Jog-Állam-Politika, 2025/3.81
DOI: 10.58528/JAP.2025.17-3.81

TANULMÁNYOK

MARIAM PILISHVILI

Permacrisis: blockchain's plan to fix the normative challenges in EU data protection law[1]

ABSTRACT

Permacrisis has also reached the doorstep of European Union (EU) personal data law. It is no surprise that this has prompted a major reevaluation of significant normative issues in the field. The primary challenge lies in the rapid growth of advanced technologies, such as blockchain. This raises the first question: "What is a blockchain?" A collection of permanent records linked together and highly resistant to alteration. In other words, a 21st-century revolution which repeatedly tests traditional frameworks such as the General Data Protection Regulation (GDPR). The GDPR's 'right to be forgotten' principle, which allows data subjects to request the deletion of their personal data, conflicts with the immutable nature of blockchain. Furthermore, the integration of blockchain into existing legal systems raises issues of compatibility and effectiveness. This paper discusses the conflict by examining several examples from EU member states, beginning with the Berlin-based company BigchainDB's initiative and extending to Italy's challenges in reconciling GDPR principles with new sector-specific requirements. Finally, it offers multi-faceted approaches necessary to address the significant challenges posed by blockchain.

Keywords: blockchain law ■ decentralized technology ■ EU law ■ European Union ■ personal data ■ permacrisis ■ tech innovators ■ legal experts ■ General Data Protection Regulation ■ right to be forgotten

I. INTRODUCTION

The convergence of blockchain technology and the European Union's GDPR poses one of the most intricate legal dilemmas of the digital era. With its core attributes of decentralization, transparency, and permanence, blockchain holds groundbreaking potential across sectors like

[1] A tanulmány megjelenését a Nemzeti Média és Hírközlési Hatóság támogatta | The publication of the study was supported by the National Media and Infocommunications Authority

finance, healthcare, and supply chain logistics.[2] Yet, these very characteristics clash with the principles of the GDPR, notably the Right to be Forgotten (Article 17) and the requirements for data minimization (Artice 5(1)(c)). This conflict highlights the broader difficulties regulators encounter in an age of continuous crisis, where technological, economic, and geopolitical upheavals intersect to fuel ongoing uncertainty.

Under the GDPR, the immutable nature of blockchain directly contradicts the requirement to erase personal data upon request. Once data is recorded on blockchain ledger, it becomes permanent, and deleting it necessitates complex technical and operational adjustments that undermine the integrity of the ledger.[3] This presents a core challenge for regulators, as it implies that GDPR compliance may require technical adjustments that could disrupt blockchain's fundamental functionality, jeopardizing its decentralized structure.[4]

Although methods like pseudonymization and hashing have been suggested, they do not entirely remove GDPR compliance risks, as hashed data can frequently be re-identified.[5] New blockchain frameworks, such as BigchainDB, aim to address these conflicts by incorporating privacy-enhancing features like permissioned networks and selective data sharing, but substantial obstacles still persist.[6] For instance, the implementation of permissioned networks could provide some control over data sharing, but this control goes against the core decentralized principles of blockchain, creating a conflict between privacy protection and decentralization.[7]

Italy's regulatory strategy offers valuable lessons for tackling blockchain compliance. The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) has stressed the importance of establishing clear accountability structures within blockchain systems, particularly in identifying ‚data controllers' and ‚processors' under the GDPR.[8] Italy has also led the way in using blockchain within public administration including its integration into the digital identity system, Sistema Pubblico di Identità Digitale (SPID), while ensuring GDPR compliance.[9] These efforts demonstrate the potential to align blockchain innovation with robust data protection standards.

The European Union has made addressing data protection challenges a key part of its digital transformation strategy. While the European Blockchain Partnership (EBP) aims to establish a cohesive blockchain framework across member states, the absence of enforceable legal provisions hinders effective im-

[2] Zavolokina et al., 2020.
[3] Finck, 2018, 88-116.
[4] Lopes – Castro – Russo, 2024.
[5] Voigt – von dem Bussche, 2017.
[6] BigchainDB: BigChain White Paper, 2020.
[7] Li – Jiang – Chen, 2017.
[8] Garante per la Protezione dei Dati Personali: Annual Report on Emerging Technologies, 2021.
[9] Mentasti, 2020; Hong – Kim, 2020, 1238.; Torres, 2018.

plementation.[10] Italy's initiatives and the EU's broader regulatory landscape reflect widespread uncertainties, especially regarding cross-border data transfers after the Schrems II ruling.[11] The global, decentralized nature of blockchain often complicates the process of ensuring adequate personal data protections as mandated by the GDPR.[12] As blockchain projects expand beyong the EU's borders, the challenges of balancing decentralized autonomy with centralized regulatory oversight will become increasingly evident.

Blockchain's ability to transform emerging industries is unquestionable. Yet, its conflict with GDPR principles underscores the challenges regulators and businesses face in striking a balance between innovation and compliance. Although technologies like BichainDB and privacy-enhancing features provide potential solutions, significant hurdles still exist. Likewise, Italy's approach showcases how decentralized technologies can be utilized in the public sector, however, greater legal clarity at the EU level is necessary to ensure that blockchain's transformative potential is fully realized within a strong data protection.

II. THE FRAMEWORK OF THE STUDY

1. Theoretical Context

As mandated by BigchainDB, blockchain technology can address GDPR concerns primarily through permissioned networks and selective data sharing. Another great example of exposing personal data while maintaining blockchain's decentralized structure has been provided by Italy's public digital identity system's approach. Both attempts have been subject to scrutiny. Italy's approach faces ongoing concerns about establishing clear accountability structures, particularly in identifying data controllers and processors, as required by the GDPR. Additionally, the integration of blockchain within a decentralized framework in the public sector may conflict with GDPR's emphasis on centralized oversight, especially in relation to data protection mechanisms.[13] In the case of BigchainDB, the use of permissioned networks limits the level of decentralization typically associated with blockchain technology. Moreover, privacy-enhancing features like selective data sharing do not entirely mitigate the risk of data re-identification, which remains a significant challenge under GDPR.

Therefore, our research will focus on evaluating whether blockchain technology, when applied strategically, can overcome the normative challenges posed

[10] EBP Declaration, 2018.

[11] Case C-311/18. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrem. Judgment of the Court (Grand Chamber) of 16 July 2020, ECLI:EU:C:2020:559.

[12] Voigt – von dem Bussche, 2017.

[13] Werbach, 2018.

by the GDPR. Specifically, we will examine how blockchain can reconcile its immutable data storage with the GDPR's requirements for personal data rights.

2. Legal Context

In our research, we will use document analysis and case studies methodologies to explore the potential of blockchain technology in overcoming the normative challenges posed by the GDPR. Through document analysis, we will closely examine the relevant legal texts, including key articles of the GDPR, to understand how blockchain's immutable data storage interacts with the requirements for personal data rights. We will also analyze case studies, including BigchainDB and Italy's initiatives, which respectively aim to address GDPR concerns through permissioned networks and integrate blockchain into public administration systems.

Additionally, we will review key literature on blockchain to enhance our understanding of its technical foundations and regulatory implications. Works such as Satoshi Nakamoto's *Bitcoin: A Peer-to-Peer Electronic Cash System*,[14] *Blockchain and the Law* by Dariusz Szostek,[15] and Mastering Blockchain by Bashir Imran, provide critical perspectives on how blockchain can help resolve legal challenges and explore how its decentralized structure can be harmonized with legal data privacy requirements.

We will also examine the views of key advisory think tanks, such as EU Blockchain Observatory and Forum, to assess how the EU perceives the use of blockchain in relation to GDPR compliance.

III. DATA AND INFORMATION

1. Historical Overview of the Right to be Forgotten

As society's perceptions of privacy, data security, and individual autonomy have changed over time, so too has the legal notion known as the Right to be Forgotten (RTBF). Its roots are in European legal traditions, where civil law systems have long placed a strong emphasis on protecting people's reputations and sense of dignity.[16]

The European Union's 1995 Data Protection Directive, which established the framework of contemporary privacy rules, was the first directive to introduce the context of data protection. When personal data was no longer required for

[14] Nakamoto, 2009.
[15] Szostek, 2019.
[16] Weber, 2011, 120-130.

the purpose for which it was gathered, society had the right to request that it be erased under Article 12(b) of the directive. However, the Directive's provisions were more restricted in scope than those of the GDPR, and the phrase 'Right to be Forgotten' was not used explicitly.[17]

With a historic Court of Justice of the European Union (CJEU) ruling in *Google Spain v. AEPD*[18] in 2014, the RTBF attracted global attention. Based on the case materials, a Spanish citizen asked Google to remove links to out-of-date and unrelated material about his financial background from its search results. Search engines are data controllers under EU law, according to the CJEU, and therefore have to comply be data users' requests to remove links that are "inadequate, irrelevant, or no longer relevant".[19] This landmark decision created a precedent for the RTBF's inclusion in the GDPR and recognised it as a fundamental right under EU law.

The RTBF was defined in Article 17 of the GDPR, which went into effect in 2018. Under certain circumstances, such as when the data is no longer reuqired for the reason it was collected, when consent is revoked, or when the data has been processed unlawfully, this clause gives data users the right to request the erasure of their personal data.[20] However, the GDPR also introduced restrictions to the RTBF, including exclusions for legal requirements, public interest, and freedom of expression.

The RTBF has impacted data privacy regulations outside of the EU, such as in Asia and Latin America. The RTBF's global reach is demonstrated by the comparable provisions found in South Korea's Personal Information Protection Act (PIPA) and Brazil's General Data Protection Law (LGPD).[21] Its application outside of the EU has been uneven, too, with certain countries prioritizing freedom of expression over data erasure rights.

The RTBF has been criticised by a number of sources despite its importance. Critics contend that it is incompatible with people's right to know and freedom of expression, especially when it comes to historical documents or prominent people.[22]

In conclusion, the RTBF has developed from a theoretical concept to a fundamental component of contemporary data protection law. The EU's commitment to protecting individual privacy in the digital age is shown in its inclusion in the GDPR. The RTBF's implementation is still difficult,[23] though, as the blockchain scenario illustrates, especially when it comes to balancing it with technical advancement and fundamental rights.[24]

[17] Kuner, 2012, 1-14.
[18] CJEU (2014). Google Spain v. Agencia Española de Protección de Datos (AEPD). Case C-131/12.
[19] CJEU (2014). Google Spain v. Agencia Española de Protección de Datos (AEPD). Case C-131/12.
[20] Voigt – von dem Bussche, 2017.
[21] Greenleaf, 2021, 169.
[22] Rosen, 2012, 88-92.
[23] Barnal, 2018.
[24] Weber – Staiger, 2021, 229-241.

2. BigchainDB's Initiative

BigchainDB is a noteworthy blockchain innovation that attempts to solve some of the fundamental drawbacks of conventional blockchain systems, specifically with regard to data privacy and GDPR compliance.[25] BigchainDB presents a hybrid architecture that combines the advantages of blockchain technology with the scalability and performance of distributed databases, in contrast to traditional blockchains, which place an absolute priority on decentralisation and immutability.[26]

BigchainDB's support for permissioned networks, which limit access to only those who are authorised, is one of its distinguishing features. Because it enables participants to manage who can access and interact with personal data stored on the blockchain, this feature is especially pertinent when it comes to GDPR compliance.[27] Public blockchains, such as Bitcoin,[28] on the other hand, are completely open, which makes it challenging to implement data protection measures.

BigchainDB has been used in a number of industries, such as intellectual property, supply chain management, and healthcare. BigchainDB, for instance, has been utilised in the healthcare industry to develop safe and compatible systems for exchanging patient data while guaranteeing adherence to data protection laws.[29] It has also made it possible for supply chain management to be more transparent and traceable without sacrificing the privacy of sensitive data.

These applications do, however, also draw attention to the continued difficulties in integrating blockchain technology with GDPR. For instance, healthcare providers can securely share patient data using BigchainDB's selective data sharing capability, but this does not completely remove the risk of reidentification or unathorised access.[30] To guarantee complete compliance with GDPR, organizations must implement extra security measures like audit trails and access controls.[31]

Hence, key initiatives proposed by BigchainDB can be placed as follows: permissioned networks, selective data sharing, and mutable data structures. The actions taken by it mark a major advancement in bringing blockchain technology into compliance with GDPR regulations. Its technological advancements, practical uses, and privacy-enhancing features show promise in balancing the flexibility demanded by contemporary data protection regulations with the immutability of blockchain. However, there are still a lot of obstacles to overcome,

[25] Werbach, 2018.
[26] BigchainDB 2.0, 2020.
[27] Zavolokina et al., 2020.
[28] Bashir, 2022.
[29] McConaghy et al., 2016.
[30] Zavolokina et al., 2020.
[31] Lloyd, 2020.

such the trade-off between control and decentralisation, the possibility of data re-identification, and legal ambiguity.[32]

3. Italy's Initiative

While tackling the difficulties presented by the GDPR, Italy has become a leader in the European Union in investigating the possibilities of blockchain technology. Italy has shown how blockchain may be incorporated into public administration systems without sacrificing data privacy standards with its creative legislative framework and useful uses. The regulatory approach, the incorporation of blockchain technology into the Sistema Pubblico di Identità Digitale (SPID), and the wider ramifications for GDPR compliance are the main topics of this section's analysis of Italy's projects.

Italy has taken a proactive but cautious approach to blockchain regulation, striking a balance between innovation and strong data security. This approach was largely shaped by the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali), which highlights the significance of openness and accountability in blockchain systems.[33] In particular, as mandated by GDPR Article 4, the Garante has emphasised the necessity of identifying data controllers and processors within blockchain networks. In decentralised systems, where several participants frequently share responsibilities for data processing, this is especially difficult.

The EU Blockchain Observatory and Forum's recommendations, which support a uniform approach to blockchain regulation among member states, are also incorporated into Italy's regulatory framework (EU Blockchain Observatory, 2020). Italy has set itself up as a role model for other EU nations looking to govern blockchain technology by implementing these recommendations.

Italy has created blockchain implementation guidelines to address this issue, mandating that companies set up transparent governance and accountability frameworks.[34] Blockchain-using public and private organisations, for instance, are required to record their data processing operations and make sure that all parties adhere to GDPR guidelines, which include purpose limitation and data minimisation. With these actions, Italy has established itself as a template for other EU nations looking to control blockchain technology.

The incorporation of blockchain technology[35] into Italy's public digital identity system is among the nation's most noteworthy initiatives. In order to access public services including social security benefits, medical information, and tax

[32] Werbach, 2018.
[33] Garante per la Protezione dei Dati Personali: Annual Report on Emerging Technologies, 2021.
[34] Mentasti, 2020.
[35] Reed, 2012.

filings, SPID gives residents a single digital identity.[36] Italy hopes to improve SPID's efficiency, security, and transparency while maintaining GDPR compliance by implementing blockchain technology.

Decentralised identity management, which enables users to manage their personal data and share it with both public and private entities selectively, is the core of blockchain's function in SPID.[37] For instance, a citizen can visit a healthcare site using their SPID credentials, giving the provider access to particular medical details without disclosing their complete identity. Since people still have control over their information, this is in line with the GDPR's principles of user permission and data minimisation.

Blockchain integration with SPID has not been without its difficulties, though. The tension between centralised oversight and decentralisation is one of the main issues. Although the decentralised structure of blockchain improves security and transparency, it makes it more difficult to enforce the accountability requirements of the GDPR, especially when it comes to identifying data controllers and processors.[38] In order to solve this, Italy has put in place hybrid models that guarantee compliance without compromising the fundamental ideas of the technology by combining blockchain with centralised oversight mechanisms.

IV. DISCUSSION

The immutability of the blockchain and its inconsistency with the GDPR's Right to be Forgotten (Article 17) are among the most controversial topics in the discussion between the two laws. Blockchain proponents contend that immutability is a fundamental characteristic that guarantees data confidentiality and integrity, making it essential for uses such as supply chain management and financial transactions. As Satoshi Nakamoto originally proposed in the Bitcoin whitepaper,[39] its core value lies in its capacity to prevent unathorized data alterations, hence increasing trustless security mechanisms. However, critics contend that there is a fundamental inconsistency between the two since immutability directly conflicts with GDPR's demand for data erasure. Michele Finck in *Blockchain Regulation and Governance in Europe*[40] claims that simple technical modifications are insufficient to address the fundamental legal incompatibility this conflict presents. Furthermore, blockchain's resistance to change can make it difficult for regulators to intervene, which presents challenges for both data protection authorities and individuals attempting to enforce their privacy

[36] Mentasti, 2020.
[37] Hong – Kim, 2020, 1238.
[38] Torres, 2018.
[39] Nakatomo, 2009
[40] Finck, 2019.

rights, as Karen Yeung and Martin Lodge point out in Algorithmic Regulation.[41]

In Blockchain and the New Architecture of Trust, Werbach challenges this view, arguing that the conflict between immutability and GDPR is not absolute because new cryptographic techniques like chameleon hashes and zero-knowledge proofs can allow for GDPR data erasure requirements to be met without sacrificing blockchain's essential features.[42]

Blockchain's immutability is one of its distinguishing features, but its not absolute. Off-chain storage and changeable blockchains are two solutions that have been put up to deal with this problem. BigchainDB's hybrid architecture, for instance, permits restricted data alteration, facilitating adherence to GDPR's erasure regulations without jeopardising the ledger's integrity.[43] As Finck explains, permissioned and mutable blockchain systems like BigchainDB introduce additional regulatory flexibility, that increases their capability to adjust to data protection regulations.[44] These answers, however, make it unclear if these systems are still legitimate blockchains or if they are an entirely distinct kind of technologies. Werbach points out that altering the immutability of blockchain for legal compliance could lead to 'blockchains in name only,' which could undermine the security and decentralisation guarantees that give the technology its value.[45]

Data erasure is still difficult to implement practically, even with malleable blockchains. To remove data from a blockchain, for instance, all parties may need to agree, which is challenging in decentralised networks.[46] Furthermore, as re-identified data would still be liable for GDPR's obligations, the possibility of data re-identification by hashing or encryption compromises the efficacy of these solutions.

The conflict between the decentralised nature of blockchain technology and the accountability requirements of GDPR is another important issue. Since decentralisation reduces single points of failure and increases transparency, it is frequently viewed as a strength of blockchain technology.[47] However, in decentralised systems where accountability is shared among several parties, it is challenging to identify data controllers and processors as required by GDPR (Article 4).

By highlighting the necessity of transparent governance structures in blockchain networks, Italy's legislative framework offers a possible remedy for this issue.[48] For instance, procedures for identifying data controllers and processors are part of Italy's blockchain integration with SPID, guaranteeing adherence to

[41] Yeung – Lodge, 2019.
[42] Werbach, 2018.
[43] BigchainDB, 2020.
[44] Finck, 2019.
[45] Werbach, 2018.
[46] Voight – von dem Busche, 2017.
[47] Sosztek, 2019.
[48] Garante per la Protezione dei Dati Personali: Annual Report on Emerging Technologies, 2021.

the accountability requirements of the GDPR. This strategy shows that accountability and decentralisation are not compatible.

Although Italy's efforts provide insightful information, they also draw attention to the drawbacks of implementing centralised oversight in decentralised systems. The fundamental tenets of deecentralisaion, like autonomy and resistance to censorship, may be compromised by hybrid models that blend blockchain by hybrid models that blend blokcchain technology with centralised processes.[49] Furthermore, businesses that operate in several jurisdictions face ambiguity due to the absence of unified EU-wide regulations, which makes achieving GDPR compliance more difficult.

V. CONCLUSION

One of the most pressing challenges and issues facing the digital age is the convergence of blockchain technology with the GDPR. The research of this study was to determine whether the inherent characteristics of blockchain–decentralization, immutability, and transparency–could be balanced with the data protection requirements of the GDPR, namely the Right to be Forgotten and accountability duties.

Through document analysis and case studies, this research demonstrated that although the immutability of blockchain presents difficulties for data erasure requirements, new solutions and critical initiatives like permissioned networks (BigchainDB) and off-chain storage (Italy's legal system) offer workable routes to compliance, and highlight the difficulties and constraints in bringing these two paradigms into harmony. The main takeaways from the analysis are summarised in this last chapter, which also considers the wider ramifications and suggests possible future directions.

The dispute between blockchain and the GDPR is a microcosm of the larger issues brought on by the quick speed of technical advancement. Although there are many obstacles in the way, there are also chances for advancement, cooperation, and creativity. Stakeholders can maximise the potential of blockchain technology while preserving people's fundamental rights by tackling these issues head-on. The lessons learnt from the blockchain-GDPR controversy will be crucial in determining how technology and regulations develop in the future as the digital world changes.

[49] Li – Jiang – Chen, 2017.

REFERENCES

- Bashir, Imran (2022): *Mastering blockchain. A technical reference guide to the inner workings of blockchain, from cryptography to DeFi and NFTs*. 4th Edition. Packt Publishing Ltd., Birmingham, United Kingdom. ISBN: 1803241063,9781803241067.
- Bernal, Paul (2018): *The Internet, Warts and All: Free Speech, Privacy, and Truth*. Cambridge University Press, Cambridge.
DOI: https://doi.org/10.1017/9781108381161.002.
- BigchainDB: BigchainDB Whitepaper, 2020. (Available at: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf. Accessed on: 26 January, 2025).
- BigchainDB: BigchainDB 2.0: *The Blockchain Database, 2020*. (Available at: https://www.bigchaindb.com/. Accessed on: 26 January, 2025).
- Case C-311/18. Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrem. Judgment of the Court (Grand Chamber) of 16 July 2020, ECLI:EU:C:2020:559. (Available at: https://curia.europa.eu/juris/liste.jsf?num=C-311/18. Accessed on: 26 January, 2025).
- CJEU: Google Spain v. Agencia Española de Protección de Datos (AEPD), 2014. Case C-131/12. (Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex-:62012CJ0131. Accessed on: 26 January, 2025).
- EU Blockchain Observatory and Forum: *Blockchain and the GDPR*. European Commission.
- European Blockchain Partnership (2018): *Declaration on European Partnership on Blockchain*. (Available at: https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership. Accessed on: 26 January, 2025).
- Finck, Michéle (2018): *Blockchain Regulation and Governance in Europe*. *Blockchains and the General Data Protection Regulation.* Cambidge University Press, Cambridge. DOI: https://doi.org/10.1017/9781108609708.
- Garante per la Protezione dei Dati Personali: Annual Report on Emerging Technologies, 2021. (Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9906288. Accessed on: 26 January, 2025).
- General data protection regulation. Regulation (EU), 679. (Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. (Accessed on: 26 January, 2025).
- Greenleaf, Graham (2021): Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. In: *Privacy Laws & Business International Report*. (Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836348. Accessed on: 26 January, 2025). DOI: https://doi.org/10.2139/ssrn.3836348.
- Hong, Seong-Ho – Kim, Heeyoul (2020): Vaultpoint: A blockchain-based SSI model that complies with OAuth 2.0. In: *Electronics*. 9(8) (Available at: https://www.mdpi.com/2079-9292/9/8/1231. Accessed on: 26 January, 2025).
DOI: https://doi.org/10.3390/electronics9081231.
- Kuner, Christopher (2012): The European Commission's proposed Data Protection Regulation: A Copernican revolution in European data protection law. In: *Bloomberg BNA Privacy and Security Law Report*. 11(6). (Available at: https://news.bloomberglaw.com/tech-and-telecom-law/the-european-commissions-proposed-data-protection-regulation-a-copernican-revolution-in-european-data-protection-law-1. Accessed on: 26 January, 2025).
- Li, Xiaoqi – Jiang, Peng – Chen, Ting et al. (2017): A Survey on the Security of Blockchain Systems. In: *Future Generation Computer Systems.* 107(2017).
DOI: https://doi.org/ 10.1016/j.future.2017.08.020.

- Lloyd, Ian J. (2020): *Information Technology Law*. 9th ed., Oxford University Press, Oxford. DOI: https://doi.org/10.1093/he/9780198787556.001.0001.
- Lopes, Dayani Christina Ferreira – de Castro, André Luis – Russo, Letíca Xander (2024): Blockchain technology: Challenges and opportunities in public finance. In: *RAM. Revista de Administração Mackenzie*. 25(3). eRAMR240208. (Available at: https://www.scielo.br/j/ram/a/sn7fFDhmqpWWP7BKHzRqtXn/?format=pdf&lang=en. Accessed on: 26 January, 2025).
DOI: https://doi.org/10.1590/1678-6971/eramr240208.
- McConaghy, Trent – Marques, Rodolphe – Müller, Andreas – De Jonghe, Dimitri – McConaghy, Troy T. – McMullen, Greg – Henderson, Ryan – Bellemare, Sylvain – Granzotto, Alberto (2016): *BigchainDB: A scalable blockchain database*. White Paper. (Available at: https://gamma.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf. (Accessed on: 26 January, 2025).
- Mentasti, Enrico (2020): Digital Identity in Italy: challenges and opportunities for the adoption in banking, insurance and utility sectors. In: *POLITesi - Archivio digitale delle tesi di laurea e di dottorato.* (Available at: https://www.politesi.polimi.it/retrieve/36b1ca60-893f-4071-83e9-6123d1a0ca42/2022_Giugno_Mentasti.pdf. Accessed on: 26 January, 2025).
- Nakamoto, Satoshi (2009): *Bitcoin: A Peer-to-Peer Electronic Cash System*. (Available at: https://bitcoin.org/bitcoin.pdf. Accessed on: 26 January, 2025).
- Reed, Chris (2012). *Making Laws for Cyberspace*. Oxford University Press, Oxford.
- Rosen, Jeffrey (2012): The Right to be Forgotten. In: *Stanford Law Review Online*. 64(2012). A(vailable at: https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf. Accessed on: 26 January, 2025).
- Szostek, Dariusz (2019): *Blockchain and the Law*. Nomos Verlagsgesellschaft, Baden-Baden. Available at: https://opus.us.edu.pl/info/book/USL53e046269db64d1c8ebe-41f47aad0595/ . Accessed on: 26 January, 2025).
DOI: https://doi.org/10.5771/9783845298290.
- Torress, Aura Cristina (2018): *Service Design and Blockchain For Digital ID*. Product Service System Design MSC AA. 2017/2018.
- Voigt, Paul – von dem Bussche, Axel (2017): *The EU General Data Protection Regulation (GDPR). A Practical Guide*. 1st ed.. Springer International Publishing, Cham. DOI: https://doi.org/10.3152676 (2017): 10-5555.
- Weber, Rolf H. – Staiger, Dominic N. (2020): Enforcing privacy through individual data access rights: A comparative study. In: Koltay, András – Wragg, Paul (eds.): *Comparative privacy and defamation*. Edward Elgar Publishing, Cheltenham and Camberley, United Kingdom. DOI: https://doi.org/10.4337/9781788970594.00022.
- Weber, Rolf H. (2011): The Right to be Forgotten: More than a Pandora's Box? In: *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2(2). (Available at: https://www.jipitec.eu/jipitec/article/view/73. Accessed on: 26 January, 2025).
- Werbach, Kevin (2018): *Blockchain and the New Architecture of Trust*. MIT Press, Cambridge, Massachusetts, United States
DOI: https://doi.org/10.7551/mitpress/11449.001.0001.
- Yeung, Karen – Lodge, Martin (eds.): *Algorithmic regulation*. Oxford University Press, Oxford.
DOI: https://doi.org/10.1093/oso/9780198838494.003.0001.
- Zavolokina, Liudmila – Ziolkowksi, Rafael – Bauer, Ingrid – Schwabe, Gerhard (2020): Management, Governance and Value Creation in a Blockchain Consortium. In: *MIS Quarterly Executive*. Vol. 19/2020.
DOI: https://doi.org/10.17705/2msqe.00022.