Blockchain and the GDPR: A Data Protection Authority Point of View

Amandine Jambert(✉)

C.N.I.L. - Commission Nationale de l'Informatique et des Libertés, Paris, France
ajambert@cnil.fr

Since the publication, in 2009, of the blockchain founding article by Nakamoto [3] more and more solutions rely on this architecture. In the process an increasing number of solution process personal data stored on this type of decentralized database. In this context the property of undeniability (i.e. once data is recorded, it cannot be altered or removed) of such solutions raise questions regarding how to assure compliance to GDPR. The French Data protection authority, the CNIL, received numerous requests from both the public and the private sector regarding blockchain projects and GDPR [1]. She thus addressed the matter in November 2018 through a publication on its website [2].

The objective of this talk was to give the main key points of the GDPR, to underline how they can apply in the blockchain context and finally to show how we hope for cryptographic techniques to solve part of the problems.

1 How Do the GDPR and Blockchain Interact?

When a blockchain contains personal data, such as public keys of individuals or personal data stored "within" a transaction, the GDPR may be applicable as it implies the processing of personal data. The second criteria for applicability will be whether the processing is performed by controllers or processors established in the EU or aiming at EU residents. Finally, this legal framework is applicable to any processing of personal data by a legal person or by a natural person not acting in the course of a purely personal or household activity. Thus, the GDPR is applicable to processing on blockchain in a wide array of cases.

Furthermore, some classical blockchain properties, especially transparency (i.e. all participants can view all data recorded) and undeniability, may have impacts on individual rights (namely, the right to privacy and the right to personal data protection) which calls for a specific analysis.

In consequence, the CNIL suggests the following initial analysis and recommendations to stakeholders who wish to use blockchain when carrying out personal data processing.

We consider in this short paper only the cases of processing on the blockchain using the payload to store personal data.

Published by Springer Nature Switzerland AG 2019
O. Blazy and C. Y. Yeun (Eds.): WISTP 2018, LNCS 11469, pp. 3–6, 2019.
https://doi.org/10.1007/978-3-030-20074-9_1

2 Which Points Require Particular Attention?

Blockchains are a technology, not a processing in itself. In consequence the questions to be answered while processing data on a blockchain are similar to the questions that would have been raised for any others processing. However, the particular properties of the blockchain might interact with those obligations in positive or negative ways.

2.1 Responsibilities

The first point of attention will be to determine a clearly defined purpose for the processing using the blockchain and to clarify the responsibilities of the actors involved.

Regarding the responsibilities, the work carried out by the CNIL has revealed that, in many cases, the person deciding to register data on a blockchain can be considered as a data controller given that the participant determines the purpose (objectives pursued by the processing) and means of data processing (data format, use of a given blockchain technology, etc).

The miners, or validators, of transactions including personal data on a blockchain are not involved in the definition of the purpose, thus they would not be considered as controller by the CNIL. Nevertheless they are still processing data, they thus would be, at best, processors. Being a processor in the GDPR implies numerous obligation stated in article 28 which might be difficult in practice for public blockchain.

Thus for those last solutions, the CNIL is currently conducting an in-depth reflection on the matter and promotes the development of solutions to address contractual relations between participants/data controllers and miners.

2.2 Risk Minimization

The second point can be summed up as the minimization of risks for data subjects when their data are planned to be used in a processing carried out on a blockchain. In some cases, these technologies are likely to raise issues regarding the GDPR or to put unnecessary high risks on individuals. Therefore, it is necessary to balance, from an early stage, the needs of using a blockchain rather than another technology with the objectives and characteristics of each processing. In addition to questioning the use of a blockchain, the data controller must also question which type of blockchain, either a public or a permissioned blockchain (as defined in [5]) should be used and how it will be used to limit the risks on individuals.

f blockchain properties are not required in order to meet the purpose of the processing, the CNIL recommends favouring other solutions that allow for fullcompliance with the GDPR.-Permissioned blockchains should be favoured as they allow a better control over personal data governance, in particular as regards transfers outside of the EU.-The requirement for appropriate safeguards for transfers outside the EU, such as binding corporate rules or standard contractual clauses, are entirely applicable to permissioned blockchain.

2.3 Data Subject's Rights

The third point of attention concerns the exercise of rights. Some of them can be exercised effectively such as the right of access and the right to portability. Others, like the right to erasure, the right to rectification and the right to object to processing, are not straightforward. In those cases, the CNIL acknowledges the existence of technological solutions that should be evaluated.

2.4 Miscellaneous

Finally, while not covered here, actors need to be as cautious as possible regarding the implementation of obligations concerning sub-contracting and the rules governing international transfers of personal data, in particular for public blockchains.

3 What Are the Technical Solutions Considered?

We can define the data manipulated on a blockchain as two categories: the identifiers (i.e. the public keys of participants) and the payload which is used in numerous processing on blockchain.

The architecture of most blockchain needs the identifier to be visible to function, thus the CNIL considers that those data, in those cases, can not be further minimized and that their retention period will be in line with the blockchain life.

On the contrary, the payload format is chosen by participants independently to the blockchain architecture. The Privacy by Design principle (Article 25 of the GDPR) requires the data controller to choose the format with the least impact on individuals' rights and freedoms.

The CNIL considered different cryptological solutions to answer the challenge, from perfectly hiding commitment, as defined in [4], to secure encryption.

As the most protective format, the CNIL considers that personal data should be preferably registered on the blockchain as a commitment. The choice of a perfectly hiding commitment scheme would ensure that, upon erasure of the witness and the data committed (both kept off the blockchain), it would no longer be possible to prove or verify which information have been committed. The commit would be considered, by the CNIL, has anonymized in such a way that it can no longer be considered personal data.

If this is not possible, one may use a hash of the data generated using a keyed-hash function, or, at least, a ciphertext.

Excluding the specific case of perfectly hidding commitment, those solutions do not provide a perfect erasure of the data, insofar as the data would still exist in the blockchain and might be recovered in a distant future depending on cryptanalysis advances. However, the CNIL observes that they are partially answering the problem of giving an effective exercise of the right of erasure. Nevertheless, their acceptability for what concerns the requirements of the GDPR should still be evaluated.

The common feature underlying some of these solutions is to store any 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 generated from a keyed hash function, etc.). It is technically impossible to grant the request for rectification or for erasure made by a data subject when cleartext or hashed data is recorded on a blockchain. It is therefore strongly recommended, from a GDPR point of view, not to register personal data in cleartext on a blockchain, and to use one of the others cryptographic solutions mentioned above.

Nevertheless, if no other solution is applicable, and when justified by its purpose, a DPIA can be carried out to evaluate whether the risk of storing the information either as a simple hash or in cleartext would be acceptable. If the conclusion are that risks on data subject are minimal then it can be exceptionally envisaged. For example when a data controller have the legal obligation to make some information public and accessible, without a retention period, the storage of personal data on a public blockchain can be envisaged, provided that the DPIA concludes that the risks for data subjects are minimal.

4 Conclusion

Blockchains raise numerous challenges in terms of compliance with human rights and fundamental freedoms that can be partially answered by technical solution. Nevertheless, it still call for a response at the European level. As one of the first authorities to officially address the matter, the CNIL will work cooperatively with its European counterparts to suggest a strong and harmonised approach.

References

1. 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
2. CNIL: Solutions for a responsible use of the blockchain in the context of personal data, November 2018. https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf
3. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system, May 2009
4. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_9
5. Smith, J., Tennison, J., Wells, P., Fawcett, J., Harrison, S.: Applying blockchain technology in global data infrastructure. Open Data Institute, ODI Technical report (2016)