Using Blockchain to strengthen the rights granted through the GDPR

F.W.J. van Geelkerken¹, K. Konings²,³

1. Corporate Law and European Law, section Law & IT, Groningen University, Oude Kijk in ‘t Jatstraat 9, 9712 EK Groningen, THE NETHERLANDS.
   F.W.J.van.Geelkerken@rug.nl
2. Corporate Law and European Law, section Law & IT, Groningen University, Oude Kijk in ‘t Jatstraat 9, 9712 EK Groningen, THE NETHERLANDS.
   K.Konings@rug.nl
3. NORD Legal LLP, Trompsingel 35, 9724 DA Groningen, THE NETHERLANDS

Abstract – In this article we delineate two ways in which Blockchain technology could be utilised to store personal data in compliance with the requirements of the General Data Protection Regulation 2016/679, and what their up- and downsides are.

Keywords – Blockchain, transparent Blockchain, opaque Blockchain, GDPR, 2016/079, compliance.

I. Introduction

Lately Blockchain seems to be the quintessential buzzword in “governance land”, and it is as if all more or less traditional governance parties want to have a stake in it. Blockchain is a term widely used, which represents an entire new suite of technologies. There is, however, substantial confusion around its definition seeing as the technology is relatively new, and can be implemented in many ways depending on the objective.

There is, however, a general consensus in the IT(-law) community that the use Blockchain-technology can, and will, change our society profoundly. It could – amongst other – have a significant effect on the position of-, and need for, trusted third parties such as public notaries, governments, banks and the cadastre, which might explain the interest of such traditional governance parties in claiming their respective stake in Blockchain.

In this article a short overview of the technological underpinnings of Blockchain will be provided to afterwards elaborate on how Blockchain technology could be used for the processing of personal data compliant with the General Data Protection Regulation[1] (hereafter referred to as ‘GDPR’).

I. Blockchain-technology

A Blockchain is in essence nothing more than a digital ledger containing lines of data or information.[2][3]

Such a ledger can contain different types of data, varying from transaction records, transactional attributes, credentials, or any other piece of data or information. As a matter of principle only lines of data can be added to this digital ledger, and none can be removed or altered.

Such a digital ledger is spread over a large number of users, computers, or ‘nodes’ within a Blockchain network, whereby not one single copy of this digital ledger is authoritative. There is not one authoritative copy for all copies synchronise with one another and are thus each of equal evidentiary value. As such if in one copy of the digital ledger a line of data or information is added, this line will be added to all other copies of the ledger.[4]

Next to that a Blockchain does not require the participant to have a high-level of trust – or any trust for that matter – in the individual nodes which make up the Blockchain network. Whereas in a traditional network the user has to trust the reliability of each nodes of the network, be it the app used for Internet banking, the connection to the central server, or the database used by the bank.

The fact that a Blockchain does not require the participant to have any trust in the individual nodes of the network is what allows the exchange of data across the globe without resorting to traditional governing entities such as banks, insurance companies, or governments. For the power of Blockchain-technology – or, in general, distributed ledger technology (DLT) – is that if one of the nodes alters pre-existing data this change will be rejected by the other nodes, and the ledger itself is most often secured by applying one or more layers of cryptography and applying game theory.

It is therefore not possible to alter pre-existing data in a Blockchain as long as there are not 50% plus one node within the network which reflect this alteration. Because in practice the individual lines of data cannot be altered, Blockchain is a very secure technology, and the data or information stored within it is to such a large extent trustworthy. Next to that Blockchain greatly increases transparency amongst its participants. Seeing as any participant to the Blockchain, be it one running a node or one merely storing data in the Blockchain, can access all contents of the Blockchain, the exchange of data or information is fully transparent.

In itself Blockchain is only one example of distributed ledger technology, what distinguishes Blockchain from other forms of DLT is, however, its use of Blocks. Each set of alterations[5] of the digital ledger is bundled into one Block and to this block a header is added consisting of a hash[6] of the preceding Block. By affixing different Blocks to each other a chain is formed, hence the name Blockchain.

Seeing as the hash is made of the preceding block, the contents of that (preceding) block cannot be altered unnoticed[7]. This principle is illustrated in image 1 – depicting a highly simplified representation of a Blockchain consisting of four Blocks – in which each consecutive Block consists of three transactions. Each of the Blocks contains a header containing a hash of the Block preceding it. As shown, if the contents of Block2 are altered, resulting in Block2’, the hash in the header of Block3 no longer corresponds with that of the contents of Block2, and that change will be rejected. If this change were accepted the hash in the header of Block4 no longer corresponds with that of the contents of Block4, and that change would be rejected.
Transparent- and opaque Blockchains

The most well-known Blockchain is the one upon which the original crypto-currency, the Bitcoin, is based. The Blockchain which formed the basis for the Bitcoin is an example of a transparent Blockchain. Anyone can open an account, become a node, and afterwards check each transaction within the network. And because Bitcoin uses a transparent Blockchain all participants/nodes have equal rights, as there is no governing body. A public Blockchain like that of Bitcoin should be distinguished from a (more) opaque Blockchain. A Blockchain can be more opaque by limiting:

- who can be a node;
- which parties get access c.q. can access the Blockchain; or
- by limiting which information the different parties can see within the Blockchain.

A more opaque Blockchain does require dependency on some sort of a trusted third party but according to Heukelom et.al.[9] a (more) opaque Blockchain[10] makes it possible to reliably and securely process personal data in compliance with the GDPR.

III. GDPR compliant processing of personal data using Blockchain technology

As stated before, the underlying principle of Blockchain technology is that stored data cannot be altered without as a consequence invalidating all subsequent blocks. As will be shown, this would a priori disqualify Blockchain as a method for the processing of personal data. Hereafter first the GDPR will be elaborated on to afterwards explain how it is possible to process personal data in a Blockchain in compliance with the GDPR.

A. The General Data Protection Regulation

The GDPR is (almost) always applicable when personal data is processed. There are a number of terms which are of crucial importance in the GDPR, each of which will be addressed in short hereafter.

Based on article 4 section 1 GDPR ‘personal data’ means;

[A]ny information relating to an identified or identifiable natural person (‘data subject’) an ‘identifiable natural person’ is defined as;

[O]ne 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.

and based on article 4 section 2 GDPR the ‘processing’ of personal data is defined as;

[A]ny 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

As such if any identifier such as name, address, telephone number, or social security number is stored (i.e. ‘recorded’ in the sense of art. 4 section 2 GDPR) in a Blockchain, this constitutes ‘processing’ of personal data and is thus subject to the GDPR. If personal data are, however, irreversibly anonymised[11] and are not relatable to an identified or identifiable natural person there is no personal data and the GDPR is not applicable.

There are two very important rights granted to the data subject in GDPR. The first of these is that the GDPR grants the data subject a right[12] to ask for rectification or completion of his or her personal data, based on art. 16 GDPR. This right, in short, entails that if stored personal data regarding a data subject is (initially) incorrect or incomplete, or has become incorrect or incomplete – because of outside changes – the data subject can ask to have these personal data altered. The second right[12] the GDPR grants a data subject is, based on art. 17 GDPR, the right to ask for erasure of his or her personal data. In short this right entails that a data subject can ask for the erasure of his or her personal data if the personal data are no longer necessary for the objective the data were provided or he or she withdraws consent for the processing.

Two further terms which are of importance in light of this research is the distinction made between the ‘controller’ and the ‘processor’ in the GDPR. A ‘controller’ is defined in on article 4 section 7 GDPR as;

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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

and ‘processor’ is defined in article 4 section 8 GDPR as;

a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Whereby in principle the ‘processor’ is mainly indirectly, through a processing agreement, and the
‘controller’ is directly obligated to comply with all obligations flowing forth from the GDPR. If personal data are stored within a Blockchain these personal data will be processed by the various participants within that Blockchain. In itself this is no more than an innovative way of exchanging personal data between the various participants within one Blockchain. As there is no hierarchical relationship – unless other agreements have been made – every participant in the Blockchain is equal, and therefore every participant is equally entitled to do what they want with the information in the Blockchain. It is therefore not really possible to speak of one processor when storing personal data in a Blockchain, but rather all participants in the Blockchain are controller. This raises a series of serious questions such as:

- how should the responsible parties take care of Blockchain security? And
- how can data subjects enforce their personal data rights against the controllers? And
- what happens in case of a data breach?

Are, for instance, all participants in that Blockchain then – based on art. 33 section 1 GDPR – obliged to report this data breach to the (national) supervisory authority?

### B. Processing personal data GDPR compliant in a transparent Blockchain

The starting point is that all participants in a Blockchain in which personal data are stored are responsible for this storage and further processing under the GDPR. The parties who run nodes within a Blockchain network are most likely processors, seeing as the primary task of these parties is to make certain the Blockchain functions for all (responsible) participants and they do not determine the purpose(s) nor the means of the processing. If the parties that run nodes are indeed processors the (responsible) participants are based on art. 28 GDPR obliged to conclude processor agreements with the parties who run nodes. This is not very practical (as it would most likely require a significant amount of processor agreements), but in theory it is certainly not unfeasible.

As stated before, one of the strong points of Blockchain technology is that one can trust the validity of information because of its inalterability. As pointed out in the previous section though, this conflicts with the GDPR which grants a right to the data subject that as soon as personal data are no longer needed these should be erased, and the data subject has the right to ask for erasure. And similarly data subjects have the right to alter incorrect or outdated personal data. Regarding the former – the erasure of personal data – this could be achieved by, instead of erasing the data, encrypting the personal data and deleting the key used afterwards. That way the (original) data would not be removed, but an (extra) block would be added detailing the encryption (and subsequent deletion of the key).

Regarding the latter – the problem of needing to be able to alter personal data once the data subject requests this – this could be achieved by adding a block with updated information. Another (potentially better) alternative would be the ‘erasure of the ‘old’ personal data by encrypting it and deleting the key and the addition of a block with the ‘new’ personal data. Either alternative would result in the inalterability character of data stored in a Blockchain not being violated.

### IV. Processing personal data GDPR compliant in a more opaque Blockchain

Processing of personal data in a more opaque Blockchain poses the same problems as it does in a transparent Blockchain. Within an opaque Blockchain – where either a party has control over 50% + 1 of all nodes, or another way of (trusted) third party governance is present – it is, however, relatively easy to conceive solutions for the aforementioned problems. It would for instance be possible to appoint one party amongst all of the responsible parties who is in charge of complying with statutory tasks (such as reporting data breaches). This is specifically the way joint controllers could organize themselves. Based on art. 26 GDPR they should determine their respective responsibilities for compliance to the GDPR in a transparent manner by means of an arrangement. This arrangement may designate a single point of contact for data subjects, a data subject may, however, exercise his or her rights against any of the controllers.

Similarly, if the parties that run nodes are deemed processors in light of the GDPR, instead of concluding numerous processor agreements based on art. 28 GDPR with the parties who run nodes, this issue can be easily solved by making joint agreements between all participants and parties that run the nodes.

Regarding the third problem, the erasure of personal data, this can easily be resolved, for the removal of personal data requires a majority of all nodes (based on the majority polling result). This means that in an opaque Blockchain whereby one party has the power over 50%+1 of all nodes, the erasure of (personal) data from the Blockchain is very feasible. In such a scenario the majority of nodes would erase the data and all other nodes would subsequently erase the data as well.

As such the obligation to erase personal data stemming from the GDPR does not prevent the storage of personal data in a Blockchain. Regarding the fourth problem, the alteration of personal data, this could quite easily be resolved in the same way as the erasure of data, by changing the stored data for a majority of all nodes. As a consequence of the majority polling result all nodes will alter the data.

### Conclusion

In this article we have delineated two ways in which Blockchain technology could be utilised to store personal data in compliance with the requirements of the GDPR, either by using a transparent- or opaque Blockchain.

The former, a transparent Blockchain, has the upside that the original intention of Blockchain technology – the non-reliance on trusted third parties – is upheld and the security-, and trustworthiness of the data remains intact. On the other hand it would require (most likely) a
significant amount of individual processor agreements, and raises a number of questions regarding the compliance to (national) statutory tasks.

The latter, an opaque Blockchain, has amongst others the upside that it requires significantly less processor agreements, there is no need to question the compliance to (national) statutory tasks, and it is possible to factually erase or alter personal data. On the other hand it would require a returning to the reliance on a trusted third party, and the security-, and trustworthiness of the data would be as high as that of the trusted third party.

References


[3] Seeing the use of, and distinction between, the terms data and information in the GDPR is confusing at best, even though there is a significant difference between them, hereafter the terms data and information will be used as they are in the GDPR.

[4] In cases where there is a discrepancy between the different ledgers – for instance because 10 changes were made simultaneously – the network resolves this by polling all nodes and the majority rules.


[6] A hash-function is a function in information sciences which converts a very large dataset into (most often) a much smaller dataset.


[8] In this case the term ‘transaction’ means any alteration i.e. addition to the chain and not necessarily any financial transaction.


[10] Instead of the terms transparent- and opaque Blockchain they refer to them as open- and closed Blockchains.

[11] Consideration 26 GDPR (only) states that the principles of data protection should not apply to […] personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, as such the anonymisation would not need to be irreversible. The different (national) supervisory authorities have, however, ruled that a reversible anonymised personal data are also personal data in the sense of Directive 95/46/EC, the predecessor of the GDPR.

[12] And conversely it creates an obligation for the processor to alter or erase the stored personal data if requested to do so by the data subject.