A blockchain-based platform for keeping logs of citizens' consents

Marija Popović[1[0000-0002-5789-4055]] and Nikola Tomašević [1[0000-0002-6620-479X]]

[1] Institute Mihajlo Pupin, University of Belgrade, Volgina 15, 11060 Belgrade, Serbia

Abstract. The development of ICTs (Information and Communication Technologies) and the usage of personal data for both research and commercial purposes over the last years have brought the question of the protection of personal data. The GDPR (General Data Protection Regulation) has defined the ways how personal data should be treated, but the application of these requirements still remains an open issue. This paper is dedicated to the research of the blockchain advantages when it comes to providing the transparency of the usage of personal data and provides proof of concept where it demonstrates the application of blockchain in working with users' consents. Hyperledger Fabric was chosen as the development platform which proves as a suitable choice when it comes to achieving transparency, immutability, and modularity.

Keywords: Transparency, Blockchain, Hyperledger Fabric, Consent.

1 Introduction

Due to the faster development of technology and the usage of information systems over the last years, the protection of personal data has become more important than ever. Numerous organizations collect data from citizens for a variety of purposes, both research and commercial. The results of data analysis can have a great impact on society, but on the other hand, citizens should be informed at any moment how their data is collected and processed in order to avoid various data malversations. The emergence of GDPR[1] (General Data Protection Regulation), a legal framework that sets guidelines for the collection and processing of personal data of European Union citizens, has completely changed the way in which personal data of individuals are treated. Nevertheless, the universal mechanisms which ensure that the regulations determined by the GDPR are adequately applied in practice still haven't been established. GDPR demands that data subjects have the right to obtain information from data controllers whether data related to them is being processed but also to have the right to withdraw their consents for using the data at any time [2][3]. Therefore, there is a need for the citizen to keep track of all his consents in order to easily transform the content of consents, and also to have the possibility to completely withdraw his consents. Data controllers also have benefits from keeping their requests for the data transparent as well - so that they can prove that they are using the data according to the previously given consents. GDPR also requires establishing at least one DPA (Data Protection Authority) per each member state territory which will have the responsibility to monitor the processing of personal data. All things considered, there is a need for exploration of the mechanisms that will enable the citizens the establishment of better control over their data, but also to facilitate the process of investigation for central authorities and proving compliance for data controllers. These are one of the goals of the European Horizon 2020 TRAPEZE project [4] which aims to connect all stakeholders in data protection under the one common platform. For providing full transparency TRAPEZE aims to store all processing activities in a decentralized manner, by collecting the data request, consent, and compliance logs. As being an immutable decentralized ledger, blockchain was chosen as the platform for storing the logs.

Blockchain advantages in terms of achieving transparency and immutability and the Hyperledger Fabric as the chosen blockchain platform will be discussed in the next section. After that, the implemented blockchain network for keeping logs of users' consents will be presented and some future work will be addressed.

2 Methodology

Blockchain has received wide recognition upon the occurrence of cryptocurrencies, such as Bitcoin and Ethereum. It was spread later to smart contract techniques, programs that contain a transaction logic needed for updating the state on the ledger and use completely distributed data storage and processing, without the central authority. As the popularity of blockchain grew, it went beyond the scope of usage within cryptocurrencies and found a new field of application in various enterprise use cases. The immutability of blockchain is based on hash cryptography, which ensures that blocks creating a blockchain network cannot be modified or tampered with. Being a distributed ledger, it eliminates a single point of failure which exists in centralized systems and also removes the need for trusting one central authority. Having the aforementioned characteristics, blockchain has proven as a convenient area of research when it comes to establishing transparency and immutability of personal data.

While numerous well-known blockchain platforms are currently being adapted to enterprise use cases, Hyperledger Fabric [5], an open-source platform established under Linux Foundation, is originally designed for these purposes and therefore offers various advantages such as modularity, pluggability, and scalability. Another fact that distincts Hyperledger Fabric from other platforms such as Bitcoin and Ethereum is that it is a permissioned platform which requires all the participants in the network to be identified and while the participants may not fully trust each other, they can be sure that all the entrants are who they claim to be. The modular architecture allows the usage of different structural units depending on the concrete need of the use case. Hyperledger Fabric is also the first platform that supports developing smart contracts in general-purpose languages, such as Java, Go, Node.js, and therefore offers more flexibility for developers who don't have to get acquainted with domain-specific languages.

3 Results and discussion

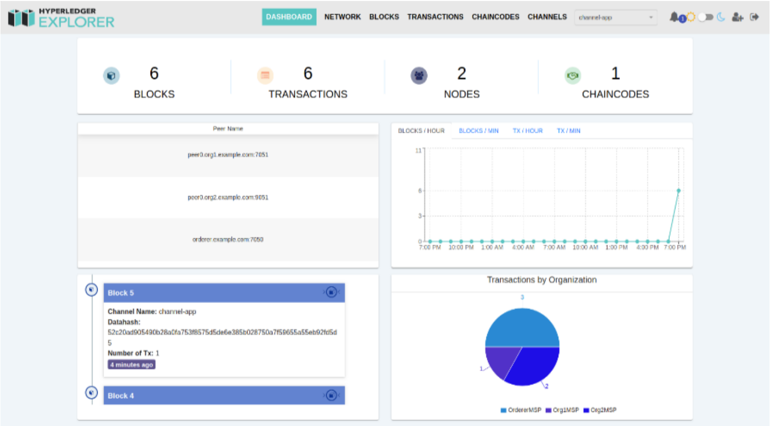
The developed platform consists of a client application and a Hyperledger Fabric network which communicate using the Fabric SDK for Node.js.

3.1 The client application

The client application is implemented in Node.js and has two most important roles: assigning a digital identity to all users who want to participate in the Hyperledger network and sending requests from users to the network. The identity assignment is done between the client application and Certificate Authority, the body that issues digital certificates to different parties. Each user that wants to participate in the network has to go through the registration and enrollment process with Certificate Authority. When these two steps are completed, the user is assigned a digital certificate which is stored in the user's wallet along with his private key. For the purpose of testing the wallet is stored in the file system. However, storages such as databases and hardware security modules should be considered for the deployment. The certificate is sent with each request to the network so that the user can be appropriately identified.

3.2 The Hyperledger Fabric network

As regards the Hyperledger Fabric network, two organizations were created, each one having one peer that form a channel. Peers, smart contracts and certificate authorities run inside docker containers. The smart contract consists of methods that perform basic operations working with users' consents: creating/reading/modifying/deleting a consent, reading all consents, reading a history of consents. The consent contains the following attributes: data subject, creation date, data category, purpose, and recipient. For monitoring the activity on the underlying blockchain network Hyperledger Explorer tool is used, which supports the visualization of the network, blocks, and transactions (Fig. 1).



6 BLOCKS

6 TRANSACTIONS

2 NODES

1 CHAINCODES

Peer Name
peer0.org1.example.com:7051
peer0.org2.example.com:9051
orderer.example.com:7050

Block 5

Channel Name: channel-app
Datahash:
52c20ad905490b28a0fa753f8575d5de6e385b028750a7f59655a55eb92fd5d
5
Number of Tx: 1
4 minutes ago

Block 4

Fig. 1. Hyperledger Explorer visualization of the realized network

The Hyperledger Fabric has proven to be a suitable choice for developing the desired platform because of the advantages for implementing the client application and smart contracts in general-purpose languages, with good support of the Fabric SDK. Furthermore, the modularity of Hyperledger Fabric allows usage of different databases for storing the world state of the platform which has proven useful while implementing this network since the initial approach was to use the LevelDB database, but with the later need for rich queries, it was replaced with the CouchDB. The future work would include testing the performance of the network by using the Hyperledger Caliper, a benchmarking tool provided by Hyperledger community.

Acknowledgment

The research presented in this paper is partly financed by the European Union (H2020 TRAPEZE project, Pr. No: 883464, H2020 LAMBDA Project, Pr. No: 809965), and partly by the Ministry of Education, Science and Technological Development of Republic of Serbia.

References

1. ‘General Data Protection Regulation (GDPR) – Official Legal Text’, *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/, last accessed 2021/05/06.
2. ‘Art. 15 GDPR – Right of access by the data subject’, *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/art-15-gdpr/, last accessed 2021/05/06.
3. ‘Art. 7 GDPR – Conditions for consent’, *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/art-7-gdpr/, last accessed 2021/05/06.
4. ‘TRAPEZE’. https://trapeze-project.eu/, last accessed 2021/05/06.
5. ‘A Blockchain Platform for the Enterprise — hyperledger-fabricdocs master documentation’. https://hyperledger-fabric.readthedocs.io/en/release-2.2/, last accessed 2021/05/06.