Networking*, *2018-Janua*, 473–475. https://doi.org/10.1109/ICOIN.2018.8343163

Wallace, A. (2018). Governance at a distance? In *Social Policy Review 21* (pp. 245–266). Bristol University Press. https://doi.org/10.2307/j.ctt9qgs5h.16