# Blockchain and the GDPR – the shift needed to move forward

Inês Campos Ruas [1], Soumaya Ben Dhaou [1] and Zoran Jordanoski [1]

[1] *United Nations University on Policy-Driven Electronic Governance (UNU-EGOV), Guimarães, Portugal*

**Abstract**

Complying with the European Union General Data Protection Regulation (GDPR) poses a significant challenge for blockchain technology and its applications. The immutability, tamper-proof nature, and decentralized structure of blockchains clash with privacy, data collection, and processing requirements outlined in the GDPR. This paper proposes critical insights into existing approaches and solutions for aligning GDPR compliance with blockchain technology. Moreover, it presents an alternative perspective that addresses the regulatory grey areas but also advocates for the need to cultivate flexibility within regulation and policy frameworks. By embracing this paradigm shift, the full potential of blockchain technology can be unleashed, fostering innovation and paving the way for transformative blockchain applications.

**Keywords**

Blockchain, GDPR, Compliance, Workarounds, Mindset

## 1. Introduction

The first blockchain implementation using a public ledger for transactions through Bitcoin happened in 2009 [1]. Since then, these concepts – Blockchain and Bitcoin – are inevitably linked.[2] However, blockchain technology has a much wider application today beyond cryptocurrencies, and its applications can vary from the execution of smart contracts, maintaining a shared and transparent system of record, auditing supply chains, and providing proof of insurance, among others [3]-[4].

GDPR was enforced on May 25, 2018 [5]. The regulation does not integrate the specific characteristics of blockchain technology. Critical issues and challenges arise in adopting and using blockchain technology by European organisations and international companies dealing with European Union (EU) data subjects. This is not only limiting the use of a potential game-changer technology for many sectors - industries, finance, government public services and humanitarian work - but also constraining innovation within Blockchain and its application [6]-[7].

This paper reflects on the alignment/misalignment of GDPR and blockchain technology. It proposes a critical discussion of the workarounds and solutions organisations and companies adopt to comply with GDPR. Based on literature reviews, case studies analysis and semi-structured interviews with experts in the field, this paper delves into the incompatibility between GDPR and Blockchain technology to investigate the existing solutions and propose an alternative perspective to approach a technology that does not follow the traditional standards.

The paper is organised as follows: Section 2 provides an overview of the current state of blockchain technology and discusses the challenges and barriers to adopting blockchain technology due to GDPR compliance. Besides, it identifies specific GDPR articles that pose the most significant challenges and explores the workarounds proposed. Section 3 describes the approach and methodology adopted. Section 4 looks into two applications of blockchain technology (tracking and tracing in the agri-food industry and data ownership in health care), highlighting the alignment of blockchain technology with GDPR and complementing this information with the current workarounds to overcome some existing frictions. Section 5 reflects on these conflicts and presents a different perspective to look into these

Proceedings EGOV-CeDEM-ePart 2023, September 04-07, 2023, Budapest, Hungary
EMAIL: ruas@unu.edu (A.1); bendhaou@unu.edu (A.2); jordanoski@unu.edu (A.3)
ORCID: 0009-0007-9667-3128 (A.1); 0000-0002-6616-349X (A.2); 0000-0003-1784-9038 (A.3)

issues to find a better balance between how GDPR protects data and privacy and how innovation within Blockchain can still be prompt.

## 2. Blockchain and GDPR

The hype raised by blockchain technology for several years is now behind us. International organisations within the United Nations (UN), such as WFP, UN Women, UNICEF, UNOPS, and UNDP, have taken the lead and are experimenting with blockchain applications and developing pilots [8]. Today, initiatives and efforts are turned toward standards, legal aspects, and regulations. International and regional organisations, as well as Governments, are setting regulatory frameworks. However, in some cases, the regulatory framework, such as GDPR, becomes the main barrier to innovation.

The World Economic Forum has signalled the struggle towards innovation, particularly with blockchain technology due to the GDPR. They advocate for more flexible regulation and policy frameworks to allow the potential and benefits of Blockchain technology to be fully realized [9].

GDPR compliance is creating several challenges and barriers to adopting blockchain technologies. Even though the potentiality and promises of blockchain technology are acknowledged, and a panoply of workarounds to make Blockchain use compliant with the EU Regulation 2016/679 GDPR are proposed [7][10]-[15], uncertainties still exist, as well as any doubts among blockchain developers and experts about the regulatory challenges. Therefore, legislators and regulators must investigate the legislation's grey areas and keep pressuring regulators for more clarity on the areas that can have different interpretations according to the specific application use case and the expert looking into it.

The GDPR challenges identified, especially for public permissionless blockchains, concerns issues on the identification of the Data Controller (Article 4(7) about Articles 24 and 32), implementation of the Data protection by design and by default principles (Article 25), the principles for Lawfulness of Processing (Article 6), Data minimization (Article 5(1)(c)), the Data subjects rights (such as the Right to Access (Article 15), Right to Rectification (Article 16), Right to erasure ('Right to be forgotten' (Article 17), Right to erasure ('Right to be forgotten' (Article 17), Right to lodge a complaint with a supervisory authority (Article 77), Right to compensation and liability (Article 82), and the Transfers of personal data to third countries (Article 44-50) [5], interview3].

This paper will focus on three GDPR articles representing significant challenges to complying with the regulation (please check Table 1).

**Table 1 (Authors) GDPR articles directly conflicting with blockchain**

| GDPR Article | Conflicting Blockchain property |
|---|---|
| Data minimization (Article 5(1)(c)) | On a public blockchain, all the data stored are available to all participants of the peer-to-peer network. This is a problem regarding data minimization since no data besides the strictly necessary should be stored. |
| Right to erasure ('Right to be forgotten (Article 17)) | Due to the architecture of blockchains, i.e., the linkage between blocks, it is only possible to erase the last block without destroying the structure of the blockchain. This impossibility of removing data from the blockchain is one of the main compliance incompatibilities. |
| Data Controller (Article 4(7) with Articles 24 and 32) | This article implies the existence of a central control authority that ensures compliance with the data protection rights of data subjects. Due to the decentralised nature of Blockchains and the disintermediation of a trusted third party, this does not exist, specifically for public blockchains. |

These challenges directly or indirectly refer to data collection and processing issues. Indeed, as a consequence of the misalignments between the blockchain technology properties and GDPR, explicitly concerning the first article of Data minimisation (Article 5(1)(c)), most authorities and experts agree it is not recommended to store personal data on the blockchain [12]. Blockchain's characteristics of immutability and traceability [16], along with its decentralised structure, are often linked to excellence

in security properties (i.e., integrity, auditability, authenticity, and availability) [13]. However, issues arise regarding privacy and data protection.

Blockchains are immutable, tamper-proof, and available to all participants in a transparent manner; thus, data integrity is guaranteed [17]. Nonetheless, this implies a direct contradiction with the data protection regulations.

Progress in blockchain research proposes some solutions. It is now possible to store the data externally (off-chain). Only the hash data is stored in the blockchain network, meaning only the private key owner will access this data. This is the person or entity deciding on control, process and modification of that data. This way, users can be granted data minimization [18]-[19].

Off-chain storage can also help overcome the lack of compliance with the Right to erasure requirement. Due to the cryptographic hashes and the links between the blocks, it is impossible to delete data in blockchains. The off-chain data can be erased, but the corresponding hash would remain on the ledger [20][20].

In the situation described previously, if the remaining hash-value is to be seen as personal data, another workaround for the second GDPR article in Table 1 (Article 17) is data purging by encryption. In this situation, all the data is encrypted, and the keys are kept outside the data storage. And even though the understanding of erasure can be seen as unclear and leaving room for interpretation, destroying the associated decryption keys makes it impossible to access the data and identify the data subject. Currently, this might be a short-term solution respecting unreadable data. Nonetheless, with Research & Development (R&D) on decryption methods, this might change quickly and not be a long-term solution [14]-[15].

From a positive perspective, developments in modern cryptography allowed storing personal data through techniques such as Zero Knowledge Proofs or Merkle proofs. These methods will add a privacy-preserving layer that allows verifying the data authenticity without revealing the information itself or the identity of individuals [20]-[21].

The third GDPR issue that we will focus on is the definition of a Data controller (Article 24), which is defined as the entity that determines the goals and means of the data. As this definition is not a linear process in blockchains due to its decentralised structure, there is no agreement on the blockchain controller, and currently, in the literature, three interpretations can be found: (1) nodes and miners are data controllers; (2) nodes and miners are not data controllers, and (3) users are the data controllers [22].[22] In any case, Smart contracts can be used to rise above Article 24 regarding the Data Controller since these allow for a dynamic consent management solution, i.e. a novel means of engaging individuals in the use of their personal information. In other words, users, nodes and miners must execute a detailed contract where their responsibilities are determined [19].

It is essential to highlight that even though solutions are proposed, and research is continuously looking for solutions to improve compliance between GDPR and blockchain, most of the misalignment seems to be case-specific. Therefore, it is not possible to propose a one-size-fits-all solution. According to each use-case of blockchain technology, blockchain architects must evaluate the need for information processing and the reason and the way this information is being collected, stored and processed [21].

This discussion becomes even more pressing with Web 3.0, a new iteration of the World Wide Web. This next evolution emphasizes decentralization, moving data away from central authorities and establishing applications and services surrounding blockchain technologies [23]. Even though Web3 is still in its infancy, this vision takes blockchain disintermediation to the next level by making it ubiquitous, encompassing not only payments and financial services but also digital identities, data and business models [24].

## 3. Methodology

This paper arises as the first output from the Systematic Literature Review (SLR) on Blockchain and GDPR, using the research engines Scopus and Google Scholar, and grey literature, such as reports and formal documents, by renowned institutions.

This SLR is still ongoing. It allowed us to realize that the solutions presented towards best practices for blockchain use cases (CNIL[2] and ENISA[3]) and compliance between blockchain and GDPR is often very technologically driven [11][20][25]-[26]. A different approach for setting the ground for this technology is suggested.

Moreover, three interviews with experts from different sectors (academy, law, entrepreneurship) have been done to complement the desk research, and more are planned to be done in the future.

## 4. Applications of blockchain technology

To better understand the friction between blockchain and the GDPR, a desk review was performed to identify the solutions and map the workarounds with the GDPR framework. Furthermore, case studies were analysed, and interviews were conducted with experts in the field to complement the explanatory and the multidimensional perspective and build a critical discussion of the proposed solution and workarounds.

Case studies observation showed that different technical solutions had been developed to overcome regulatory barriers and avoid the risks associated with GDPR compliance. These solutions allow using and adopting of blockchain technology.

For example, FRoSTA AG, one of Europe's largest manufacturers of frozen food products, implemented a blockchain technology-based solution to Track and Trace products. The Blockchain Technology-based solution allows for knowing the product origin (e.g. frozen fresh fish) by providing reliable provenance data about where the fish was captured and printed on the package. This enables consumers to obtain information on frozen fish products in the supply chain. The security linked with this ability to track and trace goods and gather information is a key requirement in the agri-food business and for environmental sustainability [27].

In the case of My Health My Data[4] (MHMD), part of the Horizon 2020 research and innovation program, they developed a dynamic consent interface that allows patients to handle their data independently to comply with the GDPR regulatory framework. MHMD will enable patients to access their data in a personal cloud from any device, anywhere. Personal data is de-identified and encrypted on this application before being available to researchers or analysts. The MHMD Technology is based on Hyperledger Fabric using Smart Contracts and complies with the GDPR [28].

Despite examples of successful compliance with Blockchain use cases and the GDPR, it is not the case for most Blockchain-developed solutions. It is often happening in a more constrained way and leads to limiting the use of the technology to its full potential. Indeed, it often creates challenges in adopting this technology [29] and discourages using Blockchain and developing potential innovative solutions.

## 5. Discussion and conclusions

Technology such as blockchain generates different opinions about how it can be used and how it uses data. This opinion often varies amongst different actors and institutions.

Some experts defend that using workarounds limits the potential of blockchain technology. They would agree with one of the interviewed experts when she mentioned in our interview that “If you want the potential of blockchain in the public sector, especially, (…) it needs to be permissionless blockchain, it needs to be open blockchain, decentralised” [Interview1]. In comparison, other experts argue that these workarounds are a necessary trade-off that will enable using those Blockchain technology advantages to avoid GDPR restrictions.

Regardless of one's stance on the utilization of workarounds, it is undeniable that blockchain technology has established its presence and is poised to endure. The level of adoption at the private level, particularly in the public sector, shows increasing interest in blockchain technology, and a solution at the regulatory level should be proposed to facilitate the use for people without risks.

[2] www.cnil.fr/
[3] www.enisa.europa.eu/
[4] www.myhealthmydata.eu/

Initiatives such as the European blockchain regulatory sandbox[5] aim to promote the dialogue between different actors in the field, such as regulators and public authorities. These dialogues bring real use cases, and their developers to present their cases and receive legal guidance. This project started this year, 2023, thus it is still early to assess its effectiveness. Moreover, work should be developed in different fronts to achieve successful results.

The Government has a key role in supporting the adoption of the technology.

Indeed, the increased interest in blockchain showed a rising need for adequate capabilities. One of the interviewed experts highlighted that besides "investing in education with a focus on the development of skills, governments could also dedicate more research funds to this technology to develop technical solutions that allow for privacy and safety" [Interview 2]. However, all the solutions proposed so far arise from a techno-centric perspective focusing only on technical solutions for improving the level of adoption of blockchain technology and reducing regulatory risks. This perspective tends to limit trust in the adoption of the technology.

While at the same time, blockchain technology can potentially increase trust as it increases transparency [interview 1]. Nonetheless, the interview highlighted how this trust relationship between "the government and its citizens could not rely only on the technology, especially when it concerns citizens that do not know much about it. And even when it regards more educated people, blockchain can be used in different domains, to the extent that it is hard for one person to understand everything about blockchain".

It is also critical to emphasise that blockchain technology is a paradigm shift. It is important to think out of the box, whether related to regulatory changes or other policies. The decentralisation property of the technology - i.e., a database (ledger) that is copied and distributed among all network users - is a unique blockchain characteristic that unsettles the traditional and centralised way systems and processes work. Before proposing any solution, it is mandatory to unlearn some ways of doing things and acquire and develop new capabilities [19]. For that, education and agility are key assets.

Blockchain technology is often presented as a disruptive technology [16]. What can be seen nowadays is how this disruption arises not so much from the technology itself - as it was thought in the beginning, but from the mindset shift it requires. It is time to consider a different direction for solutions to the conflict between Blockchain and GDPR and regulatory framework in general, shifting the focus away from R&D. Moreover, an adjustment in the high expectations associated with this technology needs to occur to allow its unfolding and growth.

Firstly, working with this technology requires a mindset shift away from the centralised processing and working we are used to. For that, as a starting point, learning and education are essential. Thus, observing the increasing use and adoption of international global entities, such as the UN, using a global technology like blockchain is important. It will enhance the interest and the need to get educated, learn more about this technology, and benefit from its potential. Moreover, similarly to the work developed by the European blockchain regulatory sandbox that is shifting away from competition and towards collaboration, this can be taken a step further, involving and bringing together more stakeholders (private sector, public sector, entrepreneurs, researchers, coders/developers, users) to discuss and create an ecosystem in order to reach some consensus.

Secondly, agility might also play an important role. It is important to consider how the GDPR may hinder innovation within blockchain technology. In other continents, with no involvement of EU citizens, blockchain technology innovation can be more needs-driven, according to the local conditions and environment. Although data protection regulations are needed, a better balance can be reached between how innovation is stimulated within Blockchain technology and how data protection regulations protect citizens and users.

It is impossible to generalise solutions for the conflicts between blockchain technology and GDPR, even though many workarounds exist nowadays. Even in European Data Protection Board (EDPB) strategy 2021-2023 and in EDPB's Workplan for 2023-24 there are references to develop additional work on "Guidelines on Blockchain" [30]-[31]. Nonetheless, it appears unlikely that with the current text of the regulation, all the current "frictions" are solved and the principle of protecting privacy prevails over the potential innovation of the technology. Thus, limiting the technology promises implies

[5] ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Sandbox+Project

that blockchain technology will not be used or explored at its full potential. Moreover, this might also discourage several initiatives and pilots of creating added value and increase trust and transparency. At the same time, the value brought by the GDPR is critical - data subjects' and their data matters. Taking into consideration the aforementioned factors and recognising the potential of blockchain technology to be leading a broad range of innovations, we propose starting to look into this (commonly referred to as) disruptive technology with a different mindset, acknowledging the paradigm shift and delving into innovative solutions and not only focusing on adapting the technology for short-term remedial responses.

Are we ready for this shift?

## 6. Acknowledgements

This document is a result of the project "INOV.EGOV-Digital Governance Innovation for Inclusive, Resilient and Sustainable Societies / NORTE-01-0145-FEDER-000087", supported by the Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (EFDR).

## 7. References

[1] Institute of Chartered Accountants in England and Wales (ICAEW). (n.d.). History of Blockchain. https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-articles/what-is-blockchain/history

[2] PricewaterhouseCoopers (PwC). (n.d). *Making sense of bitcoin, cryptocurrency and blockchain*. PwC. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

[3] Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. International Conference on Information Networking. https://doi.org/10.1109/icoin.2018.8343163

[4] Zīle, K., & Strazdiņa, R. (2018). Blockchain Use Cases and Their Feasibility. Applied Computer Systems, 23(1), 12–20. https://doi.org/10.2478/acss-2018-0002

[5] Intersoft Consulting. (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

[6] United Nations Conference on Trade and Development (UNCTDA). (2021). Harnessing Blockchain for sustainable development: Prospects and challenges. https://unctad.org/system/files/official-document/dtlstict2021d3_en.pdf

[7] Godyn, M., Kedziora, M., Ren, Y., Liu, Y., & Song, H. H. (2022). Analysis of solutions for a blockchain compliance with GDPR. Scientific Reports, 12(1), Artigo 1. https://doi.org/10.1038/s41598-022-19341-y

[8] Dumitriu, P., Helck, S., Bricks, E., Dincic, D., Yu, R., & Mueller, S. C. (2020). Blockchain applications in the United Nations System: Towards a state of readiness (JIU/REP/2020/7). Joint Inspection Unit. https://digitallibrary.un.org/record/3906141

[9] Toth, A. (2018, May 24). Will GDPR block Blockchain? World Economic Forum. https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/

[10] Suripeddi, M. K. S., & Purandare, P. (2021). Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing. Journal of Physics: Conference Series, 1964(4), 042005. https://doi.org/10.1088/1742-6596/1964/4/042005

[11] Zemler, F., & Westner, M. (2019). Blockchain and GDPR: Application Scenarios and Compliance Requirements. 2019 Portland International Conference on Management of Engineering and Technology (PICMET), 1–8. https://doi.org/10.23919/PICMET.2019.8893923

[12] Timmons, J., & Hickman, T. (2020). Blockchain and the GDPR: Coexisting in contradiction? Journal of Data Protection & Privacy, 3(3), 310–322.

[13] Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain Mutability: Challenges and Proposed Solutions. IEEE Transactions on Emerging Topics in Computing, 9(04), 1972–1986. https://doi.org/10.1109/TETC.2019.2949510

[14] Stach, C., Gritti, C., Przytarski, D., & Mitschang, B. (2022). Can blockchains and data privacy laws be reconciled?: A fundamental study of how privacy-aware blockchains are feasible. Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, 1218–1227. https://doi.org/10.1145/3477314.3506986

[15] Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. Computer Law & Security Review, 38, 105454. https://doi.org/10.1016/j.clsr.2020.105454

[16] Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for Public Services: A Systematic Literature Review. IEEE Access, 9, 13904–13921. https://doi.org/10.1109/ACCESS.2021.3052019

[17] Stach, C., Gritti, C., Przytarski, D., & Mitschang, B. (2022). Assessment and treatment of privacy issues in blockchain systems. ACM SIGAPP Applied Computing Review, 22(3), 5–24. https://doi.org/10.1145/3570733.3570734

[18] Ault, M. (2018). Why new off-chain storage is required for blockchains. IBM, Tech. Rep. https://www.ibm.com/downloads/cas/RXOVXAPM

[19] Al-Abdullah, M., Alsmadi, I., AlAbdullah, R., & Farkas, B. (2020). Designing privacy-friendly data repositories: A framework for a blockchain that follows the GDPR. Digital Policy, Regulation and Governance, 22(5/6), 389–411. https://doi.org/10.1108/DPRG-04-2020-0050

[20] Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. Blockchain: Research and Applications. https://doi.org/10.1016/j.bcra.2023.100129

[21] Schellinger, B., Völter, F., Urbach, N., & Sedlmeir, J. (2021, September 19). Yes, I Do: Marrying Blockchain Applications with GDPR. https://doi.org/10.24251/HICSS.2022.563

[22] Merlec, M. M., Lee, Y. K., Hong, S.-P., & In, H. P. (2021). A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR. Sensors, 21(23), Article 23. https://doi.org/10.3390/s21237994

[23] Wang, Q., Li, R., Wang, Q., Chen, S., Ryan, M., & Hardjono, T. (2022). Exploring Web3 From the View of Blockchain (arXiv:2206.08821). arXiv. http://arxiv.org/abs/2206.08821

[24] Buldas, A., Draheim, D., Gault, M., Saarepera, M. (2022). Towards a Foundation of Web3. In: Dang, T.K., Küng, J., Chung, T.M. (eds) Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. FDSE 2022. Communications in Computer and Information Science, vol 1688. Springer, Singapore. https://doi.org/10.1007/978-981-19-8069-5_1

[25] Haque, A. B., Islam, A. K. M. N., Hyrynsalmi, S., Naqvi, B., & Smolander, K. (2021). GDPR Compliant Blockchains–A Systematic Literature Review. IEEE Access, 9, 50593–50606. https://doi.org/10.1109/ACCESS.2021.3069877

[26] Han, S., & Park, S. (2022). A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review. IEEE Access, 10, 103888–103905. https://doi.org/10.1109/ACCESS.2022.3210110

[27] Kramer, M. P., Bitsch, L., & Hanf, J. (2021). Blockchain and Its Impacts on Agri-Food Supply Chain Network Management. Sustainability, 13(4), Article 4. https://doi.org/10.3390/su13042168

[28] Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in Biology and Medicine, 129, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130

[29] Kolan, A., Tjoa, S., & Kieseberg, P. (2020). Medical Blockchains and Privacy in Austria—Technical and Legal Aspects. 2020 International Conference on Software Security and Assurance (ICSSA), 1–9. https://doi.org/10.1109/ICSSA51305.2020.00009

[30] European Data Protection Board (EDPB). (2020, December). Strategy 2021-2023. https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2021-2023_en

[31] European Data Protection Board (EDPB). (2023, February). Work Programme 2023-2024. https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-2023-2024_en