Smart Contracts and Blockchain Tokens in light of the General Data Protection Regulation

Jodelismarko Mamoré de Melo
jodelismarko.melo@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

Novembro 2021

Abstract

Lately, different areas of knowledge have come together to solve problems in the modern world. Problems related, among others, to health, education, culture, leisure. People with different perspectives, from different places, with different cultures working together to achieve a common goal. The relationship between technology and law interferes in people's lives. Therefore, it is not new that the conflict between legal norms and technological development raises great debates and many studies. But, the entry into force of the General Data Protection Regulation and the rapid expansion of blockchain technology further fueled this debate. However, the two areas do not always agree. At certain points, technology calls for legislation to be updated. While elsewhere, the legislation makes it impossible to continue the development of the technology. Thus, data protection came to be dealt with both in the legal sphere and in the world of technology.

In this scenario, this dissertation aims to analyze the points of conflict between the legal norm and technology, namely the GDPR and the Blockchain. The requirements presented by the GDPR, whose objective is the protection of the personal data of the natural person, are investigated. The regulation presents principles, guarantees rights and determines obligations. Some of these requirements present themselves as real challenges to blockchain technology. The right to portability, the right to be forgotten, the right to rectification and the prohibition of automated individual decisions can be impediments to the development of technology. However, compliance with the standard and technology is fully possible, in view of this, this work presents case studies whose possibility of using blockchain technology in compliance with the GDPR is ratified.

Keywords: Token, Smart Contracts, Authenticity, Blockchain, GDPR.

1. Introduction

The General Data Protection Regulation (GDPR) [6] was drafted in April 2016 and entered into force in all Member States of the European Union (EU) in May 2018. This has become the main standard of personal data protection. Providing greater transparency in data processing and presenting more detailed information on how organizations should handle personal data. In addition, it grants the data subject greater control over their data and demands greater responsibility from organizations in the handling of this data.

Originally, blockchain was just the computer science term for defining a data structure whose data is arranged sequentially into blocks and the only operation allowed is to add a block to the end of the string [10]. However, today, the term blockchain is also used to represent a type of distributed recording system whose network elements (computers, often called nodes) have their own copy of the records. Each element of the network contains all operations processed in the system.

There are many different types of blockchains and blockchain applications, each with its specific capabilities and characteristics that suit different needs. Blockchain is a comprehensive technology that integrates with a wide variety of platforms and hardware around the world, so blockchain can be defined in various ways, depending on the approach presented in the scenario in question. If it's a business perspective, it can be defined in that context. If it's a technical perspective, you can also define it in that sense.

Two concepts are fundamental in using this new technology: smart contracts and tokens. Smart contracts can be considered an object in the object-oriented paradigm, as it holds state in a set of local variables and attributes. In addition, it has a set of functions that allow you to change this state and the ability to invoke functions in other contracts [17]. Tokens are cryptographic representations of blockchain assets; they can exercise and represent

functions and confer rights. Tokens can be considered blockchain-based unit of value for an organization or a project.

However, the entry into force of the GDPR in May 2018 raised many questions about the applicability of the law about blockchain technology [5] [8], for example, what level of data anonymization is sufficient for Are they not considered personal data? Or is encrypted data or the hash of some personal data considered personal data by the GDPR?

Furthermore, intrinsic blockchain properties such as immutability make it possible to question a possible incompatibility between the standard and the developing technology [15]. Thus, it is essential to identify the main elements of technology that may pose a challenge to the GDPR's requirements, in particular to the rights and freedoms of data subjects, and to present techniques applied in blockchain-based application implementations so that these applications may comply with data protection legislation. In this sense, it is necessary to analyze each point of conflict between a system in question and data protection legislation.

It cannot be generally stated that blockchain-based applications are compatible or incompatible with European data protection legislation [8]. Compliance with data protection legislation depends on a detailed case-by-case analysis, taking into account the implementation of the blockchain technology used and how the data controller proceeds about the subjects of processed data [8].

This work, in turn, discusses the conflicts of applications that use blockchain technology and data protection legislation, namely the General Data Protection Regulation. It analyzes two case studies to observe the points of conflict and their compliance with the law. In addition, it cites examples of non-compliance of these applications, that is, a form of blockchain application development in divergence with GDPR.

2. Methodology

The methodology used in the preparation of this article is based on a literary review of the main articles published so far and, mainly, a detailed analysis of the main elements of the General Data Protection Regulation that directly and indirectly impact the development of blockchain applications.

To evidence, the main conflicts between applications that use blockchain technology and data protection legislation, an analysis of two case studies are carried out to observe the points of conflict and their compliance with the legislation. In addition, it cites examples of non-compliance of these applications, that is, a form of blockchain application development in divergence with GDPR. Finally, a review of the works that were important for the research and served as a theoretical basis for the elaboration of this work is listed.

3. Background

Notwithstanding the importance of protecting personal data, it is necessary to relativize fundamental rights, that is, in each case, possible conflicts of the protected legal asset must be analyzed. Although individual rights and guarantees are universal and inalienable, they are not absolute. In certain scenarios, two or more equally protected legal assets effectively opposed, for example, an individual's right to information and the right to privacy.

In the cybernetic context, it is no different, there are many conflicts of rights in the daily life of the virtual world, with the publication of the General Data Protection Regulation (GDPR) in 2016 and its entry into force on May 25, 2018, many apparent and some authentic conflicts. The standard posed some challenges to the development of blockchain technology. About the processing of personal data, the law lists certain scenarios in which the processing can be carried out. Furthermore, it attributes obligations to data controllers, determines principles to be followed in data processing, and guarantees rights to data subjects.

3.1. GDPR

In addition to the GDPR, Article 8(1) of the Charter of Fundamental Rights of the European Union [7] and Article 16(1) of the Treaty on the Functioning of the European Union citeda2011tratado provides that everyone is entitled to the protection of personal data relating to him or her. This new standard contains in its full text 99 articles, which define the principles, establish the rights of individuals and define the obligations imposed on companies that are subject to regulation. Furthermore, data protection legislation prohibits any processing of personal data, unless the data controller has a legal basis, such as the documented consent of the data subject or if the processing is necessary to comply with legal contracts and obligations.

This means that any company that stores or processes personal information about EU citizens in EU states must comply with the GDPR, even if it does not have a commercial presence in the EU. Companies are subject to the GDPR if: the company is present in an EU country; even if there is no presence in the EU, the company still processes personal data of European residents, there are more than 250 employees, and even if there are fewer than 250 employees if data processing affects the rights and freedoms of data subjects.

3.2. Blockchain

Blockchain is a data structure whose data is sequentially organized into blocks and the only oper-

ation allowed is to add a block to the end of the sequence. Each block contains its own data and a hash of the data from the previous block, the data hash is the link between one block and another [10].

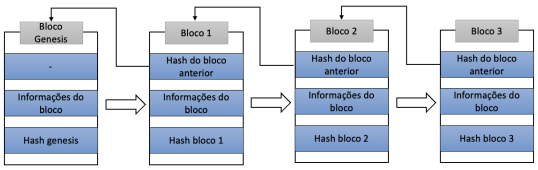

Figure 1: Blockchain

However, it is worth noting that the term blockchain is also used to represent a type of distributed recording system whose network elements (computers, often referred to as nodes) have their own copy of the records, each network element contains all the processed operations in the system. Every time a new operation is performed, all copies of the registry are updated. Blockchain technology provides a decentralized infrastructure with privacy, transparency, accountability, and authenticity to data entered into the network and, with the development of technology, it has incorporated more functionality as illustrated in Figure 3.2 [11].

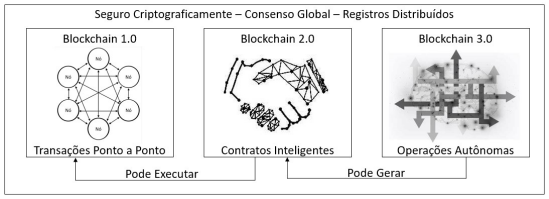

Figure 2: Blockchain Evolution

The incorporation of new features made it possible to carry out more complex activities, the different activities that the blockchain performs can be divided into three categories [1].

- Blockchain 1.0: A fully distributed ledger of transactions that are cryptographically protected and rely on global consensus.
- Blockchain 2.0: Includes smart contracts that are digitally written and signed waiting for certain conditions to be met to take effect, executing peer-to-peer transactions.
- Blockchain 3.0: A fully decentralized platform capable of autonomous operation based on distributed mathematical models.

A system capable of performing autonomous operations can determine optimal strategies to ensure global benefits and thus build better, more complex, and efficient smart contracts [11].

Furthermore, it is important to clarify that there are different blockchain implementations, each with its specific capabilities and characteristics that adapt to different needs. The blockchain can be public, private, or hybrid.

Blockchain technology is a way of storing and sharing data and has intrinsic characteristics that make it very suitable for many applications [20] [12]. The main feature of the blockchain is the immutability of [5] data, but it is not just this feature that makes this system attractive in the corporate market. In addition to the immutability of data, this technology has the characteristic of decentralization, that is, instead of large centralized providers, the blockchain is linked to a network that shares the data. Decentralization means that there is no single, more powerful entity that controls the [18] system, data is stored in a distributed, transparent and immutable way.

Although the public and private blockchain are the best-known types, there are still hybrid type blockchains. Each type with its own properties and characteristics that adapt to different needs.

In the public blockchain there is no entry limitation, participation in the network is open to anyone who wants to participate, that is, it has decentralized control and with equal participation among all members, it is certainly spread over a large geographic location and it is a feature of this model to ensure data confidentiality and integrity, but it cannot guarantee data privacy [14].

In the private blockchain, the control of the network is centralized, the possibility of accessing the network and information and processes is more restrictive. Organizations began to explore the potential of blockchain technology, but in order not to relinquish control, they established their own blockchain network [14].

The hybrid blockchain is a mixture of the previous types. These networks have characteristics present in both public and private blockchains. As an example, they mix partial privacy models and even use their own tokens, similar to cryptocurrencies. Thus, hybrid blockchains can leave some data open and transparent. However, these accesses would be restricted only to those who were allowed to operate them. Thus, an access authorization provided by the company or consortium that manages the [14] tool would be required.

There is also the consortium blockchain. A consortium blockchain is an implementation of a hybrid blockchain. These Blockchains are private Blockchains operated by a group or consortium and generally require permission. However, instead of a single body controlling it, multiple organizations can share governance. Administrators of a Consortium Blockchain can restrict users' read rights and allow a limit [4].

4. Blockchain and GDPR

Considering the points of conflict between blockchain implementations and the normative requirements of data legislation, these requirements can be organized into three distinct sets [15]: set A contains the items whose requirements are independent of the technology; set B the items whose requirements are supported by the blockchain; and a set C gathers the items whose requirements are not supported by the blockchain - see table 1.

Set A comprises the principles, rights, and obligations that do not depend on technology to be implemented, they are the principles of lawfulness, loyalty, and transparency, as well as the obligation of accountability of the data controller. This set of principles is related to how the person responsible for data processing acts about the data subject [15].

The principles of purpose limitation, data minimization, in addition to the right to information and access to personal data and the right not to be subject to automated decisions [15] still belong to set A. These principles are autonomous about technology and depend on a case-by-case detailed analysis of how each controller acts concerning the data subjects.

Set B is made up of the requirements that are supported by the blockchain. This group comprises the principle of integrity and the right of access [15]. The principle of integrity is by far what most supports the use of blockchain applications because this technology has immutability as one of its main characteristics. Changing the data inserted in the chain is very unlikely in the blockchain because it is directly related to the blockchain's ability to prevent the modification of data that has already been inserted.

Set C contains principles and rights that are not supported by the blockchain in its default configuration. This group contains the principles of accuracy, storage limitation, and confidentiality, in addition to the rights of rectification, portability, opposition, and the right to be forgotten [15]. This group has this characteristic primarily because the GDPR does not take immutable data structures into account.

The principles collectively constitute the core of the standard and are strict requirements for entities to be able to process personal data. In general, it is said that most blockchain implementations are configurable to become compliant with current data protection legislation. In principle, due to the immutability characteristic of the blockchain, requirements that are related to actions to delete, change, move the data inserted in the chain are not supported by the blockchain in its default implementation [15].

The rights already conquered by man must be guaranteed by the State, the GDPR has this purpose and, supported by the fundamental right to protection of personal data and the fundamental right to reserve the privacy of private and family life, established the protection of the person's personal data singular.

The controller has additional obligations that are specifically enforced throughout Chapter 4 of the GDPR that constitute the controller's organizational requirements. Article 5(2) of the GDPR obliges the controller to be responsible for ensuring compliance with material requirements, as well as for providing proof of compliance to authority.

Therefore, any application based on blockchain technology must comply with current legislation. It is essential to apply the principles, guarantee rights and fulfill the obligations required by law. There are fundamental principles of regulation that can be easily supported by blockchain applications and there are also principles that are independent of technology. However, blockchain technology has some intrinsic elements that appear to diverge from data protection legislation.

Deletion, alteration, processing limitation, and data portability activities, which are ensured by principles set out in the legislation, are not supported by technology by default. Although these actions are not supported by default by the technology, it is possible to use the technology in a way that meets all the requirements of the standard. Thus, to implement an application using the technology in question and compliance with the legislation, the development must observe the guidelines set out in this article.

However, it is not prudent to assess whether blockchain technology is compliant or not compliant with data protection legislation, but the implementation of the technology and how the data controller relates to the technology must be assessed in each specific case. the data subject.

Some blockchain properties, in their original configuration, are directly impacted by the GDPR. Smart contracts conflict with the prohibition of decisions made solely based on automated processing, including the definition of profiles, that produce effects in the legal sphere or that affect the data subject significantly in a similar way. NFT tokens are opposed by the principle of accuracy, the right to rectification, the right to be forgotten, and the right to portability.

About smart contracts, compliance with article 22 of the GDPR is essential. The data subject has the right not to be subject to any decision taken solely based on automated processing, including the definition of profiles, which has effects on its le-

Table 1: Princípios, Direitos e Obrigações no GDPR

	Requisito	Artigo GDPR	Conformidade
Princípios	Licitude	Art. 5, Sec. 1, let. a	Independe da tecnologia
	Lealdade	Art. 5, Sec. 1, let. a	Independe da tecnologia
	Transparência	Art. 5, Sec. 1, let. a	Independe da tecnologia
	Limitação das finalidades	Art. 5, Sec. 1, let. b	Independe da tecnologia
	Minimização dos dados	Art. 5, Sec. 1, let. c	Independe da tecnologia
	Exatidão	Art. 5, Sec. 1, let. d	Não Suporta por Padrão
	Limitação da conservação	Art. 5, Sec. 1, let. e	Não Suporta por Padrão
	Integridade	Art. 5, Sec. 1, let. f	Suportado
	Confidencialidade	Art. 5, Sec. 1, let. f	Não Suporta por Padrão
	Responsabilidade	Art. 5, Sec. 2	Independe da tecnologia
Direitos	Informação	Art. 13	Independe da tecnologia
	Acesso	Art. 15	Independe da tecnologia
	Retificação	Art. 16	Não Suporta por Padrão
	Apagamento dos dados	Art. 17	Não Suporta por Padrão
	Limitação do tratamento	Art. 18	Não Suporta por Padrão
	Portabilidade dos dados	Art. 20	Não Suporta por Padrão
	Oposição	Art. 21	Não Suporta por Padrão
	Decisões automatizadas	Art. 22	Não Suporta por Padrão
Obrigações	Registros de atividades	Art. 30	Independe da tecnologia
	Encarregado de proteção de dados	Art. 37	Independe da tecnologia
	Avaliação de impacto	Art. 35	Independe da tecnologia
	Proteção de dados por padrão	Art. 25	Independe da tecnologia
	Segurança do tratamento	Art. 32	Independe da tecnologia
	Dir dos Titulares dos Dados	Art. 24	Independe da tecnologia
	Notificação	Art. 33	Independe da tecnologia
	Comprovar conformidade	Art. 24	Independe da tecnologia
	Entidades fora da UE	Art. 27	Independe da tecnologia
	Códigos de conduta	Art. 40	Independe da tecnologia
	Certificações	Art. 42	Independe da tecnologia

gal sphere or that significantly affects it in a similar way [6].

The data subject shall have the right not to be subject to a decision, which may include a measure, which assesses personal aspects concerning him, which is based exclusively on automated processing and which produces legal effects that concern or affect him. significantly similarly, such as automatic denial of a credit application electronically or electronic recruitment practices without any human intervention.

This processing includes the definition of profiles through any form of automated processing of personal data to assess personal aspects relating to a natural person, in particular the analysis and prediction of aspects related to professional performance, economic situation, health, personal preferences or interests, reliability or behavior, location or displacement of the data subject, when it produces legal effects that concern it or significantly affect it similarly.

Concerning Tokens, it can be said that, technically, they are metadata files that are encoded using a digital file. These files contain information about the asset it is connected to, plus any additional information the NFT owner may wish to enter. For example, a specific NFT can have as metadata the following information: name, description, image, type, value. Therefore, personal information inserted in the metadata of the NFTs tokens is under the protection of the GDPR and, therefore, these tokens must comply with the principles, rights, and obligations that are in the regulation.

There are a few techniques that can be used in implementing a blockchain application and making it GDPR-compliant. The principles of data protection should not apply to information to information that does not concern an identified or identifiable natural person or to personal data made so anonymous that its holder is not or can no longer be identified [6]. Anonymization, Hash and Data Encryption

There are several ways to apply the data anonymization process to a given set of personal data, the article 29 working group has developed examples to elucidate this process [19]. In addition to this important study, there is considerable effort to demonstrate anonymization techniques such as attribute suppression, record suppression, data masking, generalization, [13], data perturbation, and synthetic data.

Hash functions take a message as input and produce an output known as a hashcode, hash result, hash value, or simply hash. More precisely,

a hash function h maps finite-length bit strings to n-bit fixed-length strings [16]. For a domain D and a given range R with h: D $\rightarrow$ R and |D| $>$ |R|, the function is many to one, implying that there are collisions, ie. , pairs of inputs with identical output, it is inevitable. Restricting ha to a domain of t-bit inputs (t $>$ n), if h were random in the sense that all outputs were essentially equally possible, then about 2^{tn} entries would map to each output, and two randomly chosen inputs would produce the same output with probability 2^{-n} (independent of t) [16].

In a strict sense, a hash function is an h function that has at least the following two properties:

- compression – a function h that maps an input x of arbitrary length of finite bit, to an output h(x) of fixed bit length n.
- easy to calculate - given a function h and an input x, h(x) is easy to calculate.

The hash function can also be used on digital files. In these cases, the result obtained with this process is a reference to the file, consequently, a reference to the information contained in this file. The hash takes care of the integrity element, it does not guarantee confidentiality or availability.

By applying the hash function in the document below, the following output is obtained as an answer: 0B4205AA296E4DD84DA5D0EE299C9546440DF0EAAE83ADB5D7BE63234A976E93.


CERTIFICADO

O Instituto Legislativo Brasileiro certifica que
JODELISMARKO MAMORÉ DE MELO, CPF nº 00539211192
realizou, na modalidade a distância, o curso sem tutoria
ÉTICA E ADMINISTRAÇÃO PÚBLICA - TURMA 03
no período de 16 abril 2014 a 6 maio 2014
com carga horária de 40 horas/aula
tendo obtido aprovação com nota: 100,00

Brasília, 6 maio 2014

Simone Dourado
Coordenação de Ensino a Distância - COEDI

Elga Lopes
Diretora Executiva do ILB

Antônio Helder Medeiros Rebouças
Diretor-Geral do Senado Federal

Figure 3: Primeiro arquivo exemplo

The hash of each of the files is uniquely and exclusively from that particular file. In the presented scenario, a brute force attack is not possible, the possibilities of combinations are infinite, any change, no matter how tiny it is, will result in a different hash. Therefore, to obtain the same result, the hash function must be applied to the same file.

Similarly, encryption is not only a technique used for pseudonymization of personal data, but data encryption is also a tool that can be used to achieve GDPR blockchain application compatibility.

Considering encrypted personal data or hash of a dataset, it can be said that this set of bits resembles a folder and inside this folder has the information, to access the data it is necessary to open it or, in this case, decrypt. The result of encrypting a dataset is information unintelligible to the human eye, the information is wrapped in a set of characters that can only be understood by a machine. Therefore, this character set should not be considered personal data.

It is worth noting that the condition of having or not having the key to reverse the encryption was not mentioned. It is important to make clear that encrypted data by itself does not have the necessary properties to be classified as personal data. The GDPR itself, by emphasizing the independence of technology, states that files or sets of files as well as their covers, which are not structured according to specific criteria, should not fall within the scope of this regulation.

Therefore, digital data that are not structured or that it is not possible to re-identify from them should not fall within the scope of the regulation. The encrypted data block is incomprehensible, that is, it is not structured according to criteria comprehensible to human beings. Therefore, it should not be covered by the data protection regulation.

Another point of the GDPR that corroborates with this is the affirmation of article 34 by stating that, as a rule, it is essential to communicate the violation of their data to the holder of personal data. However, subparagraph ”a” of item 3 of the same article states that communication to the data subject is not required if the data controller has applied adequate protection measures, both technical and organizational, and these measures have been applied to the data personal data affected by the breach of personal data, especially measures that make personal data incomprehensible to any unauthorized person to access that data, such as encryption.

In addition, another exception to the processing of personal data is in the letter ”e” of item 4 in article 34 which states: the processing of personal data with a purpose other than the purpose for which the data was initially collected and without the consent of the holder may be carried out if adequate safeguards such as encryption and pseudonymization exist.

Thus, both encryption and the hash function are essential in the process of data pseudonymization. further they are not always effective for the purpose of ensuring data privacy. In addition, it should be made clear in which scenario the encrypted data

and the hash are still personal data and, on the other hand, in which scenario the encrypted data and the hash are not considered personal data.

5. Results & discussion

With the analysis of requirements, the result is applied in two case studies of applications developed using blockchain technology: the work “Everydays: The first 5000 days” and the QualiChain project. The purpose is to demonstrate that an application may or may not comply with data protection legislation, depending on how this application was developed.

Currently, the greatest exponent of an NFT is the work “Everydays: The first 5000 days”. This work is digital art and, according to auction house Christie’s, is a “monumental collage”, it was the first purely digital work of art ever offered at auction. The metadata of the work “Everydays: The first 5000 days” can be accessed at this link: https://ipfs.io/ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz.

A blockchain containing the data in this work complies with the principles of lawfulness, loyalty, and transparency, as these principles do not depend on the technology involved in developing the application.

In this same sense, the purpose limitation principle must be analyzed with caution. At the time of data collection, the purpose of the data collected must be very well defined and established and a document with the consent of the data subject. If so, the application will comply with this principle as well.

Similar to the previous principle, the data minimization principle is customizable in a blockchain application. therefore, the data controller must, before data collection, establish what information is necessary for data processing.

However, the principle of accuracy cannot be supported by a blockchain application that contains this data. A blockchain in its default configuration does not allow data to be changed. Therefore, if, for any reason, the data subject requests the data to be changed, this task cannot be performed.

The principle of limiting conservation cannot be practiced in the scenario presented either. For example, if the owner of the data submitted requires that the data be kept only, and only, for a period of 10 years. It is not possible to limit the processing of this data for a certain time.

In a blockchain scenario, the principle of integrity is the principle that the technology comes closest to. Blockchain characteristics favor compliance with the integrity principle, data integrity is one of the pillars of the technology. Therefore, this application respects this principle.

In the opposite scenario, the principle of confidentiality is not fulfilled by the application. Indeed, this principle does not preclude the development of technology, as a blockchain can be private and guarantee confidentiality. However, in a public blockchain, this principle cannot be obeyed.

The principle of responsibility can be fulfilled by a blockchain in the scenario presented. This principle does not depend on the technology used in the processing of personal data. The principle refers to the responsibilities of the controller and the processors about the processing of personal data.

The QualiChain project aims to develop, target, and evaluate decentralized blockchain-based solutions for storing, sharing, and verifying educational certificates [17]. The solution is implemented through five main components: the smart consortium contract, the smart contract for HEIs, the client for HEIs, the recruiting application, and the consortium application.

To verify compliance with data protection legislation, it is necessary to understand exactly what and how data is stored on the blockchain. Initially, several use cases of the QualiChain project considered storing the certificate itself in the chain to guarantee its authenticity and integrity. However, there are costs associated with storing this data. The existence of such costs suggests not storing the certificates themselves in the blockchain, but only authentication or integrity data, such as a cryptographic hash of each [3] certificate. Thus, storing a cryptographic hash obtained with the SHA-256 algorithm that is only 32 bytes long is more expensive than storing a certificate that can be a file of 1 MB or more.

In addition to the cost associated with storage, compliance with data protection legislation is a challenge as data stored directly on a blockchain is immutable and cannot be deleted. Therefore, if there is personal data, it hinders the ability to implement the right to be forgotten [3].

In the QualiChain project, the smart contract contains a mapping of the certificates, which associates a unique identifier of the data subject with the cryptographic hash of their certificate. Thus, the certificate itself is not stored in the blockchain, only its hash, which must meet two important properties:

- unidirectional - cannot get input from the output (the hash);
- strong collision resistance - it is computationally infeasible to find two different entries with the same hash.

For an institution to register a certificate on the network, it must, in addition to creating its account

on the Ethereum network and joining the consortium, implement its smart contract. This smart contract can have different versions, but it must provide three essential operations:

- registerCertificate(id, hash): registers a certificate in the blockchain storing the cryptographic hash and received metadata as arguments.
- revokeCertificate(id): revokes a certificate identifying it through the cryptographic hash and the metadata received as arguments.
- verifyCertificate(id): verifies if a certain certificate is registered in the contract, and returns its result to the function caller.

As can be seen in the signature of the function that registers a certificate in the blockchain, this function takes two parameters: the id, a unique identifier of the data subject, and the certificate hash. It is worth stressing that the certificate is not stored in the blockchain, but the certificate hash, that is, what is stored in the blockchain is metadata. Considering the QualiChain project context, the principles, rights, and obligations must be analyzed to validate compliance with current legislation.

The first principles listed by the GDPR are: the principle of lawfulness, the principle of loyalty, and the principle of transparency, the QualiChain project meets these requirements. According to the GDPR, lawfulness is achieved, for example, by obtaining the consent of the data subjects for one or more purposes. For this purpose, the project has made efforts to develop an informed consent form, in addition to obtaining the consent of the data subject, informing platform users about their rights concerning their data. This term informs users of the following:

- Collected data
- Use of user data by third parties
- Users' rights to their data
- Explanation of why QualiChain processes user data
- Cookie Details
- DPO contact details

The principles of loyalty and transparency are supported by the blockchain application developed within the QualiChain project, as these principles do not depend on the technology involved in the development of the application, but on how the data controller proceeds to collect the data. Those responsible for data processing, in this case, are educational institutions that intend to insert certificates in the blockchain, must obtain from the data subject the consent form signed at the time of data collection.

In addition, data controllers process personal information only for the purpose for which it was collected. The data controller must, when collecting the data, inform the data subject of the exact purpose of the collection of this information. The QualiChain project also complies with this principle.

Another important principle is the data minimization principle, only the necessary user data will populate the system. To comply with this principle, the information entered in the blockchain is only the data necessary for the validation of the certificate.

In the context of the QualiChain project, only personal data that are necessary and compatible with the project's research objectives will be collected and processed. Personal data collected from survey participants refer to the individual's educational qualifications and titles. Gathering this information is necessary to fulfill the project's objectives, as QualiChain's goal is to provide a disruptive way of archiving, managing, sharing, and verifying educational qualifications and titles [2].

The principle of accuracy poses a greater challenge to the project, as data entered into a blockchain cannot be edited. However, in this design, a certificate is subject to revocation. Thus, cases in which certificates containing data that do not correspond to reality can be revoked. Therefore, QualiChain design complies with the principle of accuracy.

The controller can store the certificate in an on-premises environment, in the cloud, or on a peer-to-peer network. Whatever the solution developed by the educational institution, the conservation limitation principles can be met. remembering that only metadata is inserted into the blockchain, therefore this data does not need to be removed. At the cost of compromising the verifiability of the certificate, the controller may, at any time, delete the certificate. This will not prevent the use of the blockchain. Therefore, the project under review complies with the principle of conservation limitation.

As noted in the previous case study, the integrity principle is the principle most consistent with blockchain technology. The characteristics of this technology favor compliance with the principle of integrity, data integrity is one of its main pillars. Therefore, the application developed in this project meets the requirement of this principle.

The principle of confidentiality is also fulfilled by the project application. It is true that in a

public blockchain this principle cannot be fulfilled. However, again, what is inserted into the public blockchain is metadata, the personal data themselves, ie the certificates, are stored privately by educational institutions. Thus, complying with the requirement of confidentiality of personal data is required by the GDPR.

The principle of accountability for the processing of personal data can be fulfilled by the project's blockchain application. This principle does not depend on the technology used in the processing of personal data. The principle refers to the responsibilities of the data controller, which in this case refers to educational institutions, to the processing of personal data collected by them.

In the context of the QualiChain project, the processing of personal data is not subject to automated decisions. There are no automated decision implementations that assess personal aspects, in particular the analysis of professional performance, economic situation, health, personal preferences or interests, reliability or behavior, location, or displacements in the project's smart contract. Such automatic decisions are prohibited by the GDPR.

Within the scope of obligations, to identify and address any security issues, the Qualichain project prepared the data protection impact report. The consensus arising from the legal and ethical review is that QualiChain is a low-risk project about security and personal data issues [9].

The GDPR requires the appointment of a data protection officer. Dr. Spiros Mouzakitis has been named Data Protection Officer (DPO) for QualiChain [2].

Therefore, the QualiChain project complies with this requirement of data protection legislation. In addition to the obligations that have been listed so far, there are the following obligations that are also met by the QualiChain project: the registration of activities, data protection by default, the security of data processing, the duty of notification, the duty to prove the compliance of the application with data protection legislation, the drafting of the code of conduct, certifications and the obligation imposed on the data controller to guarantee the rights of the data subjects. All legal and security aspects of the technical solution that were defined before the start of platform development have been followed by the technical team.

Although QualiChain is considered a low-risk project as no sensitive data will be stored and processed, all possible measures have been taken to ensure legal compliance. The analysis of national legislation in addition to the GDPR resulted in the project's declaration of conformity, which was a unanimous decision validated by the DPO and other legal entities [9].

6. Conclusions

In the scenarios presented for the use of hashing and encryption, it is necessary to determine the possibility of re-identifying the data subject. If so, these data will still be under the protection of the regulation. If the data is not subject to reverse engineering due to computational cost or time, the data does not enjoy the status of personal data and therefore is not under the protection of the General Data Protection Regulation.

In addition, the compatibility with the legislation must be analyzed in each specific case because it cannot be said that the blockchain technology is compatible or not compatible with the GDPR, but rather the compatibility of given blockchain implementation and how the data controller relates to the data subject.

Therefore, legislation must evolve to ensure that fundamental rights are ensured regardless of the emergence of new technologies. The technology must use new features and different forms of implementation to make both of them compatible. The key point to be taken into account is the possibility of compatibility.

With the development of blockchain technology, in addition to the insertion of new features, many implementation patterns were established. Some emerged to remedy previous failures and others to fulfil different roles that were not previously supported. This technology can help solve several of the challenges required in the contemporary world, even if they are in different areas.

The main purpose of technology is to solve problems that have not been solved with existing technologies to date. Difficulties that once seemed insurmountable can now be overcome. There are many areas of usefulness for blockchain technology: education, health, financial system, culture, entertainment, among others.

The QualiChain project is an example of the application of technology. This project proposes to develop a system to verify diplomas and certificates issued by educational institutions. It uses algorithmic techniques and computational intelligence to disrupt the domain of public education, as well as its interfaces with private education, the labor market, public sector administrative procedures, and broader socio-economic developments.

Everydays: The first 5000 days is a digital work of art and, according to Christie's auction house, is a ”monumental collage”, having been the first purely digital work of art, which makes use of NFT, ever offered in an auction. It is an image in JPG format of 21069 x 21069 pixels (319,168,313 bytes), composed of another 5000 images created one by

one daily, for over 13 years by digital artist Mike Winkelmann, better known simply as Beeple and that has over 2 million followers on Instagram.

The two scenarios presented use different implementations of blockchain technology and comply with the requirements of the General Data Protection Regulation about the processing of personal data. It is important to note that a detailed analysis of each smart contract and token standard implemented is essential to determine its compliance with data protection legislation.

References

[1] M. A. Bovério and V. A. F. da Silva. Blockchain: uma tecnologia além da criptomoeda virtual. *Revista Interface Tecnológica*, 15(1):109–121, 2018.

[2] N. Chowdhury, A. Third, V. K. Ahmad Mehrbod and, C. Kontzinos, C. Botsikas, S. Scerri, I. Keck, N. Politou, and M. Correia. D8.3 qualichain data management plan. *QualiChain Project Deliverable*, 2019.

[3] N. Chowdhury, A. Third, V. K. Ahmad Mehrbod and, C. Kontzinos, C. Botsikas, S. Scerri, I. Keck, N. Politou, and M. Correia. D5.1 qualichain integrated architecture. *QualiChain Project Deliverable*, 2021.

[4] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida. Consortium blockchains: Overview, applications and challenges. *International Journal On Advances in Telecommunications*, 11(1&2):51–64, 2018.

[5] D. Duarte. An introduction to blockchain technology from a legal perspective and its tensions with the GDPR. *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law-CIJIC*, 2019.

[6] European Parliament and European Council. 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 (General Data Protection Regulation), April 2016.

[7] U. Europeia. Carta dos direitos fundamentais da união europeia. *Direito e Democracia*, page 457, 2007.

[8] M. Finck and P. Europeo. *Blockchain and the general data protection regulation - Can distributed ledgers be squared with European data protection law?* Oficina de Publicaciones, Luxemburgo, 2019.

[9] C. Kontzinos, P. Kokkinakos, P. Kapsalis, O. Markaki, V. Karakolis, and J. Psarras. Leveraging blockchain, analytics and decision support to facilitate qualifications' verification, recruitment and competency management: The qualichain project and initial results. *International Journal on Advances in Intelligent Systems Volume 13, Number 3 & 4, 2020*, 2020.

[10] K.-C. Li, X. Chen, H. Jiang, and E. Bertino. *Essentials of Blockchain Technology*. CRC Press, 2019.

[11] M. Lotfi, C. Monteiro, M. Shafie-Khah, and J. P. Catalão. Transition toward blockchain-based electricity trading markets. In *Blockchain-based Smart Grids*, pages 43–59. Elsevier, 2020.

[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, 2019.

[13] P. D. P. C. of Singapore. Guide to basic data anonymisation techniques, 2018.

[14] M. Pilkington. Blockchain technology: principles and applications. In *Research Handbook on Digital Transformations*. Edward Elgar Publishing, 2016.

[15] S. Ramsay. The general data protectionregulation vs. the blockchain: A legal study on the compatibility between blockchain technology and the GDPR, 2018.

[16] B. Schneier. *Protocol Building Blocks*. Wiley Online Library, 2015.

[17] D. Serranito, A. Vasconcelos, S. Guerreiro, and M. Correia. Blockchain ecosystem for verifiable qualifications. In *2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 192–199, 2020.

[18] A. Sunyaev. Distributed ledger technology. In *Internet Computing*, pages 265–299. Springer, 2020.

[19] WP29. Opinion 05/2014 on anonymisation techniques. Technical report, Comissão Europeia, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, 2014. (accessed: 10.06.2021).

[20] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(3):2794–2830, 2019.