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

Amandine Jambert

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

As more and more solutions rely on blockchain for processing personal data, questions regarding how to assure compliance to GDPR rose. 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 eat EU residents. 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 irreversibility (i.e. once data is recorded, it cannot be altered or removed), 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 and the cases of smart contract using personal data.

2 Which points require particular attention?

Blockchains are a technology, not a processing in itself. Thus 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[1] deciding to register data on a blockchain can be considered as a data controller given that the participant determines the purpose and means of data processing. The miners, or validators, of transactions including personal data on a blockchain would be, at best, processors. For public blockchains, 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.

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 should be used and how it will be used to limit the risks on individuals.

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.

Finally, while not covered here, actors need to be as cautious as possible regarding the implementation of obligations concerning sub-contracting an 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 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.

As the more protective format, the CNIL considers that personal data should be registered on the blockchain preferably as a commitment. If this is not possible, one may use a hash of the data generated using a keyed-hash function, or, at least, a ciphertext.

[1] The GDPR does not apply to processing of personal data by a natural person acting in the course of a purely personal or household activity.

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.).

In a general manner, it is important to avoid storing personal data in cleartext on the blockchain. 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 envisaged.

Note that the choice of the most protective solutions allows the controller to answer to most of the questions regarding the exercise of data subject rights. In particular, when using a perfectly hiding commitment scheme, the deletion of the witness and the value committed (both stored out of the chain) is sufficient to render the commitment anonymous in such a way that it can no longer be considered personal data? This solution thus allows a data controller to both respects any pertinent data retention period and respect any request of erasure.

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. Available at `https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf`, November 2018.