Legal Knowledge and Information Systems
S. Villata et al. (Eds.)

doi:10.3233/FAIA200866

Permissioned Blockchains: Towards Privacy Management and Data Regulation Compliance

Paulo Henrique ALVES [a], Isabella Z. FRAJHOF [b], Fernando A. CORREIA [a], Clarisse DE SOUZA [a] and Helio LOPES [a]
[a] *Department of Informatics, PUC-Rio, Brazil*
[b] *Law Department, PUC-Rio, Brazil*

Abstract. Data privacy and protection has been a trending topic in recent years. The COVID 19 pandemic has brought about additional challenges and tensions. For example, sharing health data across several organizations is crucial for significant control and reduction of massive infection and death risks. This implies the need for broadly collecting and using personal and sensitive data, which raises the complexity of data protection and privacy challenges. Permissioned blockchain technology is one way to empower users in controlling how their data flows through the net, in a transparent and secure way, through an immutable, unified, and distributed database ruled by smart contracts. Given this background, we developed a second layer data governance model for permissioned blockchains based on the Governance Analytical Framework principles to be applied in pandemic situations. The model has been designed to organize the relationship between data subjects, data controller, and data processor. Regarding privacy concerns, our proposal complies with the Brazilian General Data Protection Law.

Keywords. privacy, governance, blockchain, regulation, public health

1. Introduction

Data privacy and data protection became one of the most critical concerns in the digital era. In order to regulate how data can be collected and used, many data protection regulations emerged to set rules to organize this environment. These kinds of regulations aims to provide rights and duties for both users and companies, whenever the processing of personal data is taking place. Thus, data protection norms also applies, and are extremely important in this scenario, when the processing of sensitive health data is taking place.

Previous pandemic outbreak experiences like influenza, MERS-CoV, Zika, Ebola[1], and now COVID-19, showed that data sharing between health institutions and other stakeholders worldwide is fundamental to fight against the broad contamination. Moreover, considering the intensive collection of personal data in these scenarios, abiding to

[1] Data Sharing in Public Health Emergencies. Available at: `https://www.glopid-r.org/wp-content/uploads/2019/07/data-sharing-in-public-health-emergencies-yellow-fever-and-ebola.pdf` Accessed at: 10/15/2020.

data protection norms is of the utmost importance [1]. It must be noted that data protection regulations do not forbid the use of personal data in a pandemic scenario, but establishes the rules and legitimate uses that must be observed. Such compliance provides that society can benefit from the uses of such data: it protects individual's privacy and data at the same time as it allows for data utility. In this sense, contact tracing apps [2] are being implemented as a manner to allow public health institutions to track the infection movement and potentially infected people.

Just recently in Brazil, a Data Protection Regulation was enacted (Law n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais – LGPD). Due to Brazilian lack of tradition in this subject, it is important to provide society acculturation and awareness of the importance of protecting personal data in general. Furthermore, such regulation sets rules and obligations that regulates the use of personal data by public and private entities. Thus, in the pandemic scenario, controllers and processors must evaluate which of the legal basis foreseen in law authorizes the collection of users' data. It must be remarked that the LGPD establishes that individual consent is only one of the legal basis authorizing data processing. In any case, data controllers must abide to the law's principles, rights, safeguards and act in good faith. From a technology perspective, data privacy management is challenging. Data must be processed and kept in a safe ruled-base environment, and looks forward to a transparent and secure environment [3].

Therefore, we proposed a second layer of governance in permissioned blockchains solutions, since only the first layer, i.e., platform governance (permissioned or permissionless), is not able to address this challenge. We developed an architecture based on Hyperledger Fabric[2] to instantiate the proposed governance in the COVID-19 pandemic scenario. We base our model on the Governance Analytical Framework (GAF) [4] principles defining the Problem (such as the purpose limitation), Actors (data subject and data controller and processor), Social Norms (regulations), Process (data processor methodologies), and Nodal Points (technology used to connect stakeholders).

2. Related Work

Contact tracing apps are also useful data sources for disease contamination tracking. The DP-3T initiative [5] uses the Bluetooth signal to identify infected people or people who have been in touch with someone who was infected. Such applications are controversial solutions from both privacy and medical viewpoints: not only highlights the infected person but also who has been in touch with him/her and, from the medical perspective, at least 60% of the population should have the app installed in order to such solution be effective. Therefore, to preserve the user's privacy all the data should be anonymized and decentralized. Even though the authors in [6] proposed a blockchain-based application for electronic medical records management, they did no association with any data regulations. Panian [7] argues that companies and government organizations should define standards, policies, and data management processes. The author presents application-centric and process-centric models for data governance. However, those models do not present the concerns related to privacy and data management.

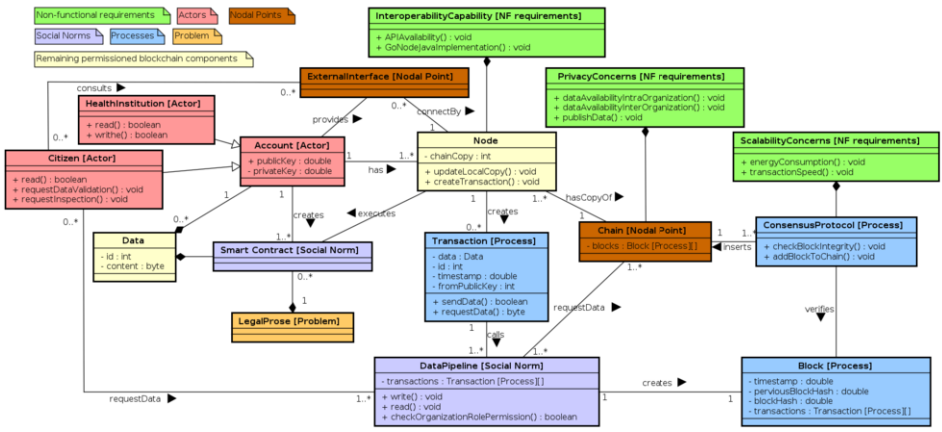
[2]Hyperledger Fabric. Available at: `https://www.hyperledger.org/use/fabric` Accessed at: 10/15/2020

As one could observe, the presented works showed essential concepts and applications regarding personal data collection and management. However, the combination of privacy management, governance model concepts and the usage of blockchain technology application to provide a safe environment for data sharing has not been explored yet. Therefore, our proposal of a second layer data governance for permissioned blockchain cames to offer a complete environment for data sharing and privacy management.

3. Blockchain Data Governance

To model the COVID-19 data governance scenario, we based our approach on the Governance Analytical Framework (GAF) [4]. The GAF is based on five principles: (i) problems, (ii) actors, (ii) social norms, (iv) processes, and (v) nodal points. This framework proposes deconstructing social problems by decomposing them on these five principles and reconstructing them by modeling the governance. This mapping helps people to identify the purpose of limitation accurately by verifying the Problem principle. The actors and norms involved can also be checked, so people are able to trigger, or even suite, the organization that broke any user's rights. Moreover, by checking the processes and nodal points, people can request how they were collected and processed. From the traceability perspective, the contact tracing apps can be modeled by the GAF principles as well.

Figure 1. GAF implementation in a permissioned blockchain architecture.



This mapping should also help health institutions to not only to elaborate explanation regarding which data will be collected, in which scenarios and range, but also to guarantee data anonymization. Permissioned blockchains fit with all the presented concepts for allowing the creation of governance rules to manage entities and data. Figure 1 depicts the GAF definitions applied to this technology. Therefore, such technology can be used to store and share pandemic data, not only as a transparent link between data subjects, data controllers, and processors, but also as a data tracker and data provider to people or any other interested entity. Through permissioned blockchain, data can be audited and used as a data source for research purposes. Self-enforcement Blockchain Smart Contracts (BSC) enhances trust between the data subject and the data controller

and processor. They guarantee: (i) self-execution and adherence of the purpose of the data processing, (ii) the historical information of the source of the collected data, who has accessed the data, thus, with whom such data was shared, and (iii) the timestamp.

Hence, BSC plays a vital role in this environment; it is responsible for roles assignment and can be used as a snapshot of activated norms in a specific moment. It also ensures transparency related to the dataflow. In this sense, differently from the presented literature, the proposed governance, detailed in [8], enables institutions to share data following previously agreed rules. The data provenance is available for citizens, researchers, government, and health institutions, which may improve the identification of data inconsistency worldwide by information comparison.

4. Conclusions

In this paper, we proposed a new data governance for privacy management in the permissioned blockchain platforms applying the GAF principles in the COVID-19 outbreak scenario. The LGPD rules guided our development towards compliance with data protection regulations. This technology is promising to support the data subjects by providing a transparent tool so that data subjects can confirm if their data was processed in accordance with data controllers' privacy policy. Also, permissioned blockchains, besides empowering data subjects, allow data controllers and processors to be accountable for their data processing activities. Like a fingerprint, the timestamp, combined with historical blocks, shall provide resources to reconstruct the data subject concessions over the law evolution. In this sense, this topic should be carefully evaluated to analyze the blockchain capability to be adherent to the legal basis and their advancement. Furthermore, the evaluation of different cryptography methods may contribute to data privacy and protection concerns.

References

[1] Bradford, L. R., Aboy, M., and Liddell, K., "Covid-19 contact tracing apps: A stress test for privacy, the gdpr and data protection regimes," *Journal of Law and the Biosciences*, 2020.

[2] van Kolfschooten, H. and de Ruijter, A., "Covid-19 and privacy in the european union: A legal perspective on contact tracing," *Contemporary Security Policy*, pp. 1–14, 2020.

[3] Karaçam, D. A., "Privacy and monopoly concerns in data-driven transactions.," in *JURIX*, pp. 145–150, 2019.

[4] Hufty, M., "Investigating policy processes: the governance analytical framework (gaf)," *Research for sustainable development: Foundations, experiences, and perspectives*, pp. 403–424, 2011.

[5] Fagherazzi, G., Goetzinger, C., Rashid, M. A., Aguayo, G. A., and Huiart, L., "Digital health strategies to fight covid-19 worldwide: challenges, recommendations, and a call for papers," *Journal of Medical Internet Research*, vol. 22, no. 6, p. e19284, 2020.

[6] Ekblaw, A., Azaria, A., Halamka, J. D., and Lippman, A., "A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data," in *Proceedings of IEEE open & big data conference*, vol. 13, p. 13, 2016.

[7] Panian, Z., "Some practical experiences in data governance," *World Academy of Science, Engineering and Technology*, vol. 62, no. 1, pp. 939–946, 2010.

[8] Alves, P. H., Frajhof, I. Z., Correia, F. A., de Souza, C., and Lopes, H., "Second layer data governance for permissioned blockchains: the privacy management challenge," 2020.