Controlling Personal Data Flow: An Ontology in the COVID-19 Outbreak Using a Permissioned Blockchain

Paulo Henrique Alves[1][a], Isabella Z. Frajhof[2], Fernando A. Correia[1][b], Clarisse de Souza[1][c] and Helio Lopes[1][d]

[1]*Department of Informatics, PUC-Rio, Brazil*

[2]*Law Department, PUC-Rio, Brazil*

{*palves,fjunior,clarisse,lopes*}*@inf.puc-rio.br; isabellazfrajhof@puc-rio.br*

Keywords: Ontology, Privacy, Data Protection, Governance, Blockchain.

Abstract: Data protection regulations emerged to set rights and duties in managing personal data. Hence, they have created a new challenge. Systems must comply with legal obligations whenever the processing of personal data takes place. From the controller's perspective, attending to such norms can be defying, as it demands a detailed and holistic knowledge of the data processing activity. From the data subject point of view, controlling and following the data flow is also complex, as many entities can be authorized to access and use one's personal data. To mitigate information asymmetry and comply with data protection regulations, we developed an ontology to identify the entities involved in personal data processing. The ontology aims to build relationships between them and to share a common understanding of rights and duties proposed by the Brazilian Data Protection Law under the COVID-19 pandemic context. Moreover, the permissioned blockchain technology emerged as a solution to manage privacy concerns and to allow the compliance to such Law. We also developed a conceptual model using such technology and provided a data governance approach to set a standard so that the reuse becomes more accurate.

1 INTRODUCTION

The massive collection of personal data, due to widespread goods and services connected to the internet, turns the discussion of regulating personal data into a high-priority item (Mulholland and Frajhof, 2020). Recently, Brazil enacted its Data Protection Law (Law n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD). Like other Data Protection Regulations, such as the GDPR in the European Union, and the Privacy and Data Protection Act in Australia, the LGPD sets the rules and principles for the processing of personal data environment. It provides rights for data subjects (DS) and establishes duties and responsibilities for data controllers (DCs) and processors (DPs). Protection norms are important when sensitive health data is being processed (Metnitz et al., 2020).

In pandemic scenarios, data sharing and communication among health institutions, public or private, and state entities are vital to the decision-making process. This data is used to define and develop public policies to contain disease spread (Cori et al., 2017). Previous pandemic outbreak experiences like influenza, MERS-CoV, Zika[1], and now Sars-CoV-2 (or COVID-19), demonstrate that data sharing between health institutions and other stakeholders is fundamental to fight against broad contamination.

In Brazil, LGPD. imposes that whenever the processing of personal data takes place, processors and controllers must observe the law's command, such as its principles, processors and controllers duties, individual rights, etc. From the controller perspective, attending to such norms can be defying, as it demands a detailed and holistic knowledge of the data processing activity. From the DS point of view, controlling and following the data flow is also complex, as many entities can be authorized to access and use one's personal

[a] https://orcid.org/0000-0002-0084-9157
[b] https://orcid.org/0000-0003-0394-056X
[c] https://orcid.org/0000-0002-2154-4723
[d] https://orcid.org/0000-0003-4584-1455

[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: 10/21/2020

data. Thus, the DS should be able to know if: the informed purpose of data use is being observed; the personal data has been shared with other non-informed partners; and once the purpose of the DC is reached, if the data is still being used, or shared, with a different purpose.

Answering these questions and providing the required transparency is also challenging from a technology perspective. Blockchain technology emerges as a possible solution to build a unified, distributed and trusted database. The data immutability provided by the consensus mechanisms ensures the unified historical information. Also, the data distribution among the worldwide network participants guarantees high data availability. Finally, permissioned blockchain applications (PBAs) allow personalized data sharing; the DSs are able to set access rules and set which data should be public, private, or accessed under case by case authorization (Velmovitsky et al., 2020).

Given the lack of policies and standards to share pandemic data, and recognizing the importance of sharing such data reliably and safely, we propose an ontology to organize roles, entities, and relationships in favor of users' privacy and data protection.

This paper is structured as follows. Section 2 focuses the data regulation background. Section 3 presents the related works in the current literature regarding pandemic data sharing, ontologies, and PBA governance. Section 4 presents our ontology, which aims to provide a model that would be used by citizens, health organizations and solution architectures to identify the main concerns when personal data is shared. In Section 5 a blockchain data model is proposed to create an environment for controlling personal data flow according to LGPD. In Section 6 we include a data governance framework based on GAF (Governance Analytical Framework) (Hufty, 2011) to improve the COVID-19 scenario definition and applied the governance concepts on a PBA. Section 7 presents conclusions and future perspectives.

2 DATA REGULATION

The constant and intense collection of personal data by a myriad of services and goods, and the pan-optical vigilance exercised over our behaviour when analyzing these collected data, highlights the importance of ensuring ways to protect one's personal data. That is, individuals must be informed about which data is being collected and for what ends, and have control and knowledge about its uses. This reflects the idea of a right to informational self-determination. Such right is put as an evolution in the information society of the classic perspective of a right to privacy as the "right to be let alone" (Rodotà, 2008), put by the U.S. Supreme Court Justices Samuel D. Warren and Louis D. Brandeis (1890). The right to informational self-determination means giving one the power to control the flow of his/her own information, and it is one of LGPD's basis (art. 1, II).

In this sense, we have highlighted four fundamental ideas from the LGPD, which will be applied in the proposed scenario. Firstly, the purpose limitation principle, which imposes that data processing must be legitimate, specific, and explicitly informed to the DS. Secondly, the data minimization principle, which means that only the strictly necessary data shall be used to satisfy the intended and informed purpose (art. 6, III). Thirdly, the law recommends the use of anonymization or pseudonymization techniques as a governance and good practice measure to ensure data security (arts. 12, 13, 46, 6, VII, VIII). Fourth, data processing must happen in a transparent manner, with the disclosure of clear, precise, and easily accessible information related to the data processing (art. 6, VI).

Furthermore, the law establishes different legal basis, beyond consent (arts. 7 and 11), which authorizes the legitimate processing of personal and sensitive data (which includes health data). Regardless of the legal basis used to process data, all DCs and DPs shall comply with the law's principles, DS's rights, and other safeguards (art. 7, § 6).

In pandemic scenarios, data protection norms are of the utmost importance (Bradford et al., 2020; Almeida et al., 2020), especially because of the fundamental right status of data protection right (Mendes and Keller, 2020; Mulholland, 2018). Thus, an ontology definition is necessary to allow a common understanding of rights and duties foreseen in the LGPD. Also, it can mitigate information asymmetry and enhance a right to informational self-determination.

3 RELATED WORK

This section aims to present the works related to: (i) identity management (Lee, 2017), data regulation and blockchain (Truong et al., 2019), blockchain ontology (Tasca et al., 2017; Palmirani et al., 2018), data governance (Alves et al., 2020) and health data management (Ekblaw et al., 2016; Jabbar et al., 2020; da Fonseca Ribeiro and Vasconcelos, 2020).

Lee (2017) presented the Blockchain-based ID as a Service (BIDaaS) for digital identity and authentication management. The proposed architecture is based on Public Key Infrastructure (PKI) for users, companies, and partners, presenting the benefits of using PKI for these system actors. However, identity management under data regulation, such as data protection regulation (e.g. LGPD), was not mentioned. Hence, issues related to consent and the access authorization revocation, for example, were not introduced to guarantee accountability as well. Therefore, in order to improve the PKI and access authorization, we developed a model that also adds a user certificate to set the rules for using personal data, allowing access revocation (as presented in the following sections).

Truong et al. (2019) proposed a design concept for a GDPR-compliant personal data management based on the Hyperledger Fabric (HF) permissioned blockchain. Even though the authors presented a hybrid on-chain and off-chain architecture to empower users to revoke the consent and erase personal data, an ontology to describe the relationships between data regulation, DSs, DCs, and DPs is missing. The paper also limits its analysis on the legal basis of consent and the possibility of revoking it. Hence, given this lack, we proposed a new ontology for PBAs and for other features foreseen in the LGPD (purpose limitation and data minimization principles).

There are blockchain ontologies proposals for different purposes, and two presented an approach towards blockchain technology and data regulation concerns. Firstly, Tasca et al. (2017) proposed a component-based blockchain ontology that approached the main connectors and subcomponents. However, data privacy is a brief topic under the security and privacy theme and lacks in-depth evaluation. Secondly, Palmirani et al. (2018) presented the PrOnto, a GDPR ontology, that provides a legal knowledge modeling based on five modules: (i) data, (ii) actors and roles, (iii) processing, (iv) legal rules, and (v) legal basis. Although the authors presented the modules in detail, the ontology is superficial and only few relationships were explained.

Alves et al. (2020) addressed the privacy's challenges to comply with data regulation in a PBA. The solution classifies the GAF concepts in the COVID-19 pandemic outbreak. However, the authors did not explain how data rectification, for example, would work, and the GAF concepts lack details. In this sense, we first addressed the presented absences and added a certificate in this architecture to deal with data rectification, data access, time limitation for data use, among others. Second, we drove into the GAF concepts to clarify the ontology application on a PBA.

In regards to health management data, Ekblaw et al. (2016) and Jabbar et al. (2020) proposed a Blockchain Smart Contract (BSC) approach for electronic medical records management to deal with the highly regulated health sector. The BSCs allow data sharing in this private P2P network. Even though this solution enables immutable logs, distributed information, and accountability, it has no association with data protection regulations. Furthermore, they developed their application under a public blockchain platform. Thus, some data had to be stored off-chain to preserve data privacy. In this sense, we proposed an entirely PBA that provides resources to comply with data protection and privacy concerns.

Even though (da Fonseca Ribeiro and Vasconcelos, 2020) have proposed a PBA for Electronic Health Records using HF, they did not discuss concerns regarding data regulation. Moreover, the proposed solution lacks data sharing details. Thus, we addressed these absences, offering a conceptual blockchain model solution based on an ontology for data protection and privacy management under LGPD.

In summary, those related works showed the main concerns regarding identity management, data regulation, blockchain, ontology, data governance, and health data management. However, none of them presented a unified solution and approached LGPD – this is the gap we propose to address in our work.

4 ONTOLOGY FOR CONTROLLING DATA FLOW

Ontologies are representations of a specific domain that aims to create a shareable and reusable model. They are also considered a useful instrument for reducing conceptual ambiguities and inconsistencies in a specific domain (Staab and Studer, 2010). In this sense, an ontology proposed for blockchain technology for a specific context, e.g., sharing personal and sensitive data, should also be created. This would allow people to get a complete understanding of the effects of sharing personal data, as well as their rights, under data protection regulations. DSs must know the purpose of data processing, who are the controllers, what are the responsibilities of the DP and DC, how, and if, they can revoke access to their information and limit its use (content and time length of data processing). Disclosing these information is mandatory (art. 9, LGPD). The traceability of the data flow is essential to turn effective the right to informational self-determination, data protection, and privacy.

In order to control the flow of personal data and decrease informational asymmetry, it must be known (i) the data source and content, (ii) who inserted the data, (iii) when the data were added, (iv) whether the data were changed, and (v) the processing purpose. Hence, the ontology development should consider these concerns to correctly represent this environment's needs by providing proof of the data integrity and provenance. Furthermore, to build a complete ontology, the entities involved should also be considered, as well as the possibility of data auditing. Governments, health organizations, researchers, citizens, and media should also be able to consult and check the data.

In this sense, our ontology aims to identify the entities and their relationship for further technological support development and to satisfy the regulation requirements. Figure 1 depicts our proposal for pandemic data management, and we will present the ontology concepts in the sequence.

Citizen is the entity responsible for: (i) query information from the data provider, and third parties who received the shared data, and (ii) request validation regarding data and metadata information, such as who and when the data were added to the database. The *Citizen* entity is also safeguarded by their rights and composed by personal data.

UserRights is the entity that represents what citizens can request, such as the copy of stored and processed data, the restriction of processing, the context usage, data deletion, and data correction, for example.

PersonalData is the entity that represents personal and sensitive data collected according to LGPD legal basis. It also includes a list of data that the user agrees to share, a list of organizations that are able to use such data, and the legal basis. We considered personal data as presented by art. 5, I and II, LGPD[2].

DataController entity can process the citizens' data when authorized by one of the legal basis foreseen in arts. 7 and 11. Thus, *DataController* is composed by *OrganizationDuties* and *UserRights*. [3]

OrganizationDuties is the entity responsible for the Legal Basis application, defining which one is applicable according to the processing context. For example, as stated by LGPD principles and DS' rights, the *DataController* shall respect *DataMinimization*, *PurposeLimitaion*, *DataDeletion* among others, as well as security and data governance concerns. Once *Citizens* share their data, s/he contributes to populate the database on behalf of society. Any society member should be able to consult the anonymized public analysis regarding the pandemic situation, even if s/he did not share his/her data.

InterfaceForConsultation entity is the *DataController* bridge to share data with the *Citizen*. The *DataController* receives the treated information from the *DataProcessor* and discloses data to citizens.

DataProcessor is the entity responsible for processing data strictly in accordance to the *DataController* commands and returning the processed data from the *DataSource* to the *DataController*. The latter can exercise the *DataProcessor* role or delegate to a third party.

AuditingOrg is the entity responsible for auditing the information originated in the *DataSource* and exercising compliance regarding the roles and data addition circumstances, e.g., this entity will evaluate unauthorized data insertion.

DataSource entity represents the database technology. To provide transparency and traceability, it is usually required to check the data provenience. Thus, the database should deliver resources to track data, as well as to provide this information to the *AuditingOrg*.

DataTransparency and ***DataTraceability*** entities represents trackable attributes to provide data transparency and traceability.

Also, according to art. 9, LGPD, the *DataController* must provide some basic information (BI) so that the *Citizen* is able to comprehend the data processing and contact the DC. Thus, the *DataController* must provide information in a straightforward manner, structured in a clear, adequate, and ostensive form, referring to the: (BI-01) specific purpose of the treatment, (BI-02) form and duration of the processing, (BI03) DC identification and contact information, (BI-04) DC and DP obligations, and (BI-05) DS rights (art. 18). This ontology is designed to empower people to check and claim for data privacy and protection, provides knowledge of collective rights (health

[2] Article 5, I: "information relating to an identified or identifiable natural person"; Article 5, II. "Personal data related to racial or ethnic origin, religious conviction, political opinion, membership of a union or organization of a religious, philosophical or political character data, health or sexual data, genetic or biometric data, when associated to a natural person".

[3] Art. 7: (i) user consent; (ii) to attend a legal or regulatory obligation by the DC; (iii) by the public administration, for shared purposes and for the execution of a public policy foreseen in law or other legal instrument; (iv) research, implementing data anonymization, when possible; (v) to attend an agreement requirement involving the DS or by his/her request, (vi) to exercise rights foreseen in judicial, administrative or arbitral procedure, (vii) to protect the life or physical state of the DS; (viii) to provide health safeguard in procedures executed by health professionals; (ix) DCs legitimate interests, and (x) credit protection. Moreover, art. 11 sets the legal basis for processing sensitive personal data, authorizes data processing when based on the following hypothesis: (a) with the user consent; (b) without the user consent in the hypothesis (ii), (iii), (iv), (vi), (vii) foreseen above, and (b.1) to protect one's health, exclusively in procedures performed by healthcare workers, health services or health authority; (b.2) to protect the DS from fraud in identity and authentication registration procedures in electronic systems, preserving DS rights, and except when it is necessary to protect DS's fundamental rights and principles which requires data protection.

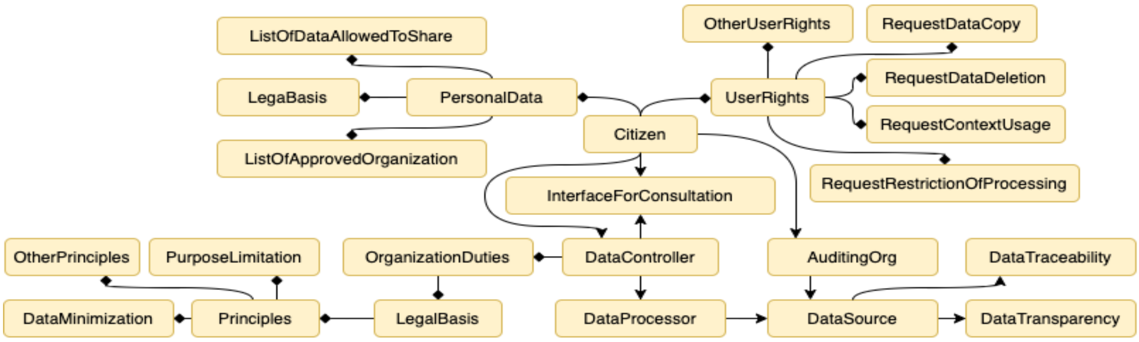

Figure 1: Ontology for Data Privacy Management and LGPD Compliance.

and social rights), and high-quality information. Also, DCs and DPs are able to efficiently provide accountability.

5 BLOCKCHAIN DATA MODEL

Permissioned blockchain platforms are applied when the environment requires privacy concerns related to business secrecy and sensitive data. Such technology can be an entirely private ecosystem or a hybrid environment. The former allows invited entities only to read and write data. The latter enables flexible rules (da Fonseca Ribeiro and Vasconcelos, 2020).

Therefore, health data management solutions have used PBAs to improve transparency and availability and provide better performance than permissionless blockchains (Kuo et al., 2019; Agbo and Mahmoud, 2019; Pongnumkul et al., 2017; Liang et al., 2017). With a restricted number of members (nodes), a new block's acceptance is faster in a permissioned than in a permissionless platform.

Data Registry. As blockchain technology enables immutable registries, the data stored builds the history of transactions, data modifications, access authorizations, and transfer values (tokens), all depending on the parameters stored on the block metadata. This history is important to evaluate if privacy and data protection concerns were respected. Such evidence may present: (i) the conditions in which the data was shared; (ii) to whom it was shared; (iii) until when this authorization is valid, and (iv) when authorization was revoked (when consent is the legal basis).

Authorization Layers. BSCs play a vital role in this environment. As data is immutable when stored in the blockchain, the BSC allows the creation of immutable contract rules specified in a programming language. Also, such technology enables users and stakeholders to get a snapshot of the environment. For instance, in a pandemic scenario, the DC and DP are able to use anonymized (or pseudonymized) sensitive data to create reports and public health actions to control the outbreak spread.

Depending on the selected platform, the blockchain technology may enable the creation of specific channels to share data privately, even when there are other network participants' presence. This enables two main features: the DS can share his/her data with distinct DCs and DPs, and the DSs are able to select which sensitive data to share. For instance, the DS can share their data with a specific research organization selecting only one certain comorbidity instead of the entire health history.

Privacy x Immutability x Revocation. One of the issues regarding blockchain technology applications when dealing with sensitive and personal data is the trade-off between immutable registries and the rights foreseen in the LGPD . Immutability guarantees the BSC conditions under which the data was processed. However, if consent is used as the legal basis, for instance, DSs can request the revocation of her/his consent regarding the usage of his/her data (art. 8, § 5). This can be challenging in this environment. Furthermore, when another legal basis is used to justify data processing, DSs have the right to object if the LGPD is not respected (art. 18, § 2). Once the DS authorizes a DC and DP to use their blockchain data, it cannot be undone by the technology.

In order to work around this issue, the usage of authorization certificates allows the DS and the DC to set expiration date, the purpose limitation, and inform which DC and DP can access the DS's data. Also, the DS and the DC can issue as many certificates as they need, including the revocation certificates when applied. Moreover, the usage of authorization certification in addition to the symmetric cryptography algorithm, such as PKI, as depicted in Figure 2, empower DSs. They are able to issue their certificates individually for each one of the DCs and DPs. Also, the DC can issue a certificate to make the DS aware of the usage of his/her data.

Furthermore, the discussion of data storage archi-

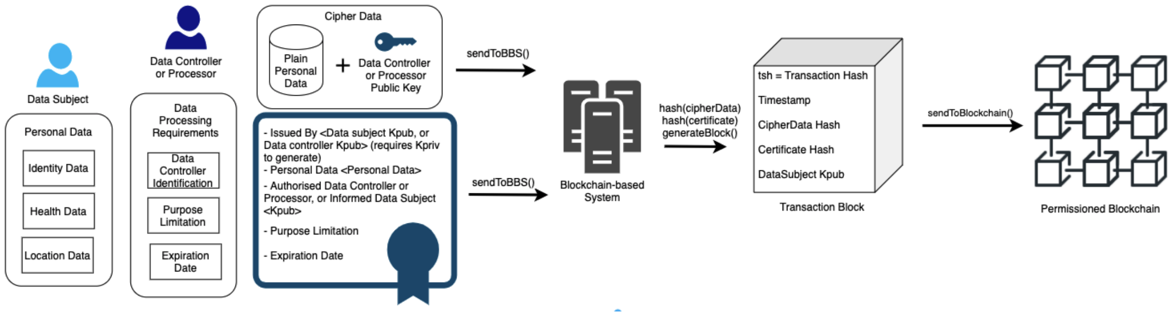

Figure 2: Blockchain conceptual model for data sharing.

tectures plays a vital role in maintaining data private and facilitating the exercise of DS's rights. In blockchain solutions, data can be stored in different ways: plain text, hashed, a link for external storage, and so on. Thus, depending on the solution's design and the complement of other computing concepts, immutability can be used in favor of the DSs. Moreover, the blockchain platform's data storage architecture and the BSC design are paramount to define the proper software architecture and data structure.

Blockchain model for data sharing. We developed a conceptual model for blockchain data sharing to empower users to manage: (i) which data should be shared; (ii) whom should have access; (iii) for how long, and (iv) controlling the purpose of data usage. This model goes towards compliance with the five BI that the DC must provide to the DS (art. 9, LGPD).

Furthermore, PKI enables the DS to share his/her data with a specific DC. First, the personal data, encrypted by the DC and DP public key, generates a cipher data and only allows the private key owner to decrypt the shared data. Second, the DS shall issue the authorization certificate using his/her private key informing: (1) his/her public key, for further localization on the blockchain; (2) the hashed data; (3) the authorized DC and DP public key; (4) the purpose, and (5) the expiration date. These two artifacts - cipher data and the DS issued certificate - are sent to the blockchain-based system. This system sends to the blockchain the hash of the cipher data and the hash of the certificate. The hash comparison guarantees that the information evaluated is the same as the original.

In summary, the block generated is composed of the transaction hash, the timestamp - both generated by the blockchain -, cipher data hash, certificate hash, and the DS public key. Thus, the DC which access the DS shared information shall inform the original authorization certificate issued by the DS and the transaction hash. Next, the blockchain-based system will check if those information are compatible with the one stored on the blockchain. The verification is composed of three steps: (i) certificate expiration date and the DS, DC, and DP public key; (ii) the transaction hash must be present on the blockchain, and (iii) the presented certificate hash is the same as the one stored in this block. If all the verification steps are positive, the blockchain-based system (BBS) sends the DS cipher data to the requester. Thus, the requester is able to decipher the cipher data using his/her private key.

6 COVID-19 BLOCKCHAIN DATA GOVERNANCE

In general, the data governance concept is related to big companies and how they manage a high volume of data. Also, data management is crucial to the interaction and decision-making between parties that have to solve a mutual problem. Even though the World Health Organization (WHO) publicly disclosed COVID-19 data, the transparency and traceability concepts were not respected. It is not possible to access who inserted the data, whether the data was properly anonymized, and what was the legal basis that authorized the processing, for example. Moreover, centralized platforms are subject to data unavailability due to internet connection or hacker attacks[4]. In a pandemic outbreak, data unavailability is especially worrying and may present severe consequences in controlling and managing the disease spread.

Many authors discuss the challenges and opportunities in the pandemic scenario, highlighting the importance of data governance and quality (Almeida et al., 2020; Shaw et al., 2020; Janssen and van der Voort, 2020). They argue that information quality depends on excellent data: management, standardization, and availability. Furthermore, GAF is another

[4] Hackers put Brazilian government on alert. Available at: https://brazilian.report/tech/2020/11/05/massive-hackers-attack-brazilian-government-on-alert/ Accessed on: 11/12/2020.

well-known approach and it is based on five principles: (i) problems, (ii) actors, (ii) social norms, (iv) processes, and (v) nodal points. This framework proposes the construction of a scenario by describing the social problems into those five principles to model the governance. Thus, this approach was used to model the COVID-19 data governance scenario.

Moreover, we chose the HF platform to support the developed blockchain model, based on the presented ontology. PBA fits with the ontology concepts. It allows for the creation of governance rules to manage entities and data, i.e., this technology enables DSs to have their rights respected, or at least have resources to request them.

As mentioned in Section 5, blockchain provides transparency, traceability, data immutability, and availability, by definition. Moreover, PBA adds a role layer that allows data management between selected entities. In this sense, such technology can be used to store and share pandemic data, not only as a transparent link between DSs, DCs and DPs, but also as a data tracker and provider to third parties. Also, PBA allows data auditing and can be used as a data source for research purposes. Self-enforcement BSCs enhance trust between the DS and the DC and DP.

Therefore, BSCs play an indispensable role; they are responsible for roles assignment and can be used as a snapshot of activated norms. They are also crucial for feeding data on the blockchain. We have used the same GAF permissioned blockchain architecture proposed in (Alves et al., 2020). It is also based on HF, as applied by Alketbi et al. (2020). Hence, we have used the following GAF principles: **Actors** are represented by HealthInstitution, i.e., the DC and/or DP; and Citizen (DS). The HealthInstitution may process data or delegate this to a third party. Such actor is also responsible for providing its identification (public key), the purpose of processing and expiration access date for each data request. **Nodal points.** are represented by BBS and Chain, which interacts directly, or indirectly, with HealthInstitutions and Citizens. They are data access points: BBS can apply graphical analysis, and the Chain is the blockchain. **Social Norms.** are represented by Certificate, BSCs, and DataPipeline. These entities set up and verify the rights to access and write data, which will define the conditions that the data would be accessed. Also, BSCs allow citizens to check the collected data and confirm, for example, the compliance to data minimization principle. **Processes** are represented by Transaction, Block, and ConsensusProtocol entities, which manage data in order to check the primary attributes; they are used to create the link between the blocks. **Problem** is represented by the LegalProse, which is used to describe the scenario in abstraction level in plain text on the BSCs. It also specifies the organization's duties and user rights.

Thus, a PBA structured under GAF allows data governance to deal with data accountability and trustworthy data sharing in pandemic situations. According to the access rules established on the permissioned blockchain, data available to public consultation allows governments to provide fast response in a pandemic outbreak. Furthermore, unified governance will enable institutions to share data following previously agreed rules. Data provenance is available for citizens, researchers, government, and health institutions, which may improve the identification of data inconsistency worldwide by information comparison.

7 CONCLUSIONS

In this paper, we presented the ontology that we have designed to aid DSs, DCs and DPs, to enhance some of the LGPD provisions. We also discussed a conceptual model for data sharing based on a permissioned blockchain. This was improved by the use of PKI and digital certificates that provide resources to grant, check, delete, correct, or revoke (when applicable) personal data. Finally, we developed an architecture based on GAF concepts and HF in the COVID-19 outbreak scenario.

However, other limitations should be considered. As there is a vast literature regarding cryptography, our discussion may lack an in-depth analysis of this topic. Moreover, blockchain interoperability is another topic often discussed, and this may affect our architecture directly. Nonetheless, there is no established agreement regarding models and connectors to interoperate in blockchain systems; the usual solution is developing an Application Programming Interface (API) for each platform.

In addition, the architecture designers should also consider the different blockchains' performance, i.e., the number of transactions per second, before defining the most suitable platform. There are many other permissioned platforms, and they perform differently. We chose HF because it is an open-source project, with many literature reviews.

Furthermore, we have discussed the only thr LGPD. Thus, this approach could be adapted for other data regulation scenarios. Therefore, the presented limitations will be treated as the roadmap for future works in order to improve the current approach.

Finally, other important future work is related to an empirical analysis of the proposed ontology. We decided to intensely discuss the ontology, governance, entities, attributes, and relationships before starting the next step: the qualitative evaluation.

REFERENCES

Agbo, C. C. and Mahmoud, Q. H. (2019). Comparison of blockchain frameworks for healthcare applications. *Internet Technology Letters*, 2(5):e122.

Alketbi, A., Nasir, Q., and Talib, M. A. (2020). Novel blockchain reference model for government services: Dubai government case study. *International Journal of System Assurance Engineering and Management*, pages 1–22.

Almeida, B. d. A., Doneda, D., Ichihara, M. Y., Barral-Netto, M., Matta, G. C., Rabello, E. T., Gouveia, F. C., and Barreto, M. (2020). Personal data usage and privacy considerations in the covid-19 global pandemic. *Ciência & Saúde Coletiva*, 25:2487–2492.

Alves, P. H., Frajhof, I. Z., Correia, F. A., de Souza, C., and Lopes, H. (2020). Permissioned blockchains: Towards privacy management and data regulation compliance. In *Legal Knowledge and Information Systems - Volume 334: JURIX*, pages 211–214. IOS Press.

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

Cori, A., Donnelly, C. A., Dorigatti, I., Ferguson, N. M., Fraser, C., Garske, T., Jombart, T., Nedjati-Gilani, G., Nouvellet, P., Riley, S., Van Kerkhove, M. D., Mills, H. L., and Blake, I. M. (2017). Key data for outbreak evaluation: Building on the ebola experience. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 372(1721).

da Fonseca Ribeiro, M. I. and Vasconcelos, A. (2020). Medblock: Using blockchain in health healthcare application based on blockchain and smart contracts. In *ICEIS (1)*, pages 156–164.

Ekblaw, A., Azaria, A., Halamka, J. D., and Lippman, A. (2016). 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*, volume 13, page 13.

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

Jabbar, R., Krichen, M., Fetais, N., and Barkaoui, K. (2020). Adopting formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system. In *ICEIS*, pages 261–268.

Janssen, M. and van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the covid-19 pandemic. *International Journal of Information Management*, 55:102180.

Kuo, T.-T., Zavaleta Rojas, H., and Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. *Journal of the American Medical Informatics Association*, 26(5):462–478.

Lee, J.-H. (2017). Bidaas: Blockchain based id as a service. *IEEE Access*, 6:2274–2278.

Liang, X., Zhao, J., Shetty, S., Liu, J., and Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, pages 1–5. IEEE.

Mendes, L. S. and Keller, C. I. (2020). A new milestone for data protection in Brazil.

Metnitz, P. G., Zajic, P., and Rhodes, A. (2020). The general data protection regulation and its effect on epidemiological and observational research. *The Lancet Respiratory Medicine*, 8(1):23–24.

Mulholland, C. and Frajhof, I. Z. (2020). *A LGPD e o novo marco normativo no Brasil.* Arquipelago, 1st edition.

Mulholland, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, 19(3):159–180.

Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., and Robaldo, L. (2018). Pronto: Privacy ontology for legal reasoning. In *International Conference on Electronic Government and the Information Systems Perspective*, pages 139–152. Springer.

Pongnumkul, S., Siripanpornchana, C., and Thajchayapong, S. (2017). Performance analysis of private blockchain platforms in varying workloads. In *2017 26th International Conference on Computer Communication and Networks*, pages 1–6. IEEE.

Rodotà, S. (2008). A vida na sociedade da vigilância: a privacidade hoje. Renovar, Rio de Janeiro.

Shaw, R., Kim, Y.-k., and Hua, J. (2020). Governance, technology and citizen behavior in pandemic: Lessons from covid-19 in east asia. *Progress in disaster science*, page 100090.

Staab, S. and Studer, R. (2010). *Handbook on ontologies*. Springer Science & Business Media.

Tasca, P., Thanabalasingham, T., and Tessone, C. J. (2017). Ontology of blockchain technologies. principles of identification and classification. *SSRN Electronic Journal*, 10.

Truong, N. B., Sun, K., Lee, G. M., and Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 15:1746–1761.

Velmovitsky, P. E., Souza, P. A. D. S. E., Vaillancourt, H., Donovska, T., Teague, J., Morita, P. P., et al. (2020). A blockchain-based consent platform for active assisted living: Modeling study and conceptual framework. *Journal of Medical Internet Research*, 22(12):e20832.

Warren, S. D. and Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, pages 193–220.