CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

BLOCKCHAIN

Solutions for a responsible use of the blockchain in the context of personal data

Blockchain is a technology with a high potential for development that raises many questions, including on its compatibility with the GDPR. For this reason, the CNIL has addressed this matter and offers concrete solutions to actors who wish to use it to process personal data. Blockchain is a technology on which personal data processing can rely but it is not a data processing operation with its own purpose.

1- Who is the data controller in a blockchain?

The 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.

However, the CNIL observes that **participants**, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered as **data controllers**.

Indeed, blockchain participants define the purposes (objectives pursued by the processing) and the means (data format, use of blockchain technology, etc.) of the processing.

More specifically, the CNIL considers that the participant is a data controller:

- when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal);
- when the said participant is a legal person and that it registers personal data in a blockchain.

For example, if a notary records his or her client's property deed on a blockchain, the said notary is a data controller. In addition, if a bank enters its clients' data onto a blockchain as part of its client management processing, it is a data controller.

2- Are all actors involved in a blockchain data controllers?

No. Miners are only validating transactions submitted by participants and are not involved in the object of these transactions: therefore, they do not define the purposes and the means of the processing.

Furthermore, natural persons who enter personal data on the blockchain, that do not relate to a professional or commercial activity, are not data controllers (pursuant to the "purely personal or household activity" exclusion set out in Article 2 of the GDPR).

For example, a natural person who buys or sells Bitcoin, on his or her own behalf, is not a data controller. However, the said person can be considered a data controller if these transactions are carried out as part of a professional or commercial activity, on behalf of other natural persons.

3- What happens if several participants jointly decide to carry out processing operations on a blockchain?

When a group of participants decide to carry out processing operations with a common purpose, the CNIL recommends to identify beforehand the data controller. For example, the participants may create a legal person in the form of an association or economic interest group. They may also choose to identify one participant who makes decisions for the group and to designate the said participant as a data controller.

Otherwise, all participants could be considered joint controllers, as provided by Article 26 of the GDPR, and must therefore determine, in a transparent way, their respective responsibilities to ensure compliance with the regulation.

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.

 Regarding smart contracts, as for any software, the algorithm developer may simply be a solution provider or, when the said algorithm developer participates in the processing, may be qualified as a data processor or data controller depending on its role in determining the purposes of the processing.

The key points

- The CNIL considers that the participant may be qualified as a data controller:
  - when the said participant is a natural person and the processing is related to a professional or commercial activity;
  - when the said participant is a legal person that registers personal data in the blockchain;
- When a group of entities decides to carry out processing operations on a blockchain for a common purpose:
  - the CNIL recommends that the participants take a common decision about the data controller's responsibilities:
    - either by creating a legal person to be the data controller;
    - or by designating the participant that makes decisions for the group as the data controller;
  - otherwise, all participants are likely to be considered as being joint controllers.

4- Are there data processors, within the meaning of the GDPR, in a blockchain?

Yes, such as smart contract developers who process personal data on behalf of the data controller.

For instance, a software developer offers a solution to an insurance company, in the form of a smart contract that enables passengers to be automatically reimbursed when their flight has been delayed. This developer would be qualified as a data processor if he or she intervenes in the processing of personal data, the insurance company being the data controller.

In some cases, miners can also be considered data processors, within the meaning of the GDPR. Indeed, they follow the data controllers' instructions when 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 chain rules, to carry out its transaction).

They should therefore establish a contract with the participant, acting as data controller, which specifies each party's obligations and which reproduces the provisions of Article 28 of the GDPR (for further information on the data processor's obligations, click here).

For example, if several insurance companies decide to create a permissioned blockchain for their processing operations, the purpose of which is compliance with their KYC ("Know Your Customer") obligations, they may decide that one of them is the data controller. In this case, the other

insurance companies, which validate transactions as miners, are likely to be considered as data processors.

 Given the practical difficulties that can be raised by qualifying miners as data processors in a public blockchain (particularly for the obligation to formalise relations with the data controller in the form of a contract), the CNIL is carrying out an in-depth reflection on this matter. Stakeholders are also encouraged to use innovative solutions allowing them to ensure compliance with data processors' obligations under the GDPR.

The key points:

- In a blockchain, the data processor, within the meaning of the GDPR, can be:
  - the smart contract developer who processes personal data on behalf of the participant, who is the data controller;
  - the miners who validate the transaction containing personal data on a blockchain.
- 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.

How to minimize the risks for data subjects when a processing is carried out on a blockchain?

1- Carefully assess beforehand the need to use a blockchain, particularly a public one

Blockchain's characteristics are not without consequence on compliance with the obligations arising from the GDPR. As part of its Privacy by Design obligations (Article 25), the data controller must give prior thought to the appropriateness of choosing this technology to implement its processing.

Indeed, a blockchain is not necessarily the most suitable technology for all data processing; it can be a source of difficulties for data controllers in terms of compliance with the obligations set out by the GDPR.

For example, transfers outside of the European Union (EU) can be particularly problematic, especially in the case of public blockchains.

As a reminder, all transactions on the blockchain involve:

- a request to validate the transaction (and therefore potentially personal data) being sent to all miners of the chain;
- an update to the blockchain by adding a new block on the chain for all participants.

However, whether they are miners or not, participants can be located in countries outside of the EU. This therefore raises the question of compliance with obligations for transfers outside of the EU (for further information see the page on "Data transfers outside of the EU [FR]").

While appropriate safeguards for a transfer outside the EU may be used in a permissioned blockchain, such as standard contractual clauses, binding corporate rules, codes of conduct or even certification mechanisms, the CNIL observes that these safeguards are harder to implement in a public blockchain, given that the data controller has no real control over the location of miners.

The key points:

- If blockchain properties are not required in order to meet the purpose of the processing, the CNIL recommends favouring other solutions that allow for full compliance 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 blockchains.

2- Choose carefully the format under which the data will be registered

The data minimisation principle requires that the data collected be relevant and limited to what is strictly necessary in view of the purposes for which they are processed. Furthermore,

personal data cannot be stored for an unlimited time: a data retention period [FR] must therefore be defined according to the purpose of the data processing.

However, one of the characteristics of blockchains is that the data registered on a 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.

Some technical solutions, set out below, should be examined by stakeholders in order to solve this issue.

> The CNIL recognizes the value of these solutions but, at this point, questions their ability to ensure a full compliance with the GDPR. This subject is one of the issues for which a reflection at the European level is essential

As a reminder, a blockchain can contain two categories of personal data:

The identifiers of participants and miners:

Each participant has an identifier comprised of a series of alphanumeric characters which look random, and which constitute the public key to the participant's account. This public key is linked to a private key, known only by the participant (for further information on cryptology, click here[FR]).

The very architecture of blockchains means that these identifiers are always visible, as they are essential for its proper functioning.

The CNIL therefore considers that this data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence.

Additional data (or payload):

Besides the participants' identifiers, the additional data stored on the blockchain can contain personal data, which can potentially relate to individuals other than participants and miners.

As a reminder, the principle of data protection by design (Article 25 of the GDPR) requires the data controller to choose the format with the least impact on individuals' rights and freedoms.

The CNIL considers that personal data should be registered on the blockchain preferably in the form of a commitment[1]. If this is not possible, one may register the data in the form of a hash generated using a hash function with a key, or, at least, in the form of an encryption ensuring a high level of confidentiality.

[1] A "commitment" is a cryptographic mechanism that allows one to "freeze" data in such a way that it is both possible - with additional information - to prove what has been frozen and impossible to find or recognise such data by using this sole "commit" .

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.).

 If justified by the purpose of the processing and if a data protection impact assessment (DPIA) has proven that the residual risks are acceptable, personal data may exceptionally be stored on the blockchain, in the form of a traditional fingerprint (without a key) or even in cleartext. Indeed, some data controllers may have the legal obligation to make some information public and accessible, without a retention period: in this particular case, 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.

The key points:

- Given that the participants' identifiers, i.e. their public keys, are essential to the blockchain's proper functioning, the CNIL considers that it is not possible to further minimise them; the retention period is in line with that of the blockchain.
- With respect to additional personal data, in order to ensure compliance with data protection by design and by default and data minimisation obligations, the CNIL recommends solutions in which data is processed outside of the blockchain or, in which the following are stored on the blockchain, in order of preference:
    - a commitment of the data;
    - a hash generated by a keyed hash function on the data;
    - a ciphertext of the data.
- If none of these solutions can be implemented, and when justified by the purpose of the processing, and when a DPIA has proven that the residual risks are acceptable, data can be stored either using a hash function without a key or, in the absence of any other possibilities, in cleartext.

How to ensure the effective exercise of rights?

The GDPR was designed to give individuals back their control over personal information. It therefore significantly strengthens individuals' rights against those who process their data and, in addition, creates new rights (for an explanation on individuals' rights in the age of the GDPR, click here[FR]).

Besides minimising risks to individuals, as mentioned above, the format chosen to register the data on a blockchain can also facilitate the exercise of individual rights.

Though the effective exercise of some rights does not seem to be problematic, applying the right to erasure, the right to rectification and the right to object to a blockchain is worth considering a more in-depth analysis.

1- Rights that are entirely compatible with a blockchain

The information right of data subjects is not problematic: the data controller must provide concise information that is easily accessible and formulated in clear terms to the data subject before submitting personal data to miners for validation.

The same applies for the right of access and the right to portability: the CNIL considers that the exercise of these rights is compatible with blockchains' technical properties.

2- Technical solutions for the exercise of rights to move closer towards a compliance with the GDPR

The CNIL observes that it is technically impossible to grant the request for erasure made by a data subject when data is registered on a blockchain. However, when the data recorded on the blockchain is a commitment, a hash generated by a keyed- hash function or a ciphertext obtained through "state of the art" algorithms and keys, the data controller can make the data practically inaccessible, and therefore move closer to the effects of data erasure.

- **For example, the mathematical properties of some commitment schemes[2] can ensure that upon erasure of the elements enabling it to be verified, it will be no longer be possible to prove or verify which information has been committed. The commitment itself would therefore no longer represent any risk in terms of confidentiality. The information would also need to be deleted in other systems where it has been stored for processing.**
- **Another example is the deletion of the keyed hash function's secret key, which would have similar effects. Proving or verifying which information has**

[2] When a commitment scheme is perfectly hiding, deleting the witness (i.e. the element that allows to verify that a given value is committed in a given commit) and the value committed is sufficient to render the commitment anonymous in such a way that it can no longer be considered personal data.

been hashed would no longer be possible. In practice, the hash would no longer pose a confidentiality risk. Once again, the information would also need to be deleted in other systems where it has been stored for processing.

Excluding the specific case of some commitment schemes, these solutions do not, strictly speaking, result in an erasure of the data, insofar as the data would still exist in the blockchain. However, the CNIL observes that it does allow data subjects to get closer to an effective exercise of their right of erasure. Their equivalence for what concerns the requirements of the GDPR should be evaluated.

 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 not to register personal data in cleartext on a blockchain, and to use one of the cryptographic solutions mentioned above.

As regards the right of rectification, the impossibility to modify the data in a block must cause the data controller to enter the updated data in a new block. Indeed, a subsequent transaction can cancel an initial transaction, even though the first transaction will still appear in the chain. The same solutions as those applied following a request for deletion of personal data could be applied to erroneous data when such data requires deletion.

Although this approach is somewhat different, it requires, similarly to other rights, a careful consideration in advance regarding the right to restriction (introduced by Article 18 of the GDPR) and to human intervention in the context of entirely automated decision-making (Article 22 Paragraph 3).

For example, it would be possible to restrict the use of data in smart contracts, simply by including this possibility in advance in the programme.

It appears that an exclusively automated decision arising from a smart contract is necessary for its performance, given that it enables the fulfilment of the very essence of the contract (i.e., the reason for which the parties concluded the contract). With respect to the suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, the data subject should be able to obtain human intervention, to express his or her point of view and to contest the decision after the smart contract has been performed. The data controller should therefore provide the possibility of human intervention allowing the data subject to contest the decision even if the contract has already been performed, and regardless of what is registered on the blockchain.

The Key points:

- The rights of information, of access and of portability are not, at first glance, particularly problematic on the blockchain technology.
- Similar to risk minimization, the choice of a proper cryptological method to store the data allows the data subject to move closer to an effective exercise of his or her rights: erasure of data stored outside of the blockchain and of elements enabling their verification, which allows for access to the proof recorded on the blockchain to be cut off and makes the data difficult and even impossible to retrieve;
- Taking that data subject's rights into account while writing the programme, i.e. prior to the implementation of a smart contract, allows for processing restriction or human intervention requests to be granted;
- The equivalence of these solutions with the requirements arising from the GDPR, in particular for what concerns retention periods and the right to erasure, requires a thorough evaluation.

What about security requirements?

The different properties of a blockchain (transparency, decentralisation, tamper-proof and disintermediation) mainly rely on two factors: the number of participants and miners, and on a set of cryptological mechanisms.

For permissioned blockchains, depending on the potential divergence or convergence of participating actors' interests, the CNIL recommends carrying out an evaluation of the minimal number of miners which would ensure the absence of a coalition that could control over 50% of powers over the chain.

The CNIL also recommends setting out technical and organisational procedures to limit the impact of a potential algorithm failure (particularly the publication of a vulnerability on a cryptographic mechanism) on the security of transactions, including an emergency plan to be implemented enabling algorithms to be changed when a vulnerability is identified.

Furthermore, the governance of changes to the software used to create transactions and to mine should be documented, and technical and organisational procedures should be set out to ensure an alignment between planned permissions and practical application.

Particular attention should be granted to the measures implemented to ensure the blockchain's confidentiality if it is not public.

Any data controller carrying out processing through transactions on a blockchain should ensure the security of secret keys used, for example by ensuring that they are stored on secure media.