Privacy and Data Protection Concerns Regarding the Use of Blockchains in Smart Cities

Luis Felipe M. Ramos
University of Minho
Rua da Universidade, 4710-057
Braga, Portugal
lfelipe.sm@gmail.com

João Marco C. Silva
United Nations University (UNU-EGOV), INESC TEC &
University of Minho
Rua de Vila Flor 166, 4810-445,
Guimarães, Portugal
joaomarco@di.uminho.pt

ABSTRACT

In this work we investigate which aspects of data protection regulation must be carefully observed when implementing Blockchain-based projects in smart cities. This technology provides interesting properties and allows governments to develop flexible and innovative data management systems. Nevertheless, realizing the benefits of using Blockchains requires understanding the government processes along with the legal framework and political setting imposed on government. Though it is a buzzword, Blockchain may not always be the best solution for data processing, and carrying out a Data Protection Impact Assessment could allow an analysis of the necessity and proportionality of the mechanism. Furthermore, principles relating to security of data remain applicable to Blockchains. We discuss points of interaction between Blockchain technology and the European Union data protection framework, and provide recommendations on how to better develop Blockchain-based projects in smart cities. The findings of the study should provide public sector actors with a guideline to assess the real necessity and better format of a Blockchain-based application.

CCS CONCEPTS

• Security and privacy → Privacy protections; • Social and professional topics → Privacy policies; • Applied computing → E-government;

KEYWORDS

Privacy, Personal Data, GDPR, Blockchain, E-Gov, Smart Cities

ACM Reference format:

<do not remove / editorial placeholder for author names>. 2019. <do not remove / editorial placeholder for paper title>. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV'19), Melbourne, Australia, February 20-22, 2019*, <00> pages. https://doi.org/00.0000/0000000.0000000

1. INTRODUCTION

In order to achieve the Sustainable Development Goals (SDG), adopted by the United Nations members in 2015, many cities have looked for the benefits of adoption of Information and Communication Technologies (ICT) to improve their operational and organizational capabilities. The movement towards the digitization of cities infrastructure through sensing technology (e.g., Internet of Things) and the use of that vastly increased flow of information to furnish adaptive urban planning, amenities and services, has provided us with smarter cities [10].

Among these ICTs used in smart cities, one of them has standed out - the Distributed Ledger Technology (DLT). The DLTs represent a unique technology in two ways: (i) it is distributed in nature, i.e., the network of users must agree about the state of the ledger by a consensus mechanism, rather than relying on a third-party intermediary; and (ii) users can add new transactions with digital assets (e.g. records, acts, and states) on the ledger, the record of which is rendered immutable, transparent, and auditable yet resistant to censorship and manipulation due to the technology's cryptographic and distributed foundations [6].

The most famous application of DLTs is the Blockchain, which was introduced by Satoshi Nakamoto with its cryptocurrency, Bitcoin [8]. Altough the term Blockchain does not refer to just one technology, it is used to group a set of different computational technologies, in order to provide a digital ledger with important characteristics, as immutability, transparency, and trustworthiness [9].

For that reason, governments around the world are looking to develop public services based on Blockchain, with more than 30 countries already investing in projects related to this technology [12]. Some examples can be found in central banks [2], the modernization of land registration and administration [4], the increase of voter confidence in elections [7], and even to provide new systems for digital identity management [11]. For all that to function as planned, the use of personal data from the citizens is

ICEGOV '19, February 20-22, 2019, Melbourne, Australia

ACM ISBN 000-0-0000-0000-0/00/00...$15.00
https://doi.org/00.0000/0000000.0000000

of vital importance. However, in today's world it has become increasingly important to comply with the legislation protecting the treatment of personal data.

In that sense, many countries are currently drafting and enforcing new legislation on that matters. This new legislation intend to protect the processing of personal data, especially the cross-border flow of personal information, and between public and private actors, including natural persons, associations and undertakings (EU GDPR, Regard 5). Examples of recent regulations on the subject can be found in the European Union (EU)[2], Brazil[3], Morocco[4], and Singapore[5].

This new legal and technological framework demands an increase attention from the actors responsible for the implementation of Blockchain-based projects in governments. They will be in charge of assuring the correct design of technical aspects, in order to meet the requirements imposed by the legislation and avoid the serious sanctions and fines provided for therein.

Blockchain is a technology with a high potential for development that raises many uncertainties, including questions on its compatibility with the recently enforced EU GDPR and other data protection rules. In that sense, we intend to investigate in this work which aspects of data protection regulation must be carefully observed when implementing Blockchain-based projects in smart cities.

The remainder of this article is organized as follows: in Section 2 we discuss some considerations presented in the EU GDPR; in Section 3 we describe the Distributed Ledger Technologies enphasizing the Blockchain; Section 4 presents some possible interactions between blockchains and the EU GDPR; conclusion remarks and early recommendations are summarized in Section 5.

2. DATA PROTECTION FRAMEWORK

After many years of massive use of the Internet to communicating, shopping, promoting products and bring people and business together, there is a sense of insecurity resulting of these virtual relations, becoming essencial to give back to individuals the control of how their personal data are used, strengthening the legal certainty and practical security to individuals, economic agents and public authorities [5].

Aiming at this goal, the European Union enhanced its legal framework by publishing in 2016 the General Data Protection Regulation (GDPR), which is a key milestone in the control of the treatment of personal data, with the purpose of facing the new challenges imposed by the evolution of new technologies and market globalization.

The EU GDPR introduced a set of new rules among which is the obligation to designate a Data Protection Officer (DPO), rules on pseudonimization, changed the rules on obtaining consent, eliminated the notifications and authorizations system, implemented the "right do be forgotten", and introduced very high fines for data breaches.

For all that reasons, the EU GDPR has been used as a benchmark by other countries in the drafting of they own new data protection legislation. And because of that, in our work we will focus on its guidelines that might be applied in developing and implementing Blockchain-based projects.

2.1. Scope of the EU GDPR

In order to correctly implement Blockchain-based projects that comply with the EU GDPR, it is important to notice who is subjected to the regulation, and what activities might suffer its effects.

The EU GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (EU GDPR, Article 4.1).

The processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (EU GDPR, Article 4.2).

So whenever a Blockchain contains personal data, the GDPR is applicable. The architecture and characteristics specific to Blockchains will, however, have consequences on how personal data is stored and processed. The impact of Blockchains on individual rights (namely, the right to privacy and the right to personal data protection) therefore calls for a specific analysis.

2.2. Principles of Data Protection

According the EU GDPR, the principles of data protection should apply to any information concerning an identified or identifiable natural person (Regard 26). These principles set out obligations for businesses and organizations that collect, process, store or perform other operation on individuals' personal data.

The GDPR, in its Article 5, outlines six data protection principles an entity must mandatorily comply with when processing personal data. These principles relate to:

- **Lawfulness, fairness and transparency** - an entity must process personal data lawfully, fairly and in a transparent manner in relation to the data subject;
- **Purpose limitation** - one must only collect personal data for a specific, explicit and legitimate purpose. One must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose;
- **Data minimisation** - one must ensure that personal data processed is adequate, relevant and limited to what is necessary in relation to the processing purpose;

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.
[3] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
[4] https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf.
[5] https://sso.agc.gov.sg/Act/PDPA2012.

- **Accuracy** - one must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request the erase or rectification of erroneous data that relates to them, and one must do so within a month;
- **Storage limitation** - one must delete personal data when it is no longer necessary. The timescales in most cases aren't set. They will depend on the business' circumstances and the reasons why the data is collected;
- **Integrity and confidentiality** - one must keep personal data safe and protected against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

3. DISTRIBUTED LEDGER TECHNOLOGIES AND BLOCKCHAINS

A distributed ledger is essentially an asset database that can be shared across a peer-to-peer (P2P) network of multiple sites, geographies or institutions, and where all participants of the network keep an identical copy of the ledger, in such a way that any modification is reflected to all copies in a very short time [13].

Although the term "Blockchain" is often associated with another term that refers to a larger family of technologies (DLTs) – which include but are not limited to Blockchains - for the purpose of this work we will focus our analysis on Blockchain technology alone given that DLT solutions that are not Blockchains are still too recent and too rare for a proper generic analysis.

3.1. Characteristics of Blockchains

Blockchain applications enable transactions to be aggregated in 'blocks', which are then added to a 'chain' of existing blocks using a cryptographic signature. The security and accuracy of the assets stored in the ledger are maintained through the use of mathematical properties based on public key cryptography and signatures to control who can do what within the shared ledger [13].

Generally Blockchains are defined by the following properties:

- **Transparency** - all transactions recorded in the ledger are visible to all participants of the network, providing public verifiability;
- **Decentralisation** - several copies of the Blockchain coexist on different computers;
- **Immutability** - the ledger allows only the inclusion of data, and once it is recorded, it becomes technically infeasible to be altered or removed; and
- **Disintermediation** - all decisions are made by consensus among the participants, without a central trusted third party or middle man.

These properties result from the combination of technologies such as distributed ledgers, public key encryption, cryptographic hash functions, and consensus protocols, that allows the design of different types of Blockchains for different purposes.

3.2. Classification of Blockchains

It is possible to classify Blockchain implementations into three categories [6, 12]: *(i)* public; *(ii)* permissioned; and *(iii)* private. They vary from each other by the different permission levels that different categories of participants are assigned to:

(i) Public Blockchains are accessible to all participants, anywhere in the world. Anyone can join or leave the network at any time, record a transaction, take part in the validation of the blocks or obtain a copy of them, without any previous control;

(ii) Permissioned Blockchains have rules that set out who can take part in the validation process or even register transactions. They can, depending on the case, be accessible to all or be restricted;

(iii) Private Blockchains are controlled by a unique actor who alone oversees participation and validation.

Due to the Bitcoin and similar cryptocurrencies, the first classification is the most-known, as these digital currencies tend to operate in public Blockchains, where any participant in the network can see all transactions already made and update the ledger with new ones. This is also the riskiest type of Blockchain, according to [1]. Permissioned Blockchains allow any user to see the history of transactions, but only selected members can update it. Because it contains more restrictive rules about who can participate, observe and validate transactions, this model is emerging in industry sectors, being used for the exchange of tangible and intangible assets between enterprises. Finally, according to some experts [1], the parameters of the private Blockchains do not respect the traditional properties of Blockchains, such as decentralisation and shared validation. In any case, private Blockchains do not raise specific issues regarding their compliance with the EU GDPR. They can be considered traditional distributed databases.

4. INTERACTIONS BETWEEN BLOCKCHAINS AND THE EU GDPR

Innovation and the protection of individuals' fundamental rights are not two conflicting goals. In fact, the EU GDPR does not aim at regulating technologies *per se*, but regulates how actors use these technologies in a context involving personal data.

For this reason, stakeholders who wish to use Blockchains when carrying out personal data processing in smart cities context should pay attention to some crucial points and best-practice recommendations. Although it isn't possible to require the organizations to ensure that there will be no data breaches or undue data processing, they should be guided by the principle of accountability, whereby they must be able to prove they comply with the regulation (EU GDPR, Article 5.2).

The EU GDPR, and more broadly classical data protection principles, were designed in a world in which data management is centralised within specific entities. In this respect, the decentralised data governance model used by Blockchain technology and the multitude of actors involved in the processing of data lead to a more complex definition of their role.

Considering that, in a specific Blockchain context it is possible to identify three actors:

- **Accessors** - users who have the right to read and hold a copy of the ledger in the Blockchain;
- **Participants** - users who have the right to make entries and update the ledger (i.e., make a transaction for which they request validation);
- **Miners** - users who validate a transaction and create blocks by applying Blockchain rules of consensus for acceptance by the community.

According to the EU GDPR, a controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In that sense, we align with [1], that consider "Participants", who have the right to write on the Blockchain and who decide to send data for validation by the miners, to be considered as data controllers, as they define the purposes (objectives pursued by the processing) and the means (data format, use of Blockchain technology, etc.) of the processing. More specifically, a "Participant" shall be considered a data controller when he/she is a natural person and that the personal data processing operation is related to a professional or commercial activity, or when the participant is a legal person and that it registers personal data in a Blockchain.

As the "Miners" are only validating transactions submitted by participants and are not involved in the object of these transactions, they can not be considered as data controllers. Similar idea applies to the "Accessors", who do not process any personal information.

If a group of "Participants" decide to carry out processing operations with a common purpose, Article 26 of the EU GDPR demands them to determine, in a transparent manner, each one responsibilities to ensure compliance with the obligations under the regulation. Otherwise they could be considered joint controllers. Data subjects (i.e. those whose personal data is recorded on the Blockchain) must know which entity they can refer to in order to effectively exercise their rights, and data protection authorities must have a contact point who can be held accountable for the processing carried out.

In the case of using Smart Contracts in a Blockchain, its developers who process personal data on behalf of the data controller will be considered data processors, according to Article 28 of the EU GDPR. The same applies for "Miners" when they follow the data controllers' instructions for checking whether the transaction meets technical criteria (such as a format and a certain maximum size, and that the participant is allowed, according to the Blockchain rules, to carry out its transaction). In both cases, they should establish a contract with the data controller, which specifies each party's obligations and which reproduces the provisions of Article 28 of the EU GDPR.

4.1. Recommendations for the Use of Blockchains in Smart Cities

In order to minimize the risks for data subjects when a processing is carried out on a Blockchain, two precautions are vital to take into consideration:

1) Carefully evaluate beforehand the need to use a Blockchain, particularly a public one - not all data processing will be better performed on a Blockchain, as it can be a source of difficulties for data controllers in terms of compliance with the obligations set out by data protection regulations. Article 25 of the EU GDPR determines that data controllers shall implement appropriate technical and organisational measures for ensuring that, by design and by default, the best technology and practices are applied, in order to meet the requirements of the regulation and protect the rights of data subjects.

When using a permissioned Blockchain it is possible to implement appropriate safeguards to secure cross-border flow of personal information, such as standard contractual clauses, binding corporate rules, codes of conduct or even certification mechanisms. However, in a public Blockchain it becomes harder to implement these safeguards, as the data controller has no real control over the location of "Miners" or the copies of the ledger.

In general, using an open or permissioned Blockchain only makes sense when multiple mutually mistrusting entities want to interact and change the state of a system, and are not willing to agree on an online trusted third party. [14] presents a flowchart to help the decision making process of adopting a Blockchain-based solution.

2) Choose carefully the format under which the data will be registered - the data minimisation principle defined in Article 5(1)c of the EU GDPR requires that the data collected be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Also, a data retention period must be defined according to the purpose of the data processing, in order to avoid storing personal data for an unlimited time.

However, due to its characteristics, data registered on a public Blockchain cannot be technically altered or deleted: once a block in which a transaction is recorded has been accepted by the majority of the participants, that transaction can no longer be altered in practice. This may present serious obstacles for the data subjects who wish to exercise their right to be forgotten.

There is two categories of personal data that can be registered on a Blockchain:

- **Identifiers**: it consists of a string of alphanumeric characters used to identify each entity, constituting its public key. This public key is mathematically linked to a private key, known only by the entity, which is used for its authentication in the network. The very architecture of Blockchains means that these identifiers are always visible, as they are essential for its proper functioning.
- **Additional data**: any other data contained within a transaction that is stored on the Blockchain can contain personal data (e.g.: diploma, property deed), which can potentially relate to individuals other than "Participants" and "Miners" and that may be directly or indirectly identified. Article 25(1) of the EU GDPR

requires the data controller to choose the format with the least impact on individuals' rights and freedoms.

Towards the latter issue, it is suggested to store the additional data in the form of a commitment scheme[6] on the Blockchain. If that solution is not possible, then the personal data should be register in the form of a hash generated using a hash function with a key, or, at least, in the form of an encryption (ciphertext) ensuring a high level of confidentiality.

The common feature underlying some of these solutions is to store any additional data in cleartext outside of the Blockchain (such as, for example, on the data controller's information system) and to store on the Blockchain only a proof of existence of the data (e.g. commitment, hash value generated with a cryptographic hash function, etc.).

5. CONCLUSIONS

The growing interest in using Blockchain-based applications by governments, in order to offer more efficient public services and increasing trust in public sectors should be cheered, as this technology provides interesting properties and allows flexibility to develop innovative data management systems. Nevertheless, realizing the benefits of using Blockchains requires understanding the government processes along with the legal framework and political setting imposed on government.

Determining whether to implement a Blockchain-based application is about risk management and conducting a Data Protection Impact Assessment (DPIA). Blockchain may not always be the best solution for data processing, and carrying out a DPIA could allow an analysis of the necessity and proportionality of the mechanism and, where necessary, enable the identification of cases in which other solutions may be more suitable. For that reason, public organizations should carefully determine whether they need Blockchain in the first place, particularly a public one. If Blockchain properties are not required in order to meet the purpose of the processing, it is recommended favouring other solutions that allow for full compliance with the data protection legal framework.

In addition to questioning the use of a Blockchain, the data controller must also question which type of Blockchain should be used. If the choice is to go forward, permissioned Blockchains should be favoured as they allow a better control over personal data governance, in particular as regards cross-border transfer of personal data.

Also, it is important to practice data minimization when registering data on a Blockchain; Notably, organizations think they may need the tech when they really don't, meaning that a careful assessment of whether it's necessary must be considered up front. As in some cases, these technologies are likely to raise issues regarding the data protection legal framework. Thus, some aspects, such as the implementation of obligations concerning sub-contracting or the rules governing cross-border transfers of personal data, require particular attention from actors using Blockchains, in particular for public Blockchains.

Furthermore, principles relating to security of data remain entirely applicable to Blockchains. These systems can take different shapes and the choices made by data controllers (between a permissioned Blockchain and a public Blockchain, between different formats for recording data on blocks, etc.) can have a significant impact, both positively and negatively, on risks to individuals' rights and freedoms. In that sense, we intend to develop further works accompanying specific implementations of Blockchain-based solutions in different governmental sectors, in order to verify how they manage the restrictions imposed by GDPR and other data protection regulations, and how they work with the characteristics of the Blockchain technology to design appropriate systems.

ACKNOWLEDGMENTS

This paper is a result of the project SmartEGOV: Harnessing EGOV for Smart Governance (Foundations, Methods, Tools) NORTE-01-0145-FEDER-000037, supported by Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (EFDR).

REFERENCES

[1] CNIL. 2018. *Solutions for a responsible use of the Blockchain in the context of personal data*. Technical Report. Commission Nationale Informatique & Libertés. 10 pages. https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

[2] European Central Bank and Bank of Japan. 2018. *Securities settlement systems: delivery-versus-payment in a distributed ledger environment – Stella project report phase 2.* Technical Report March. https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf

[3] Oded Goldreich. 2001. *Foundations of Cryptography*. Vol. I. Cambridge University Press, Cambridge, UK.

[4] Christiaan Lemmen, Jacques Vos, and Bert Beentjes. 2017. Ongoing Development of Land Administration Standards: Blockchain in Transaction Management. *European Property Law Journal* 6, 3 (2017), 478–502. https://doi.org/10.1515/eplj-2017-0016

[5] Filipa Matias Magalhães and Maria Leitão Pereira. 2018. *Regulamento Geral de Proteção de Dados* . Manual Prático (2 ed.). VidaEconómica, Porto, Portugal.

[6] Roger Maull, Phil Godsiff, Catherine Mulligan, Alan Brown, and Beth Kewell. 2017. Distributed ledger technology: Applications and implications. *Strategic Change* 26, 5 (2017), 481–489. https://doi.org/10.1002/jsc.2148

[7] Teogenes Moura and Alexandre Gomes. 2017. Blockchain Voting and its effects on Election Transparency and Voter Confidence. In *Proceedings of the 18th Annual International Conference on Digital Government Research (dg.o '17)*. ACM, New York, NY, USA, 574–575. https://doi.org/10.1145/3085228.3085263

[8] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. , 9 pages. https://bitcoin.org/bitcoin.pdf

[9] Arvind Narayanan and Jeremy Clark. 2017. Bitcoin's Academic Pedigree. *Commun.* ACM 60, 12 (2017), 36–45. https://doi.org/10.1145/3132259

[10] Jason Potts, Ellie Rennie, and Jake Goldenfein. 2017. Blockchains and the crypto city. *it - Information Technology* 59, 6 (2017), 285–293. https://doi.org/10.1515/itit-2017-0006

[11] Rogelio Rivera, José G. Robledo, Víctor M. Larios, and Juan Manuel Avalos. 2017. How Digital Identity on Blockchain can contribute in a smart city environment. In *2017 International Smart Cities Conference (ISC2)*. 1–4. https://doi.org/10.1109/ISC2.2017.8090839

[12] Paolo Tasca and Claudio J. Tessone. 2017. Taxonomy of Blockchain Technologies. Principles of Identification and Classification. arXiv:arXiv:1708.04872v2

[13] Mark Walport. 2015. Distributed ledger technology: Beyond block chain. Technical Report. UK Government Office for Science, London. 1–88 pages.https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment{_}data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[14] Karl Wüst and Arthur Gervais. 2018. Do you need a Blockchain?. In *2018 CryptoValley Conference on Blockchain Technology (CVCBT)*. 45–54. https://doi.org/10.1109/CVCBT.2018.00011

[6] A commitment scheme is a basic ingredient in many cryptographic protocols that enables a party to commit itself to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later [3].