Blockchain-based consent manager for GDPR compliance

Juan Camilo Vargas[1]

Abstract: The General Data Protection Regulation represents great challenges for companies. This paper proposes a model of consent management for personal data that uses blockchain technology to help address part of these challenges. On the one hand, the model aims to facilitate compliance with the regulation and offer an agile tool for consent control and interaction between data subjects, controllers and processors. On the other hand, it aims to offer data subjects a tool to assert their rights and get bigger control over their consents and indirectly over personal data. A proof of concept was developed using Hyperledger Fabric and allowed to identify the benefits and challenges of the model.

Keywords: GDPR, blockchain, consent, Hyperledger, Personal data economy.

1 Introduction

The General Data Protection Regulation - GDPR - came into force in May 2018. At that time, a significant proportion of companies considered that they were not fully prepared to comply or even had major gaps in compliance with this regulation [WPS18]. GDPR represents great challenges for companies not only from an administrative and legal perspective but also from a technical one, mainly in the areas of data security, data management and automation [Ib18]. The fines for non-compliance can amount to 20 million euros or 4% of the total annual global revenues of the company.

From the point of view of data administration, some solutions are available on the market that seek to help companies comply with regulatory requirements. Some of them focus on the administration of the consent that users must give for the processing of personally identifiable information (PII). Despite the benefits for companies, these solutions have some limitations: they can represent silos of information inside or outside the organization and don't give the user control and full visibility over their PII. Each controller can acquire or implement different mechanisms to handle consents. This creates a practical barrier that does not allow data subjects to easily maintain control over the consents across different organizations or countries. Over time, this represents a loss of control over their personal data, one of the main objectives of this regulation.

On the other hand, from a business perspective, the value of the data market has grown during the last five years at significant rates (9% in 2017) and is expected to surpass the threshold of 60 billion Euro in 2020 [Id18]. However, with the entry into force of GDPR

[1] Fraunhofer IAO, Competence Team Identity Management, Nobelstr. 12, 70569 Stuttgart, vargasjcamilo@gmail.com

many companies face difficulties to monetize personal data that has been consented since purchasing companies do not have agile mechanisms to verify the conditions under which the consents were granted and if they fully comply with the regulation. Lack of trust between companies reduces the growth of personal data market that conforms to regulation.

An alternative model of consent management of personal data is proposed using blockchain technology. As one of the types of distributed ledger technologies, blockchain offers novel security, trust and interaction features that can add value to the consent management model for the processing of personal data. In its most basic form, a blockchain can be described as a database that is decentralized and immutable and that keeps historical records of transactions and digital assets through a peer-to-peer network. The proposed model considers as participants in a blockchain network the three main actors defined in the GPDR: data subjects, data controllers and the data processors. Optionally, the model can allow authorities to be integrated into the network as a fourth participant with limited rights to the supervision of partial information upon request. These actors interact around consent facilitating compliance and accountability by companies in their role as data controllers and data processors and facilitating the exercise of subject's data rights. Additionally, the model can offer two novel advantages: On the one hand, it allows data subjects to easily decide where their data goes and to know where it is and for what purposes and by whom it is processed. It also provides a tool to make subsequent decisions and requests related to it in order to exercise the data rights established in the regulation. On the other hand, the model can be used by new fairer data monetization systems that share revenue with the data subjects according to the data they provide (see examples [HEN18] and [Pi18]).

2 Methods

The concept of the blockchain-based consent manager was conceived as a business network modelled on a permissioned federated blockchain [VK17] under the control of the actors themselves, i.e. under the control of the data subjects, controllers and processors. These are defined within the blockchain network as nodes that not only validate transactions but can also control who has access and can read or write in the ledger. A proof of concept was implemented using the Hyperledger Fabric framework [Hy18A] as it provides adequate tools for agile development on enterprise blockchain solutions. Figure 1 describes the overall vision of the proposed model.

In a normal operation, when a data subject consents the processing of his PII and the data controller collects and stores the data (1), a digital version of the consent is created as an asset and is registered in blockchain (2). This digital consent contains information that includes the categories of data consented, the purposes of processing, the conditions of storage or processing time and the identification of the data controller, joint controllers and processors if they exist. In other words, the consent contains the information that gives form to the privacy policy and terms and conditions of the data controller. For the purposes of the proof of concept, the format of the consent was adopted and modified from the standard proposed by the consent receipt recommendation by the Kantara Initiative [Ka17].

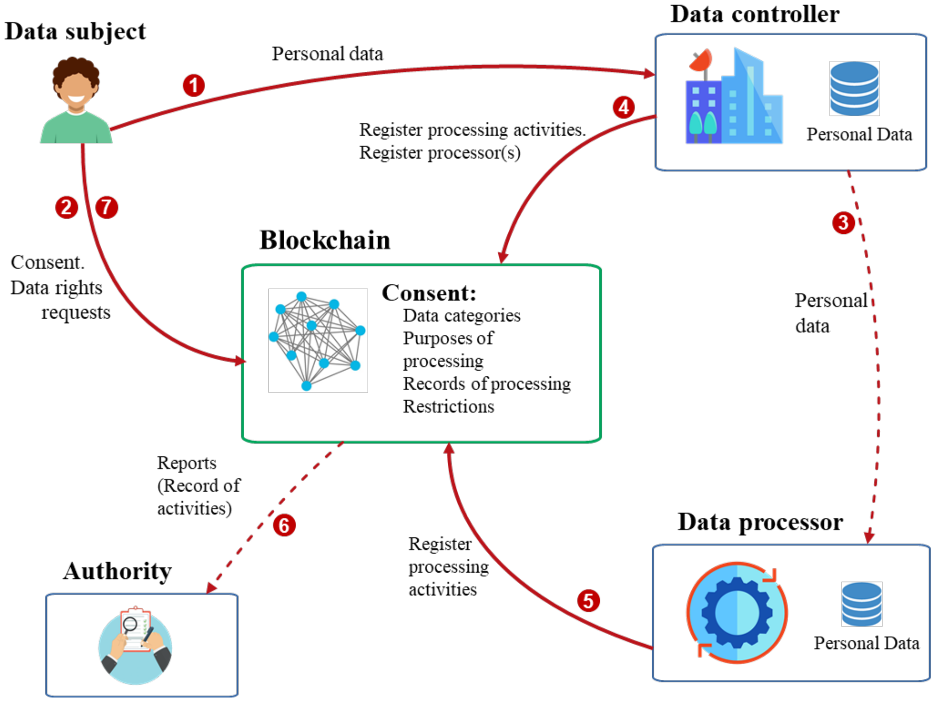

Fig. 1: Blockchain-based consent manager general concept.

Once the consent is created in the blockchain, the personal information of the data subject is stored off-chain, that is, in the data controller's data base. Storing any personal information in a blockchain is not considered as a good practice as the data could not be modified or deleted later which can go against the right of modification and right to be forgotten [CLP18] [Bl18].

When the controller passes personal information to a data processor (3) a new transaction in the blockchain is executed (4). This transaction includes details of data and allowed processing like what data is exactly transferred (data categories), to whom, for what purposes and the period and conditions of processing. In the same way, the processor can register in the blockchain (5) processing activities listed in article 6 of GDPR, e.g. processing for the performance of a contract or passing the information to authorities for the performance of task carried out in the public interest.

Additionally, the data subject is granted access to the blockchain so he can execute two types of activities (7): From one part, he can see the history of transactions related to his consent. That means, he is able not only to access to the conditions that rule the given consent but also he can see the activities the controller and processor(s) have registered in the network in relation to his data. For example, the subject would be able to have a list of the processors that are executing or have executed processing activities on his data and under what conditions as well as their contact data.

From the other hand, the subject can make requests related to his data rights established in the regulation. For example, if the subject considers that one or more processors are carrying processing activities that he considers to be outside the scope of the consent or that he doesn't want to consent anymore, he can request a restriction for processing (Art. 18) or simply withdraw his consent (Art.7). Requests for data erasure (Art.17), correction of data (Art.12) and access to data (Art. 15) were also implemented in the PoC.

From the data controllers and processors' perspective, the network becomes not only a source of immutable information that includes the business rules they have agreed upon and also the registered transactions in relation to specific subjects' data but also a log of processing activities. Thus, the ledger keeps most of the information that these actors must record according to article 30 and matches the models for registering processing activities suggested by the German Conference of Independent Federal and State Data Protection Authorities [Sa18]. Optionally, under request of authorities (Art.30 num.4) controllers and processors could make available for them all or partial information stored in the ledger.

These main activities (2), (4), (5) and (7) represent transactions in the blockchain. These were modelled as chaincode, i.e. in the form of Smart Contracts that are stored in each of the nodes of the network and define the logic of the interaction between its participants.

3 Results

The demonstrator of the concept was used to simulate the consent management process with data from a fictitious group of online stores (data controllers) that requests their customers' personal data (data subjects) for purposes of behaviour analysis on their websites and e-marketing strategies through third parties (data processors). The system made it possible to analyse the applicability of the model as well as some of the challenges facing a possible implementation in a production environment.

The Hyperledger Fabric framework provided usefulness and agility in the creation of the proof of concept in this particular business application. It also provides functionalities such as the creation of channels that allow different companies to participate in the network and still share only part of the information, allowing intra-company collaboration while maintaining privacy.

One of the main challenges identified lies in its integration with the legacy systems of the different organizations. Additionally, a system of association and governance is required to maintain the network and to provide the standardization of information storage formats related to the consents among all participating organizations.

4 Discussion

From the technical point of view, a detailed analysis is required regarding the scalability and performance of the system. The implementation of the concept by a single company does not necessarily need a blockchain implementation [Pe17]. The advantages of the blockchain technology for the enterprise are truly delivered when multiple entities that do not fully trust each other interact within a business network.

Blockchain features allow to create applications that eliminate the need to fully rely on third parties or intermediaries. However, this does not fully apply to the present case. Although there is an immutable record of the activities executed on the data, companies still have the possibility to process or replicate PII without registering such activities on the network, still requiring subjects to give their trust to controllers and processors.

From another point of view, the model can offer advantages to companies for regulatory compliance and can be easily implemented with currently available platforms. However, much of the real value for people lies in the possibility of having this mechanism whenever PII is delivered regardless of which company or in which country. This implies that the general adoption of the concept represents a major challenge. An implementation could be done in public permissioned blockchain platforms so companies of all sizes and from different countries can easily integrate it to their custom systems. For this, a further analysis on the type of blockchain network and the platform to be used is needed. Moreover, the creation of protocols and standards for the storage of consents for the use of personal data like the Consent Receipt Recommendation [KIa17] is imperative to ensure interoperability.

Compared to actual regular operations, this model provides greater transparency to users regarding their personal data. The problem of losing control of personal digital data once it is shared clearly remains. Initiatives such as Self Sovereign Identity and Kantara Initiative are currently looking for solutions to this problem. In addition to offering advantages to companies, this concept is intended to add to these initiatives.

5 Conclusion

The blockchain-based consent model represents an option that provides transparency to the relationship between data subjects, controllers and processors. It is an alternative proposal that can add value to data management in companies and facilitate GDPR compliance. Additionally, it can add value to the data subjects since the concept provides an agile mechanism of visualization and control over PII that is not currently used and that allows them to make informed decisions about their own data.

Although the concept is not a definitive solution to the loss of control over personal data, it is a relatively easy to implement alternative that in turn can offer improvements to the current handling of consents for data processing.

Bibliography

[Bl18] Blockchain Bundesverband: Blockchain, Data Protection, and the GDPR, https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf, 2018.

[CLP18] Compert, C.; Luinetti, M.; Portier, B.: Blockchain and GDPR How blockchain could address five areas associated with GDPR compliance, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=61014461USEN, 2018.

[HEN18] Hawthorne, D.; Engel, Serafin L.; Norta, A.: Blockchain and GDPR. How Blockchain Could Address Five Areas Associated with GDPR Compliance, https://datawallet.com/pdf/datawallet_whitepaper.pdf, accessed 09/10/2018.

[Hy18A] Hyperledger Fabric, https://www.hyperledger.org/projects/fabric, accessed 01/10/2018

[Ib18] IBM: IBM Study: Majority of Businesses View GDPR as Opportunity to Improve Data Privacy and Security, https://www.prnewswire.com/news-releases/ibm-study-majority-of-businesses-view-gdpr-as-opportunity-to-improve-data-privacy-and-security-300649173.html, 2018.

[IdL18] IDC International Data Corporation; Lisbon Council: European Data Market Study. First report on facts and figures, http://datalandscape.eu/sites/default/files/report/EDM_D2.1_1stReport-FactsFigures_revised_21.03.2018.pdf, 2018.

[Ka17] Kantara Initiative Inc.: Consent Receipt Recommendation V1.0 Report, https://kantarainitiative.org/file-downloads/file-download-consent-receipt-recommendation-v1-0-report, 2017

[Pe17] Peck, Morgen E.: Do You Need a Blockchain?, https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain, 2017.

[Pi18] Pickciochain, https://pikciochain.com, accessed 30/09/2018

[Sa18] SACHEN-ANHALT. Hinweise und Muster zum Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DS-GVO, https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/verzeichnis-der-verarbeitungstaetigkeiten-nach-artikel-30-ds-gvo/, accesed 01/11/2018

[VK17] Voshmgir, S.; Kalinov, V.: Blockchain. A beginners Guide, https://blockchainhub.net/blockchain-technology, 2017.

[WPS18] Winton, A.; Ponemon, L.; Schreiber, M.: New Study Highlights Lack of GDPR Preparedness, https://iapp.org/news/a/new-study-highlights-lack-of-gdpr-preparedness, 2018.