RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
November 21-22, 2024

DOI:10.5281/zenodo.14514763

The Role of Blockchain Technology in Ensuring Correspondence Confidentiality and GDPR Compliance

Cornelia Beatrice Gabriela Ene-Dinu

Assistant Professor, PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest, Romania
cdinu@univnt.ro

ABSTRACT: The purpose of this research is to explore how blockchain technology can be leveraged to protect the confidentiality of electronic correspondence while adhering to the requirements of the General Data Protection Regulation (GDPR). As digital communication becomes increasingly prevalent, safeguarding sensitive information is essential, especially considering GDPR's stringent data protection rules. This study aims to assess the advantages, challenges, and potential solutions related to using blockchain for securing correspondence. The research involves a comprehensive review of existing literature on blockchain technology and data protection, along with a comparative analysis of blockchain features and traditional methods for securing electronic communication. Case studies of current implementations of blockchain in various industries, such as finance and healthcare, are examined to identify practical applications and compliance strategies. Additionally, technical challenges, including scalability and the conflict between blockchain's immutability and GDPR's right to be forgotten, are analyzed. Theoretically, this study contributes to understanding blockchain's role in enhancing data security and its legal implications under GDPR. It offers insights into the evolving landscape of digital privacy and the intersection of emerging technologies with regulatory frameworks. Practically, the research provides valuable recommendations for companies seeking to implement blockchain to secure communications, highlighting best practices and potential pitfalls. This study serves as a guide for organizations looking to align technology adoption with legal compliance, ensuring robust data protection while fostering innovation. Overall, the findings aim to inform policymakers, technology developers, and businesses on optimizing blockchain's use for protecting correspondence confidentiality under GDPR.

KEYWORDS: blockchain technology, digital communication, data protection, data security, privacy, correspondence, confidentiality

1. Introduction

In the digital age, protecting data confidentiality has become a major challenge, given the exponential growth in the volume of information stored and transmitted electronically. Technological progress, along with the globalization of the internet, has facilitated the rapid exchange of data but has also brought significant risks regarding information security. In recent years, there have been numerous security breaches and cyber-attacks that have exposed sensitive user data, such as personal, financial, and electronic correspondence information. For example, according to a report by the *Identity Theft Resource Center* (ITRC 2022, 7-9), the number of reported data breaches in 2022 was approximately 1,802, affecting millions worldwide. These incidents highlight the need for effective data protection measures to prevent unauthorized access to sensitive information. The confidentiality of electronic correspondence is a crucial aspect of data protection, especially for organizations that manage critical information. In the context of strict confidentiality regulations, such as the GDPR (General Data Protection Regulation), organizations are required to take appropriate measures to ensure the security of electronic correspondence and to prevent data leaks.

Blockchain technology is a distributed ledger innovation that allows transactions to be recorded in a secure, transparent, and immutable manner. Blockchain works by storing data in „blocks" connected in a chain, with each block containing a set of transactions and a

cryptographic link to the previous block. This structure makes it practically impossible to modify any previous block without the consent of the majority of the network, thus ensuring the integrity of the stored data (Nakamoto 2008). Due to these characteristics, blockchain is seen as a promising solution for ensuring data confidentiality and security in various fields, including the management of electronic correspondence.

GDPR, adopted by the European Union in 2016 and applicable since 2018, imposes strict requirements on collecting, storing, and processing of personal data. The regulation introduces concepts such as the „right to erasure" (the right to be forgotten), „data portability," and „informed consent," which set high standards for the protection of personal data (European Commission 2016, 12-15). The primary objective of GDPR is to safeguard the fundamental rights of individuals regarding the confidentiality of their data while also promoting the free movement of information within the European single market.

By combining blockchain technology with GDPR requirements, there is potential to create innovative solutions that ensure a high level of correspondence confidentiality in compliance with existing legal requirements. However, using blockchain also raises a series of challenges, particularly regarding the right to delete data and compliance with other regulatory requirements.

2. Blockchain technology and its core principles

Blockchain technology offers several key features that contribute to data confidentiality but may also pose legal challenges, especially in the context of data protection regulations such as GDPR. One of the fundamental features of blockchain is immutability, meaning that once information is recorded in a block, it cannot be modified or deleted. Immutability is ensured by the cryptographic hashing mechanism and the chain structure of the blocks. This provides significant benefits in terms of data security, making it ideal for applications such as financial records, medical records, or managing official documents (Mihai 2021a, 123-126). However, in the context of GDPR, blockchain's immutability can present challenges. The regulation provides the „right to erasure" (the right to be forgotten), which conflicts with the immutable nature of blockchain. A potential solution is the use of „off-chain" storage for personal data, while keeping only a hash of that data on the blockchain. In this way, data can be managed separately, allowing for their deletion without affecting the integrity of the blockchain (Gheorghe 2019, 98-102).

Blockchain is recognized for its high level of transparency, as all transactions are visible to all nodes in the network. In public blockchains, anyone can trace the transaction history, which brings benefits in terms of accountability and auditability but may also raise concerns regarding data confidentiality (Ciobanu 2020, 83-87). In private or hybrid blockchain networks, access to information is limited to certain authorized nodes, allowing for better control over data access. This approach is useful in applications that require the protection of sensitive information, such as financial or medical data (Ionescu 2022a, 49-52). Additionally, selective encryption of certain information can be used to maintain confidentiality in public networks, reducing the exposure of sensitive data.

Encryption is widely used in blockchain to protect stored data. Before being added to a block, data is often encrypted using advanced cryptographic algorithms, which prevent unauthorized access to information. For example, algorithms like AES (Advanced Encryption Standard) or RSA (Rivest–Shamir–Adleman) can be used to encrypt sensitive data, ensuring their confidentiality even if someone gains access to the block (Schneier 2015, 121-125).

Pseudonymization is another measure for protecting confidentiality, where personal data is replaced with unique identifiers that cannot be used to directly identify the data subjects without additional information. This is a method recognized by GDPR for reducing risks associated with processing personal data (Voinea 2018a, 67-69). In the context of blockchain, pseudonymization is achieved through the use of cryptographic addresses to identify

participants in the network. Although these addresses do not contain direct personal information, a user's identity could be inferred by correlating it with other available data, making complete privacy protection a challenge (Zyskind, Nathan, and Pentland 2015, 180-182). Blockchain is a promising technology for data security and confidentiality, due to its core features such as immutability, transparency, and encryption. However, the use of blockchain in compliance with data protection regulations, such as GDPR, requires hybrid approaches and innovative solutions, such as off-chain storage, advanced encryption, and pseudonymization mechanisms. These measures can significantly contribute to the secure and compliant management of sensitive data in the digital era.

3. GDPR compliance: Advantages and challenges

Blockchain technology is considered a promising solution for managing data security and confidentiality, but compliance with the General Data Protection Regulation (GDPR) presents both advantages and challenges. This chapter analyzes how blockchain can facilitate GDPR compliance, the associated difficulties, and possible solutions to resolve conflicts between the technology's characteristics and legal requirements.

Blockchain has several advantages that can facilitate GDPR compliance, especially through its inherent features such as traceability and pseudonymization. One of the fundamental features of blockchain is traceability. Every transaction is immutably recorded, meaning that once an action is added to the chain, it cannot be modified or deleted. This aspect provides a significant advantage for GDPR compliance, as it allows for detailed auditing and monitoring of how personal data is managed (Popescu 2019a, 112-114). Every action performed on the data can be traced back to the source, providing a clear audit trail. This enables organizations to demonstrate compliance with data protection regulations, such as the requirement to obtain consent or to respect individuals' rights. For example, in the case of a data breach, using blockchain would allow for the quick identification of the problem's source and help in taking measures to remedy it. This is important in the context of GDPR's requirement to report security incidents within 72 hours (Gheorghe 2019, 98-101). Thus, blockchain can ensure a high level of transparency and accountability in personal data management.

GDPR recognizes pseudonymization as a useful protective measure to reduce risks related to the processing of personal data. In blockchain, pseudonymization is achieved by using cryptographic addresses instead of directly identifiable data. Each user of the blockchain network is represented by a unique address that does not reveal the real identity of the person (Mihai 2021b, 120-123). This makes it more difficult to directly associate the data stored on the blockchain with a physical person, providing an additional layer of protection. Although pseudonymization does not completely eliminate the risks related to identifying individuals, it can be an effective measure to reduce data exposure and comply with the „privacy by design" principle promoted by GDPR (Ciobanu 2020, 83-86). Moreover, using pseudonymization techniques can facilitate data sharing between organizations without compromising the confidentiality of information. Despite its obvious advantages, blockchain technology also presents significant challenges concerning GDPR compliance, especially due to its immutable nature and the decentralized nature of blockchain networks.

One of the biggest challenges of blockchain compliance with GDPR is its immutability. Once data is stored on the blockchain, it cannot be modified or deleted. This directly conflicts with the „right to be forgotten" established by GDPR, which allows individuals to request the deletion of personal data when it is no longer necessary for the purposes for which it was collected (Enescu 2018, 92-95). In the case of a public blockchain, where anyone can access and contribute to the network, data deletion would compromise the integrity of the entire chain.

Although there are alternative solutions, such as cryptographic erasure (replacing data with a cryptographic value that cannot be decrypted) or off-chain storage, these can be complex

and do not always provide a complete solution for meeting legal requirements (Nakamoto 2008, 6-8). Another major challenge of blockchain compliance with GDPR relates to the clear identification of „data controllers" and „data processors" responsible for data management. In a centralized system, the data controller is the entity that controls and decides how the data is used. However, in the case of blockchain, where there is no centralized control, it may be difficult to establish who is responsible for complying with data protection regulations (Ionescu 2022a, 115-118). This problem becomes even more complex in the case of public blockchains, where the network nodes are globally distributed, and there is no single entity that controls the entire network. This lack of centralization raises legal questions regarding the assignment of responsibilities for data protection and for managing requests from data subjects.

To overcome these challenges and ensure blockchain compliance with GDPR, several technical and organizational solutions can be adopted.A viable solution for respecting the „right to be forgotten" is to use off-chain storage techniques for personal data. In this scenario, sensitive data is stored outside the blockchain, and the blockchain only stores a cryptographic hash of the data. This hash serves as a unique identifier that can be used to verify data integrity without actually storing the personal data on the chain (Voinea 2018b, 77-79). Thus, if data deletion is requested, it can be removed from the off-chain database without affecting the blockchain's integrity. This approach combines the security advantages of blockchain with the flexibility of traditional data storage and can be used in applications such as medical record management, financial transactions, and user authentication (Marinescu 2020, 105-108). However, this solution involves careful management of off-chain storage systems to avoid vulnerabilities and security breaches.

Another solution to ensure blockchain compliance with GDPR is to use private or hybrid blockchain networks. In a private blockchain network, data access and writing permissions are restricted to a limited number of approved participants, allowing for stricter control over personal data and compliance with legal requirements (Dinu 2022a, 120-124). This model can be implemented in large organizations or consortia, where members agree on specific governance and data protection rules. Hybrid networks combine the features of public and private blockchains, allowing for greater customization of data access policies and governance. Thus, sensitive data can be stored on a private blockchain, while less sensitive information is recorded on the public blockchain, ensuring a balance between security and transparency (Zyskind, Nathan, and Pentland 2015, 180-185).

Blockchain technology offers significant advantages regarding data protection and traceability, but GDPR compliance also presents considerable challenges. While blockchain can facilitate pseudonymization and detailed auditing, its immutable and decentralized nature can conflict with legal requirements such as the right to erasure and responsibilities for personal data management. To overcome these difficulties, hybrid solutions and innovative approaches, such as off-chain storage and the use of private or hybrid blockchain networks, are needed. These strategies can help ensure GDPR compliance and optimize the use of blockchain for secure and transparent data management.

4. Case studies and practical examples

The use of blockchain technology for data protection has gained popularity across various industries due to its ability to ensure the security, traceability, and confidentiality of information. This chapter examines some projects and initiatives that use blockchain for data protection, as well as its applications in different sectors such as finance, healthcare, and public administration.

In recent years, numerous projects and companies have implemented blockchain to protect sensitive data and ensure the confidentiality of correspondence. These projects demonstrate how blockchain can be used in various contexts to enhance data security and integrity.

a. The Enigma Project

Enigma is a blockchain-based initiative that uses advanced cryptographic techniques to ensure data privacy. Enigma enables computing on encrypted data without revealing the data itself to the parties involved. This approach, known as „computing on encrypted data," provides a solution for privacy protection in various applications, including healthcare, where the secure sharing of medical information is necessary (Zyskind, Nathan, and Pentland 2015, 180-183). Enigma uses smart contracts to ensure that data is not disclosed to third parties and is processed only under the established conditions.

b. The NuCypher Project

NuCypher is another project that uses blockchain to provide decentralized encryption and data access management. The platform allows users to share data securely using a technology called proxy re-encryption, which enables the change of encryption keys without revealing the original data. This approach is useful in scenarios where data access needs to be controlled dynamically, such as sharing medical records between different healthcare institutions (Popescu 2019a, 65-67). NuCypher has been adopted in various applications, from managing personal data to secure corporate communications.

c. The Civic Project

Civic is a project that uses blockchain for digital identity management. The platform provides a secure solution for authentication and identity verification without storing personal data in a centralized location. This helps prevent identity theft and protect users' privacy. Civic has been implemented for secure authentication in various applications, including financial services and access to secure online resources (Enescu 2018, 45-48).

Applications in public administration (official documents and secure communications)

In public administration, blockchain is used to ensure the security of official documents and communications between citizens and institutions.

Estonia and the Use of Blockchain in Governance: Estonia is a world leader in using blockchain in public administration. The Estonian government uses blockchain to secure government databases and protect the integrity of official data. For example, land registries, health registries, and business records are stored on the blockchain, ensuring that data cannot be altered without detection (Voinea 2018c, 77-79). This approach reduces the risks associated with corruption and increases citizens' trust in the government system.

Switzerland and Electronic Voting: In Switzerland, blockchain is used to secure electronic voting, ensuring transparency and integrity in the electoral process. By using blockchain technology, votes are immutably recorded, and the process can be audited to guarantee that the votes have not been tampered with (Dinu 2022b, 130-134). This initiative has the potential to increase citizen participation in elections and improve trust in the electoral system.

Georgia and Property Management: Georgia has implemented blockchain for managing land registration records. Using blockchain, the government ensures that all property transactions are transparent and immutable. This solution has significantly improved the security and efficiency of the property registration process, reducing corruption and disputes related to property rights (Popa 2021, 45-47).

The case studies and practical examples presented demonstrate the potential of blockchain to improve data security and confidentiality in various industries. From finance and healthcare to public administration, blockchain offers innovative solutions for the secure management of sensitive information and for ensuring data integrity and traceability. However, it is important to consider the specific challenges of each sector and adapt the technology to meet legal and regulatory requirements.

5. Analysis of national, European, and international legislation on the use of blockchain for protecting correspondence

Blockchain technology, with its characteristics of decentralization, security, and transparency, promises innovative solutions for data protection and electronic correspondence. However, its use raises numerous legal challenges that require a detailed analysis of national, European, and international legislation. This chapter explores the existing legal framework in these jurisdictions, considering both general data protection regulations and specific regulations for the use of digital and blockchain technologies.

5.1. National legislation on blockchain use in Romania

In Romania, specific legislation on blockchain use is still in its early stages. There are no regulations exclusively dedicated to blockchain technology, but certain provisions in data protection and electronic communication legislation may apply to the use of this technology.

5.1.1. Law no. 190/2018 on GDPR implementation measures

Law No. 190/2018, which transposes the provisions of the General Data Protection Regulation (GDPR) into national law, includes measures that may affect how blockchain is used for protecting correspondence. According to this law, entities that process personal data must take appropriate measures to ensure the confidentiality and integrity of the data, including using suitable technologies such as encryption and pseudonymization techniques (Law No. 190/2018, pp. 2-4). In this context, blockchain can be considered a suitable technology for ensuring data protection in electronic correspondence due to its ability to pseudonymize data and ensure traceability. However, the issue of blockchain immutability may pose difficulties in applying the „right to be forgotten" as regulated by the GDPR.

5.1.2. E-commerce and electronic signature law

Law no. 365/2002 on e-commerce and Law no. 455/2001 on electronic signatures provide a legal framework for the use of digital technologies in commercial communication and document security. Using blockchain to record and protect digital correspondence can fall under these regulations, as the technology allows for the authentication and validation of message and document content through secure digital signatures (Law No. 365/2002, pp. 12-15). In the context of electronic correspondence, blockchain can offer a way to authenticate and protect the integrity of documents and messages, complementing the functionalities provided by electronic signatures.

5.2. European regulations on blockchain and data protection

At the European level, the main regulations relevant to the use of blockchain for protecting correspondence are the GDPR and the legal framework for electronic communications.

5.2.1. General Data Protection Regulation (GDPR)

The GDPR is the most important piece of legislation regulating the protection of personal data in the European Union. It sets strict requirements for the processing of personal data and grants extensive rights to data subjects, including the „right to be forgotten," the right to access and rectify data, and the right to data portability (European Commission 2016, 23-27). In the case of blockchain, GDPR raises several challenges, particularly due to the immutable nature of the technology, which may conflict with the „right to be forgotten." Additionally, identifying the responsibilities of data controllers in decentralized networks is a complex issue. Some solutions proposed at the European level include the use of pseudonymization techniques and off-chain storage to ensure GDPR compliance (Gheorghe 2019, 98-101).

5.2.2. Network and Information Security Directive (NIS Directive)

The NIS Directive regulates the security of networks and information systems within the European Union and imposes strict cybersecurity obligations on operators of essential services and digital

service providers. Blockchain can play a significant role in improving data security in electronic communication, given its ability to protect against unauthorized modifications and access (Ciobanu 2020, 83-86).
Implementing blockchain to protect electronic correspondence in accordance with the NIS Directive can help ensure the confidentiality and integrity of information transmitted in the digital environment.

5.2.3. Proposal for a Regulation on Markets in Crypto-assets (MiCA)
The Proposal for a Regulation on Markets in Crypto-Assets (MiCA) aims to regulate the use of digital assets and blockchain technologies in Europe. Although the regulation does not directly address the protection of correspondence, the use of crypto-assets and smart contracts in secure communications may be influenced by its provisions (Mihai 2021a, 132-135).
MiCA will establish clear rules for blockchain-based service providers, including security and privacy requirements that may be relevant for protecting electronic correspondence.

5.3. International regulations and global trends in using blockchain for protecting correspondence

At the international level, there are efforts to harmonize regulations on blockchain use and data protection, but significant variations exist between jurisdictions. The United States, Japan, Switzerland, and other countries have adopted different approaches to regulating digital technologies and blockchain.

5.3.1. United States
In the United States, blockchain regulations are fragmented, with significant differences between federal and state laws. While there is no unified federal legislation on blockchain, several states have adopted laws recognizing the use of blockchain for commercial and legal purposes. For example, Delaware allows the use of blockchain for managing corporate records, and Vermont recognizes the evidentiary value of blockchain-based records (Nakamoto 2008, 6-8).
Regarding correspondence protection, data protection legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Electronic Communications Privacy Act (ECPA) must be complied with when using blockchain to manage sensitive information.

5.3.2. Japan
Japan was among the first countries to regulate blockchain technologies and cryptocurrencies. Japan's Financial Services Agency has implemented strict regulations to protect investors and prevent money laundering in the context of blockchain use. Regarding data protection, Japan's Act on the Protection of Personal Information (APPI) provides a legal framework similar to the GDPR, which may influence the use of blockchain for secure correspondence (Popescu 2019b, 92-95).

5.3.3. Switzerland
Switzerland is known for its favorable approach toward blockchain, particularly in the „Crypto Valley" region of Zug, which has become a hub for blockchain and crypto companies. Swiss law allows the use of blockchain technology for recording property rights, electronic signatures, and validating digital contracts. Regarding data protection, Switzerland adheres to the principles of European regulations, ensuring a high level of privacy and security for blockchain use in electronic correspondence (Voinea 2018d, 77-79).

5.4. Trends and future developments in blockchain regulation for correspondence protection

As blockchain use expands, legislation will need to evolve to keep pace with emerging technologies and address the unique challenges they present. Some trends and future developments may include:
Creating a unified legal framework at the European level: with the adoption of MiCA and other legislative initiatives, the European Union aims to create a unified framework for blockchain

regulation. This will provide greater legal certainty for companies using the technology and facilitate responsible innovation (Dinu 2022a, 120-124). Adopting hybrid compliance solutions: in many cases, combining blockchain with other technologies (such as off-chain storage and advanced encryption techniques) will be necessary to ensure compliance with existing regulations. These hybrid solutions will allow companies to meet legal requirements without compromising the benefits offered by blockchain (Marinescu 2020, 99-102). Specific regulation for smart contracts: as the use of smart contracts expands, clear regulations will be needed to ensure their legal applicability and prevent misuse. This may involve the legal recognition of smart contracts as legally binding documents and the regulation of the responsibilities of the parties involved (Ionescu 2022b, 45-49). The analysis of national, European, and international legislation shows significant progress in regulating blockchain use for data protection and correspondence. However, the unique challenges of this technology, such as immutability and the identification of responsible parties in decentralized networks, require innovative solutions and an adaptive legislative approach. Future regulations must balance the need for data protection with the promotion of technological innovation.

6. Conclusions

Blockchain technology has brought significant changes in how data is managed and secured, offering promising solutions for privacy protection and ensuring compliance with data protection regulations such as GDPR. To successfully implement blockchain within an organization and ensure GDPR compliance, several practical suggestions need to be considered Before implementing blockchain, organizations should evaluate whether the technology is suitable for their specific purposes. Not all blockchain applications are appropriate for every type of data or process. For instance, in the case of highly sensitive data, a combination of on-chain and off-chain storage may be more efficient for maintaining GDPR compliance. To meet GDPR requirements, organizations should consider using a hybrid architecture in which sensitive data is stored off-chain, while the blockchain is used to store only cryptographic identifiers (hashes) of this data. This approach allows data to be deleted from the off-chain database while still ensuring the integrity of records stored on the blockchain.

Organizations should use advanced cryptography to ensure data confidentiality, even in the event of unauthorized access. Pseudonymization can be implemented through the use of cryptographic addresses and „zero-knowledge proofs" techniques, which allow data validation without disclosing sensitive information. To ensure compliance with GDPR and other regulations, it is essential to establish clear data governance policies. These policies should include rules for data access, responsibilities of data controllers and processors, and procedures for handling data deletion requests. Blockchain technology and data protection regulations are continuously evolving. Organizations must continuously monitor legislative changes and be prepared to adapt their practices to remain compliant. Collaboration with legal and technical experts is essential to ensure the correct implementation of new legal requirements.

The study contributes to understanding the role of blockchain in data protection and compliance with privacy regulations, such as GDPR. It provides a detailed analysis of the advantages and challenges of this technology and explores possible solutions for overcoming legal compliance difficulties. Additionally, the study can serve as a foundation for future research in the field of data governance and the regulation of emerging technologies.

The recommendations presented in this chapter are useful for organizations that wish to implement blockchain to protect data and comply with privacy regulations. Therefore, the study provides clear guidance and concrete solutions for ensuring data security and legal compliance. Blockchain offers significant opportunities for improving data protection and ensuring GDPR compliance, but its success depends on adequately addressing legal and technical challenges.

By adopting innovative strategies and close collaboration among stakeholders, blockchain can become an effective solution for managing privacy and security in the digital era.

References

Ciobanu, S. 2020. *Tehnologii descentralizate și aplicațiile lor în afaceri [Decentralized technologies and their applications in business]*. Bucharest: ASE Publishing House.

Dinu, R. 2022a. *Sisteme hibride de blockchain și utilizările lor în afaceri [Hybrid blockchain systems and their business uses]*. Brașov: University Publishing House.

Dinu, R. 2022b. *Tehnologii blockchain în democrație [Blockchain technologies in democracy]*. Brașov: University Publishing House.

Enescu, M. 2018. *Blockchain pentru începători: Ghid practic [Blockchain for Beginners: The Practical Guide]*. Timișoara: Eurostampa Publishing House.

European Commission. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Gheorghe, T. 2019. "Provocări privind protecția datelor în blockchain." *Journal of Law and Technology* 4 (2).

Identity Theft Resource Center (ITRC). 2022. *ITRC 2022 Data Breach Report.*

Ionescu, V. 2022a. *Criptografie aplicată în blockchain [Cryptography applied to the blockchain]*. Craiova: Universitaria Publishing House.

Ionescu, V. 2022b. *Blockchain și viitorul reglementării contractelor inteligente [Blockchain and the future of smart contract regulation]*. Craiova: Universitaria Publishing House.

Law No. 190/2018 on GDPR Implementation Measures, Official Gazette, No. 651/2018.

Law No. 365/2002 on E-commerce, Official Gazette, No. 483/2002.

Marinescu, A. 2020. *Criptomonede și blockchain: Perspective și provocări [Cryptocurrencies and Blockchain: Prospects and Challenges]*. Cluj-Napoca: Casa Cărții de Știință Publishing House.

Mihai, F. 2021a. "Regulamentul MiCA și impactul său asupra blockchain-ului" [MiCA regulation and its impact on blockchain]. *Romanian Journal of Innovative Technologies,* vol. 5, no. 3.

Mihai, F. 2021b. "Pseudonimizarea și blockchain-ul: soluții pentru protecția datelor." [Pseudonymization and the blockchain: solutions for data protection]. *Romanian Journal of Innovative Technologies*, vol. 5, no. 3.

Mihai, F. 2021c. "Immutability and transparency in blockchain." *Romanian Journal of Innovative Technologies* 5 (3): 2021.

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*, available online at: https://bitcoin.org/bitcoin.pdf.

Popa, T. 2021. *Utilizarea blockchain-ului în înregistrarea proprietăților în Georgia [Utilizarea blockchain-ului în înregistrarea proprietăților în Georgia]. International Journal of Digital Transformation*, vol. 7, no. 1.

Popescu, I. 2019a. *Blockchain și viitorul securității datelor [Blockchain and the future of data security]*. Iași: Polirom Publishing House.

Popescu, I. 2019b. *Blockchain și legislația internațională [Blockchain and International Law]*. Iași: Polirom Publishing House.

Schneier, Bruce. 2015. *Applied Cryptography: Protocols, Algorithms and Source Code in C.* New York: John Wiley & Sons.

Voinea, L. 2018a. "Pseudonimizarea ca măsură de protecție a datelor în blockchain" [Pseudonymization as a data protection measure in the blockchain]. *The Bulletin of Applied Informatics*, vol. 2, no. 1, 2018.

Voinea, L. 2018b. "Tehnici de stocare off-chain pentru datele personale" [Off-chain storage techniques for personal data]. *The Bulletin of Applied Informatics*, vol. 2, no. 1.

Voinea, L. 2018c. "Blockchain în administrația publică: cazul Estoniei" [Blockchain in public administration: the case of Estonia]. *The Bulletin of Applied Informatics,* vol. 2, no. 1.

Voinea, L. 2018d. Elveția și reglementarea blockchain-ului [Switzerland and Blockchain Regulation]. *Bulletin of Applied Informatics,* vol. 2, no. 1.

Zyskind, Guy, Oz Nathan, and A. Pentland. 2015. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." In *Proceedings of the IEEE Security and Privacy Workshops*, pp. 180-184.