Toward a GDPR Compliant Blockchain Governance Framework

Hasan Mahmud[1], A. K. M. Najmul Islam[1], Bilal Naqvi[1], and Matti Mäntymäki[2(✉)]

[1] LUT University, 53850 Lappeenranta, Finland
{hasan.mahmud,najmul.islam,syed.naqvi}@lut.fi
[2] Turku School of Economics, University of Turku, 20014 Turku, Finland
matti.mantymaki@utu.fi

Abstract. Recent research has highlighted multiple incompatibilities between blockchain technology and the General Data Protection Regulation (GDPR) regarding data controller and data deletion. Such incompatibilities impede the adoption of blockchain technology on a larger scale. This paper aims to resolve these incompatibilities, exploring the issues that need to be considered while developing a GDPR compliant blockchain governance framework. We collected data using 20 semi-structured interviews and discussions from 18 different IT companies involved in blockchain-based service development. We analyzed the data using the Gioia approach. We identified three major governance dimensions that must be considered for GDPR compliant blockchain services, namely community, blockchain protocol, and compliance; each of which has several sub-dimensions. Our study extends prior governance frameworks, suggesting the guidelines to comply with GDPR requirements. This guidelines might help organizations to build a GDPR compliant blockchain business model. Based on our findings, we also put forward directions for future inquiry.

Keywords: Blockchain · Blockchain governance · Compliance · GDPR · Off-chain storage

1 Introduction

Blockchain, a distributed ledger technology, allows participants of the network who may or may not trust each other to agree on a decision without the intervention of any central authority [1, 2]. The inherent features of blockchain technology such as immutability, removal of middlemen, decentralized decision-making, and anonymity [2, 3] have allured many organizations around the world to adopt and experiment with blockchain, paving the way for the emergence of the blockchain economy [2]. Later, the development of smart contracts, algorithms that run automatically without risk of downtime, censorship, or fraud, following the rules enacted in the contract, has further facilitated the adoption of blockchain across different industries [2]. Despite the increasing public

© IFIP International Federation for Information Processing 2022
Published by Springer Nature Switzerland AG 2022
S. Papagiannidis et al. (Eds.): I3E 2022, LNCS 13454, pp. 471–484, 2022.
https://doi.org/10.1007/978-3-031-15342-6_36

interest and technological developments, governance of business and industry applications of blockchain is not well understood [2]. Prior research suggests that the lack of an appropriate governance model is challenging the widespread adoption of blockchain technology [4, 5].

The General Data Protection Regulation (GDPR) has a significant impact on blockchain implementation. The implementation of the GDPR has raised several tensions regarding security, privacy, and the protection of personal data related to blockchain technology [5]. Among these, two overarching factors identified by the European Parliamentary Research Service (EPRS) are as follows.

- There shall be at least one central data controller who is responsible for ensuring data integrity and compliance with the GDPR [6]. GDPR requires data controllers and processors to obtain unambiguous consent of data subjects for their data to be processed [7]. This provides data subjects a right to know about what data is being collected and for what purposes. This also obligates data controllers and processors to remove the data that are no longer relevant [7]. It renders full control of data back to the data owners [8]. On the contrary, blockchain is a decentralized platform having no central data controller. Therefore, there is a lack of consensus among the practitioners and scholars of blockchain regarding who should be considered data controller or owner [6].
- Data must be modified or deleted when necessary [6]. Contrary to this, due to immutability by design, blockchain is an append-only ledger to which data can only be added. Deletion or removal of data from the blockchain is contradictory to blockchain design principles [6].

These two tensions play a critical role in the widespread adoption of blockchain. Organizations are struggling to find way(s) to design blockchain-based services, and to comply with these regulations. However, given the pervasive impacts of these tensions, scholars have attempted to suggest several approaches to tackle them. For example, to resolve the paradox of the data controller, scholars suggest defining participating nodes as controllers [9], miners as processors [10], joint controllers for federated blockchain [11], and developers as processors for smart contracts [12]. Similarly, to overcome the tension between data deletion and modification, scholars identified three methods [13]. First, storing personal data off-chain, storing a hash of personal data in the blockchain, and finally creating a link between them. Second, define a consensus mechanism to delete blocks. Third, using smart contracts to revoke access. Although scholars suggest a few techniques to comply with the GDPR requirements, they did not provide any guidelines on what needs to be considered while implementing these techniques. Thus, existing literature lacks GDPR compliant blockchain governance framework. Furthermore, our literature review indicates that there are few empirical studies on how organizations are adapting GDPR requirements with their blockchain design [14]. As such, blockchain governance frameworks suggested in existing literature [1, 2, 5, 15] fundamentally ignore the necessity of a separate governance framework to tackle the unique requirements of GDPR.

Therefore, this paper is guided by the research question (RQ): *What are the issues organizations must consider while developing a GDPR compliant blockchain governance framework?* To answer the above RQ, we conducted 20 semi-structured interviews among 18 different IT companies operating in Finland. After analyzing the interview data, we identified three main dimensions that the organizations must consider when developing the GDPR compliant governance framework: community, protocol, and compliance. The community comprises various issues related to stakeholders, communication, development, and decision rights. The protocol comprises issues related to consensus algorithms, incentives, and off-chain storage. Finally, compliance includes issues related to roles and responsibilities, accountability, and data collection and consent management. With these findings, we contribute to the existing literature on blockchain governance [1, 2, 5, 15] by including GDPR requirements.

The rest of the paper is organized as follows. Section 2 describes the background on blockchain and blockchain governance. Section 3 presents our research method whereas Sect. 4 discusses the identified dimensions and sub-dimensions that a GDPR compliant blockchain governance framework should consider. Section 5 illustrates the theoretical and practical implications. Finally, Sect. 6 concludes the paper.

2 Blockchain Governance

Blockchain governance refers to "the means of achieving the direction, control, and coordination of stakeholders within the context of a given blockchain project to which they jointly contribute" [1]. Research demonstrates that despite widespread interest in blockchain among researchers and practitioners, the adoption of blockchain is thwarted by the lack of governance models [5, 16]. Therefore, recently researchers have begun to develop blockchain governance frameworks, identifying different facets of blockchain and borrowing themes from different disciplines such as IT, management, and social science [5]. For example, Beck et al. [2] proposed a blockchain governance framework identifying themes from the Information Technology (IT) governance framework. They identified three dimensions of blockchain governance: decision rights, accountability, and incentives. Decision rights concern the generation and implementation of decision proposals, as well as the ratification and monitoring of decisions [2]. Accountability refers to which degree actors are responsible for their actions and decisions. Finally, incentives entail what motivates stakeholders to behave responsibly.

Again, observing the multitude of similarities between blockchain and Open-source Software (OSS), Pelt et al. [1] proposed a blockchain framework governance invoking OSS literature. They identified six dimensions of blockchain governance: (i) f*ormation and context* highlight the relevant background information (purpose, license) of blockchain (ii) *roles* define the roles of stakeholders in different layers (iii) *incentives* capture the motivational factors (iv) *membership* denotes the participation and management of the membership (v) *communication* focuses on the different formal and informal way of communication between stakeholders (vi) *decision making* describes how decisions are made, monitored, and controlled. Additionally, they discussed all these dimensions from the perspective of three layers: (i) *Off-chain community* includes a wider community of a blockchain, and governance mechanism focuses on the ties

of the community (ii) *Off-chain development* includes the governance of the software development process and the protocol maintenance (iii) *On-chain protocol* consists of all the governance mechanisms taking place in the blockchain. For example, the decision-making process, consensus protocol, and rules of interaction. Furthermore, utilizing the concept from social science, Tan et al. [5] categorized nine blockchain governance decisions into three groups: (i) *micro-level* focuses on blockchain infrastructure, modularity, and standards in building, upgrading, and adoption of the blockchain. Micro-level governance defines infrastructure and application architecture and interoperability (ii) *Meso-level* deals with the governance of collective decision-making and actions. It includes the mechanisms related to decision-making, incentive, and consensus (iii) *Macro-level* governance concerns the rules and norms that are specific to a particular constitution, culture, history, and legal foundations. The decision domain consists of the organization of governance, accountability of governance, and control of governance.

However, though it is clear that there are some studies on blockchain governance, research on GDPR compliant blockchain governance is still lacking. In this current study, considering the multiple tensions between blockchain and GDPR and based on the different existing blockchain governance frameworks, we propose some issues/agendas for developing a blockchain governance framework that is GDPR compliant.

3 Research Method

3.1 Data Collection

We collected data using 20 semi-structured interviews and discussions from 18 different IT companies in Finland. All these companies were running blockchain-related projects when we conducted these interviews. The interviews had three major themes: 1) the importance of blockchain for the companies, 2) challenges the companies face with blockchain-based solutions, and 3) the GDPR-related specific challenges they face and how do they comply with the GDPR requirements. The interviewees had diverse backgrounds not just limited to technical but included interviewees from business and legal domains. The major roles of the interviewees include CEO, CTO, head of research, software developer, service designer, and legal expert. The interviews lasted approximately one hour on average. Due ethical concerns were considered including seeking permission from the interviewees. Notes were also taken during the interviews.

3.2 Data Analysis

We used the Gioia method [17] to analyze the interview data. In typical inductive research, data collection and analysis processes are partially overlapped. This was also the case in our study. However, certain steps can be recognized in our data analysis process, which we discuss next. There were three stages in our analysis. In the first stage, we went through the interview data several times and assigned codes to describe different segments of the content. Table 1 shows the codes that were generated at this stage with the associated quotes from the data. In the second stage, we categorized the related codes to develop more abstract concepts, which are also known as second-order

Table 1. Key concepts and associated codes with examples

2nd order Concept	Example code/1st order concept	Example quotes
Many stakeholders in a blockchain system	Developers, smart contract developers, validators or miners, investors, and end-users	"Blockchain-based systems can have various entities. For example, if you think about blockchain-based healthcare data storage, different branches of hospitals, patients and doctors can be part of the networked system." "Well, the participants in any blockchain-based system differ in different domains."
Communication is the key to further development	Online discussion forums, offline events, formal and informal interactions	"We understand that frequent communication is important for the community. We will arrange regular workshops and events so that everyone can be up to date." "Informal interactions can happen in different blogs and forums as well. The community members can start a discussion using the facility."
Development ideas are described in the community	Development team, anyone can propose ideas	"Any stakeholder can propose ideas for development. Then it is agreed within the community." "A process needs to be in place in deciding which development ideas to be implemented."
Decision rights belong to key stakeholders	Core developers or lead developers, the data subject, miners, validators	"The data belong to the data subject. They should be able to decide what to do with it." "The validators can be the participating organizations in the network. They can manage necessary decision making inside the network."

(*continued*)

Table 1. (*continued*)

2nd order Concept	Example code/1st order concept	Example quotes
Data validation happens using consensus algorithms	PoW, PoS, PoA, PBFT, or any combination	"When a data is entered into the block, the validation happens with consensus algorithm." "Well, there are different consensus algorithms, and a blockchain can have combinations of multiple for validating the data."
Incentives are needed for the stakeholder's	Validators or miners need incentives	"We can use reputation allocation for the participants." "The participants who have validated most blocks are rated as honest validators"
Off-chain storage for GDPR compliance	Off-chain data can be removed or updated when necessary	"We store the personally identifiable information and other types of metadata in the off-chain. Hash and signature of the metadata are stored in the on-chain." "Managing the access rights in off-chain is important. We have used traditional storage like access mechanism for the off-chain."
Roles and responsibilities in accordance with GDPR	Data controller, processor, data protection officer	"Data controller can be the experts from the company who understands the data and how it can be used." "Though we have not yet decided who can be the data processors, it is certainly needed in blockchain-based organizations."

(*continued*)

Table 1. (*continued*)

2nd order Concept	Example code/1st order concept	Example quotes
Accountability in accordance with GDPR	The data controller makes sure that GDPR requirements are fulfilled	"We use smart contact to validate the data controllers' roles and any data loss." "As a financial aid institution, we use a blockchain-based system so that the money spent and where it's coming from is transparent. The responsible person can be easily identified in case of any problem arises." "If the data management lifecycle and data collection volume is lower, the accountability is easier to manage. Hence, we have taken the approach of less data collection to avoid the case of accountability."
Data Collection and Consent Management	The organization collects user data and consent as well	"We will try to collect as minimal data as possible. Data that is not related to our work, we don't collect that." "We only collect purposeful data." "The consents are stored in the archive until the user revokes it."

concepts. Finally, in the third stage, we aggregated the second-order concepts into three broader themes or dimensions: community, blockchain protocol, and compliance toward building a GDPR compliant blockchain governance framework. The derived dimensions along their corresponding sub-dimensions have been depicted in Fig. 1.

4 Towards a GDPR Compliant Blockchain Governance Framework

Our interview data revealed several sub-dimensions, which we grouped under three main dimensions as presented in Fig. 1. Next, we elaborate on these dimensions.

4.1 Community

The decentralized nature of the blockchain system is characterized as a community of various interest groups. To manage and coordinate this entire community toward a

common goal, it is important to have a governance mechanism that defines the roles of different stakeholders, their ways of communication, shared development ideas and implementation responsibilities, and the authority and rights to make the decisions. Lacking any proper governance system may jeopardize the success of the blockchain ecosystem.

Our data analysis revealed that a blockchain ecosystem consists of various actors such as blockchain developers, smart contract developers, data controllers, validators or miners, investors, and end-users. Stakeholders possess a substantial influence on the functioning of the system and, at the same time, they are affected by it [18]. This is because the stakeholders shape the blockchain protocol rules and once the rules are implemented, the blockchain protocol shapes stakeholders' activities [19]. Therefore, a

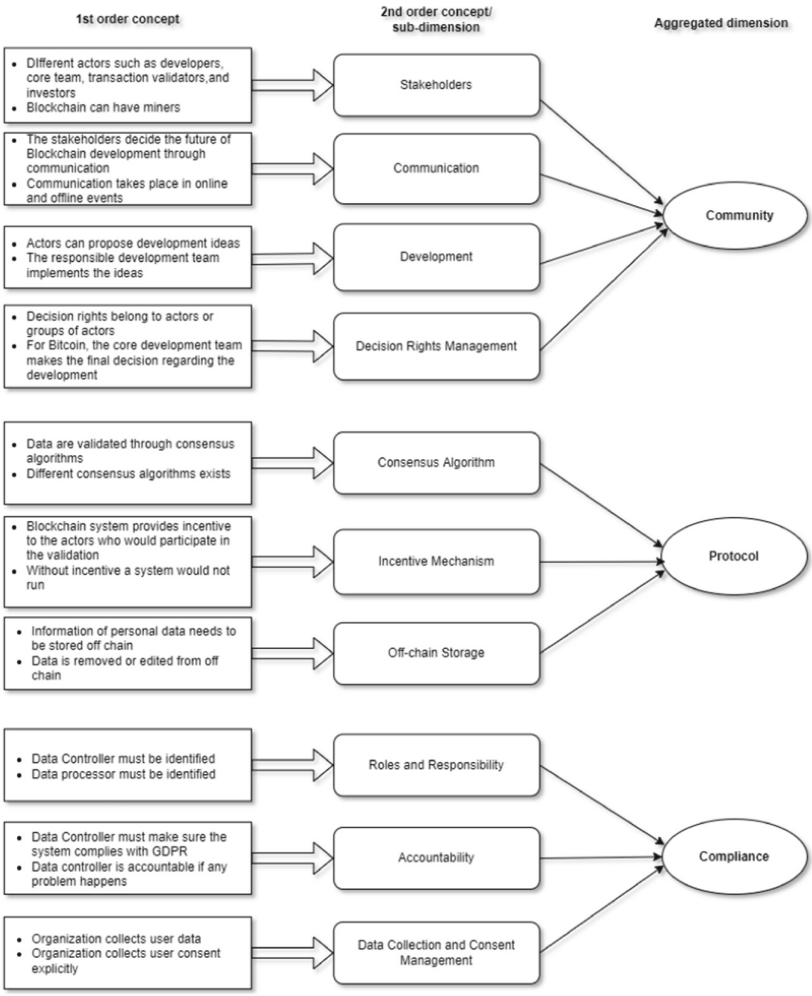

Fig. 1. GDPR compliant blockchain governance dimensions and sub-dimensions

blockchain governance framework needs to highlight the definitions of all stakeholders, their inclusion criteria, their roles and responsibilities, and their modus operandi. One of the challenges concerning stakeholders is the data portability that is possessed by different participants of distributed systems. So, it is also important to have guidelines about the information creation, sharing, and availability outside the blockchain (even before its creation) in the governance model.

After defining the stakeholders, it is important to set rules and norms to be followed by the stakeholders while communicating in the community. The governance framework may include the tools to be used for discussions related to community or development, how the discussion will be coordinated, and how to reach an agreement about the discussion [1]. Again, in the community, especially the open-source community, any actor can propose development ideas. It is unlikely that all ideas are implementable. Therefore, there is a need for a mechanism to choose the best idea to be implemented. Besides, regular maintenance and updates are required for the smooth functioning of the system. Regular monitoring also helps to identify potential threats, which in turn helps to ensure the safety of the system. As such, monitoring and maintenance should come under the purview of the governance framework.

Finally, decision-making rights should be entrusted to a particular actor or group of actors. Blockchain governance is the placement and enactment of decision rights [20]. It includes a set of officially granted rights and obligations to make decisions, give orders, and take certain actions independently in the system [2]. The governance framework should highlight how decisions are made, implemented, and controlled. Some of the key decision areas to be included are the voting mechanism, consensus mechanism, personal data protection, dispute resolution, and the development of the blockchain network.

4.2 Protocol

The protocol specifies the rules and regulations for managing the blockchain network. Our interview data revealed three sub-dimensions of the protocol that needs to be considered in the blockchain governance framework: consensus algorithms, incentive mechanisms, and off-chain storage. Consensus algorithms are used to validate data and add the data to the blockchain. It is a fault-tolerant technique used to establish an appropriate agreement across the blockchain network. Various consensus algorithms exist such as Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA). In PoW, participating nodes constantly try to validate the block, using their computing power. This mechanism is often criticized for its extensive consumption of energy [21]. On the other hand, PoS is an energy-efficient alternative to PoW, in which consensus is reached by the nodes with a larger proportion of stake in the network. PoA is used in permissioned and private blockchains [22]. In PoA, a set of trusted entities known as validators are responsible to add new blocks to the network. This provides comparatively better performance as it requires fewer validators and less computational power. Respondents of our interview suggest that a blockchain system can use multiple consensus algorithms considering scalability, performance, and security issues.

Network participants should be incentivized for contributing to the network. Incentive mechanisms can also be part of the consensus algorithms. Without the incentive,

a blockchain system would not be successful. Participants can be rewarded with pecuniary or non-pecuniary incentives or both. The governance framework should determine how incentives will be provided for the roles accomplished by the participants such as developers, miners or validators, off-chain contributors, etc. Besides, it is also important to underscore what factors motivate the community members and why node operators want to contribute [1].

The last sub-dimension of protocol that has emerged from the interview data is the maintenance of off-chain storage for storing personal data. This off-chain storage has been suggested by the experts as a way to comply with the GDPR requirements of personal data modification and deletion. In the off-chain storage, data can be deleted, modified, and added. The idea is that all personal data, as deemed by the user, will be stored in off-chain storage. After storing data, a hash value will be generated by algorithms. The generated hash value will then be tagged and synched with the corresponding on-chain network. As a result, when users need to modify or add any personal data, they will be able to do so in the off-chain storage, which will in turn be updated in the on-chain database also. Again, if the users want to delete all their data, then the concerned hash value index will be removed from the off-chain storage, which ultimately will make users' records traceless in the on-chain. To manage the off-chain storage, the governance framework should have guidelines regarding who will be the owner or controller of the off-chain storage, who will be responsible for maintaining this storage, and what would be the process of data modification and deletion, and the responsibility of the user thereon.

4.3 Compliance

Our final theme is directly related to GDPR compliance, which emphasizes defining the roles and responsibilities of the stakeholders and their accountabilities, consent management, and data minimization. GDPR requires appointing a data controller (Article 24, 26), data processor (Article 28), and data protection officer (Article 37) to protect personal data. According to the GDPR, *a data controller* is responsible to implement suitable measures to protect the data subject's rights and to ensure that the data is being processed duly by the data processor. If there is more than one entity responsible for decision-making, a joint controller should be defined. Data controllers ensure the protection of users' data. The *Data processor* processes the data under the supervision of the data controller. *The data protection officer* informs and advises the data controller or the processor and monitors the compliance of GDPR. By *accountability*, GDPR requires that organizations take appropriate technical and organizational measures to protect personal data and be able to justify the effectiveness of those measures if the necessity arises to do so. *Consent* refers to the data subject's wishes that signify agreement to process personal data. Before the collection of personal data, users' consent should be obtained, explicitly mentioning what personal data will be collected, why the data will be processed, and how long the data will be stored. Data needs to be collected as minimally as possible.

GDPR compliant blockchain governance guidelines need to devise who will be the data controller, data processor, and data protection officer, what would be their qualifications and job responsibilities, to whom they will be accountable, what technical and organizational measures should be taken to protect personal data and how those

can be implemented, what would be the controlling mechanisms, and what would be the consequence of a failure of data protection. Regarding consent management, the governance framework may indicate how users' consent will be obtained, how users will be informed about the type of data, the purpose of data collection, and storing periods, and how they can revoke their given consent, etc.

5 Discussion

5.1 Theoretical Implications

Our paper has three major theoretical contributions. First, to the best of our knowledge, our paper on toward developing a blockchain governance framework is the first to accommodate GDPR requirements. The governance frameworks proposed by prior studies are mainly centered on identifying various governance dimensions drawing on different theories and expert interviews without considering GDPR or other regulatory requirements. For example, Beck et al. [2] discussed blockchain governance for blockchain economy—decentralized autonomous organizations (DAO)—drawing on dimensions from IT governance literature: decision rights, accountability, and incentives. Again, Pelt et al. [1] proposed a blockchain governance framework, consisting of six dimensions: formation and context, roles, incentives, membership, communication, and decision making, and three layers: off-chain community, off-chain development, and on-chain protocol. They based their findings on expert interviews, case studies, and an open-source software governance framework. More recently, Goldsby and Hanisch [15] have proposed a blockchain governance model, highlighting the coordination and control challenges faced in blockchain governance contexts and their coping strategies. However, these prior studies did not consider the tensions between GDPR and blockchain design. In our paper, we underscore the possible ways of overcoming those tensions. Therefore, our study extended prior governance frameworks [1, 2, 15] by adding GDPR requirements.

Second, our research identified major concepts related to GDPR compliance of blockchain. Under these concepts, we have identified three dimensions namely community, protocol, and compliance. We have also described what kinds of considerations should be taken concerning these dimensions. Especially, under compliance, we described the roles, responsibilities, and accountabilities of different actors such as data controllers and data processors.

Third, in contrast to prior literature [e.g., 1], we have identified that off-chain storage is a part of the blockchain protocol to be compliant with GDPR. For example, under the off-chain storage sub-dimension, we described how off-chain storage could be used to accommodate the GDPR requirements of data modification and deletion. Our results also reveal that many issues must be considered when governing such off-chain.

5.2 Practical Implications

Our study has several practical implications. First, our interview with the expert revealed that the adoption of blockchain is hindered by the lack of a GDPR compliance governance framework. They are struggling with GDPR requirements while using blockchain

technology. We provided a list of considerations that might help organizations to build a GDPR compliant blockchain business model. Second, understanding how blockchains are governed and how GDPR requirements are met is imperative for policymakers [23]. Our findings will help them in setting standards and practices to expedite the adoption of blockchain technology.

Third, our findings highlight the need for a GDPR-centric blockchain design approach. With this, we suggest blockchain architects proactively consider GDPR requirements and include the GDPR design requirements in the system architecture. This echoes what EPRS [6] suggested by noting that "blockchain architects need to be aware of this [challenge] from the outset and make sure that they design their respective use cases in a manner that allows compliance with European data protection law". The findings of our paper would help blockchain architects while considering how to proactively include GDPR requirements in the system architecture.

6 Limitations and Future Research Directions

The present study has limitations that also guide to spur future research. First, the study is based on industry experts from Finland. Future research could be benefited by considering a more extensive set of experts from different industries and different countries. Second, we proposed different dimensions and considerations in developing a GDPR compliant blockchain by considering the viewpoints of the interviewees who were involved in different cases. With this approach, we managed to identify the key issues that are valid for multiple cases. However, for a more in-depth understanding, future scholars may pursue to validate our recommendations through in-depth case studies.

7 Conclusion

To address the current gap in blockchain governance literature, we attempted to answer the question of how blockchain can be designed that also comply with GDPR requirements. In this regard, we interviewed industry experts who are using blockchain in their organizations. Upon scrutinizing the interview data using the Gioia method, we derived three core dimensions and ten sub-dimensions. We underscored that the organizations could overcome the tensions between GDPR and blockchain by following our recommendations in designing their blockchain.

Acknowledgment. This study was financially supported by the Foundation for Economic Education (www.lsr.fi).

References

1. van Pelt, R., Jansen, S., Baars, D., Overbeek, S.: Defining blockchain governance: a framework for analysis and comparison. Inf. Syst. Manag. **38**, 21–41 (2020). https://doi.org/10.1080/10580530.2020.1720046

2. Beck, R., Müller-Bloch, C., King, J.: Governance in the blockchain economy: a framework and research agenda. J. Assoc. Inf. Syst. **19**, 1 (2018)
3. Zheng, X.R., Lu, Y.: Blockchain technology–recent research and future trend. Enterp. Inf. Syst. 1−23 (2021). https://doi.org/10.1080/17517575.2021.1939895
4. Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., Irani, Z.: A framework for analyzing blockchain technology adoption: integrating institutional, market and technical factors. Int. J. Inf. Manage. **50**, 302–309 (2020)
5. Tan, E., Mahula, S., Crompvoets, J.: Blockchain governance in the public sector: a conceptual framework for public management. Gov. Inf. Q. **39**, 101625 (2022). https://doi.org/10.1016/J.GIQ.2021.101625
6. EPRS: blockchain and the general data protection regulation can distributed ledgers be squared with European data protection law? (2019). https://doi.org/10.2861/535
7. Tankard, C.: What the GDPR means for businesses. Netw. Secur. **2016**, 5–8 (2016)
8. Truong, N.B., Sun, K., Lee, G.M., Guo, Y.: GDPR-Compliant personal data management: a blockchain-based solution. IEEE Trans. Inf. Forensics Secur. **15**, 1746–1761 (2020). https://doi.org/10.1109/TIFS.2019.2948287
9. Bayle, A., Koscina, M., Manset, D., Perez-Kempner, O.: When blockchain meets the right to be forgotten: technology versus law in the healthcare industry. In: Proceedings - 2018 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2018, pp. 788–792 (2019)
10. Jambert, A.: Blockchain and the GDPR: a data protection authority point of view. In: Blazy, O., Yeun, C.Y. (eds.) WISTP 2018. LNCS, vol. 11469, pp. 3–6. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-20074-9_1
11. Dutta, R., Das, A., Dey, A., Bhattacharya, S.: Blockchain vs GDPR in collaborative data governance. In: Luo, Y. (ed.) CDVE 2020. LNCS, vol. 12341, pp. 81–92. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-60816-3_10
12. Kondova, G., Erbguth, J.: Self-sovereign identity on public blockchains and the GDPR. In: Proceedings of the ACM Symposium on Applied Computing, pp. 342–345 (2020)
13. Haque, A.B., Islam, A.K.M.N., Hyrynsalmi, S., Naqvi, B., Smolander, K.: GDPR compliant blockchains-a systematic literature review. IEEE Access. **9**, 50593–50606 (2021)
14. Rieger, A., Lockl, J., Urbach, N., Guggenmos, F., Fridgen, G.: Building a blockchain application that complies with the EU general data protection regulation. MIS Quart. Executive **18**, 263–279 (2019). https://doi.org/10.17705/2MSQE.00020
15. Goldsby, C., Hanisch, M.: The boon and bane of blockchain: getting the governance right. Calif. Manag. Rev. **64**(3), 141–168 (2022). https://doi.org/10.1177/00081256221080747
16. Batubara, F.R., Ubacht, J., Janssen, M.: Challenges of blockchain technology adoption for e-government: a systematic literature review. In: ACM International Conference Proceeding Series (2018).https://doi.org/10.1145/3209281.3209317
17. Gioia, D.A., Corley, K.G., Hamilton, A.L.: Seeking qualitative rigor in inductive research: notes on the gioia methodology. Organ. Res. Methods **16**, 15–31 (2013). https://doi.org/10.1177/1094428112452151
18. Allen, D.W.E., Berg, C., Markey-Towler, B., Novak, M., Potts, J.: Blockchain and the evolution of institutional technologies: implications for innovation policy. Res. Policy **49**, 103865 (2020). https://doi.org/10.1016/J.RESPOL.2019.103865
19. Rossi, M., Mueller-Bloch, C., Thatcher, J.B., Beck, R.: Blockchain research in information systems: current trends and an inclusive future research agenda. J. Assoc. Inf. Syst. **20**, 1388–1403 (2019). https://doi.org/10.17705/1jais.00571
20. Ziolkowski, R., Miscione, G., Schwabe, G.: Decision problems in blockchain governance: old wine in new bottles or walking in someone else's shoes? J. Manag. Inf. Syst. **37**, 316–348 (2020). https://doi.org/10.1080/07421222.2020.1759974
21. O'dwyer, K.J., Malone, D.: Bitcoin Mining and its Energy Footprint (2014)

22. Singh, P.K., Singh, R., Nandi, S.K., Nandi, S.: Managing smart home appliances with proof of authority and blockchain. In: Lüke, K.-H., Eichler, G., Erfurth, C., Fahrnberger, G. (eds.) I4CS 2019. CCIS, vol. 1041, pp. 221–232. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22482-0_16
23. Wright, A., de Filippi, P.: Decentralized blockchain technology and the rise of lex cryptographia. SSRN Electron. J. (2015).https://doi.org/10.2139/SSRN.2580664