Journal of Integrated Information Management

Vol 10, No 1 (2025)

Jan-June 2025

Innovations and Contradictions in Applying Blockchain Technology in Records Management under General Data Protection Regulation

Nikolaos Kareklas, Artemis Chaleplioglou

doi: 10.26265/jiim.v10i1.41216

To cite this article:

Kareklas, N., & Chaleplioglou, A. (2025). Innovations and Contradictions in Applying Blockchain Technology in Records Management under General Data Protection Regulation. *Journal of Integrated Information Management*, *10*(1), 49–58. https://doi.org/10.26265/jiim.v10i1.41216

Journal of Integrated Information Management electronic journal

Innovations and Contradictions in Applying Blockchain Technology in Records Management under General Data Protection Regulation

Nikolaos Kareklas, Artemis Chaleplioglou
Department of Archival, Library & Information Studies, University of West Attica, Athens, Greece
nkareklas@uniwa.gr [**ORCID**: 0009-0008-6228-5992], artemischal@uniwa.gr [**ORCID**: 0000-0002-6519-7428]

Article Info

Article history:
Received 28 April 2025
Received in revised form 12 May 2025
Accepted 02 June 2025

http://dx.doi.org/10.26265/jiim.v10i1.41216

Abstract:

Purpose – *This review aims to highlight the innovations and contradictions of Blockchain Technology applications in Records regarding the General Data Protection Regulation (GDPR) of the European Union (EU).*

Design/methodology/approach – *An extensive literature review was conducted, which revealed of many articles based on research into blockchain, most written from a legal perspective. This report focuses on the extent of analysis of the contradiction that exists between Blockchain information storage and international personal data protection legal requirements, with an emphasis on EU. The variety of proposed solutions to overcome this issue are discussed.*

Findings – *The incompatibility between blockchain technology and data privacy is because of three fundamental inconsistencies: (a) Data cannot be modified once inserted into a block, which conflicts with the right to delete and correct them; (b) Data is publicly available in each participant of the blockchain, a function that conflicts with the principles of confidentiality, accountability, and the designation of a central data processor; and (c) The data is stored indefinitely, in conflict with the GDPR principles related to the purpose, necessity and minimizing of information.*

Originality/value - *This paper presents an original analysis of the implications of adopting Blockchain in Records Management, as well as the implications arising from GDPR.*

Index Terms — Records management, Information Governance, Blockchain Technology, GDPR.

I. Introduction

The advancements in technology have led to an increase in better information management systems. One such system is blockchain, which refers to a digital method used to record information, making it difficult to cheat, modify, or hack [1]. Essentially, blockchain can also be defined as transactions that are duplicated or distributed across a large computer network. A set number of transactions characterizes each block within the chain. Essentially, ledgers are added whenever a transaction occurs within the entire blockchain [1]. Blockchain operates as a Decentralized Ledger Technology, allowing data management by many individuals. Blockchain is crucial in business management, as it simplifies traceability and verification of various commercial transactions, logistics, or product manipulations [2]. In this context, a multistep operation can be easily traced, making tracking and operations more efficient. Blockchain also secures transactions, accelerates data processing, and reduces compliance costs [1]. As an unchangeable digital ledger, blockchain prevents modifications that could lead to malpractices costing businesses. The encryption component also enhances security, preventing unauthorized access.

There are different types of blockchains, including public, hybrid, private, and sidechains. Public blockchains have no restrictions on people's access. Because they are permissionless, anyone with internet access can participate and perform transactions [1]. In contrast, private blockchains are controlled by permission rights, meaning unauthorized personnel cannot access them. Validator participation and open access are not allowed in this case [2]. For hybrid blockchains, both decentralized and centralized features are combined. There is a significant difference between blockchain for record management and blockchain used in general data protection regulation (GDPR) [1]. This review examines the differences between these two and how they relate to blockchain technology.

II. Methodology

This literature review aimed to examine whether blockchain technology can be effectively used in records management without infringing on the General Data Protection Regulation (GDPR) regulations. To investigate this, a thorough review of scholarly and technical sources was performed using reputable academic databases such as Google Scholar, Scopus, and Web of Science, among others. The chosen literature includes peer-reviewed journal articles, white papers, regulatory guidelines, and case

studies published between 2014 and 2025. This multi-source approach provided a well-rounded understanding of both the legal restrictions imposed by GDPR and the technical capabilities of blockchain to ensure transparency, security, and accountability in records management systems.

The primary focus was on technical articles addressing compatibility issues between blockchain transaction recording and the GDPR. Books were also considered to clarify the differences between the two study components. The main challenge encountered was finding material suitable for completing the literature review assignment. Few scholarly articles cover the topic of data management in blockchain. Most reports were irrelevant to this study's aims, making it difficult to find accurate materials. The following inclusion criteria were applied: first, articles were checked for relevance to the study topic; specifically, the report topics should include either blockchain in records management or blockchain and GDPR. Those that passed this criterion were examined for the second criterion, a publication date limit. Only books or papers published between 2012 and 2025 were considered. This chronological period was chosen because of its proximity to the preparation of the EU GDPR regulation, which was adopted on April 14, 2016, and became law on May 25, 2018. Credible data management reports, conference papers, and technology journals were prioritized based on their relevance to the topic.

The methodology also involved participating in seminars, conferences, and workshops on blockchain. In computer science, conference papers and workshops are regarded as equally credible as journal publications because they undergo thorough peer review. It is common for major blockchain advances to be presented at these events before appearing in journals.

III. Blockchain Technology in Records Management

As a distributed ledger, blockchain technology is fundamentally a records management technology [3]. Although the technical details of each platform vary significantly depending on the specific applications of blockchain, the primary purpose of this technology is to maintain valid digital documents that are resistant to violations of their transaction logs and transparent for subsequent review [4]. According to Vigna & Casey (2019) [5], the distinctive features of blockchain technology today make it a reliable platform for various social, economic, and political transactions and interactions. This perspective is echoed by Markey-Towler (2018) [6], who argue that blockchain is a revolutionary technology for records management, as it redistributes power flows and challenges the monopoly control of states and other traditional elites over public records.

A key issue in records management literature is the reliability of systems in ensuring accountability, especially given historical concerns that archives have often been shaped to serve dominant political and social interests rather than democratic transparency [7]. Therefore, guaranteeing archive validity is a critical prerequisite in many fields where management systems identify the essential infrastructures needed to achieve relevant goals [3]. This is vital for all organizations or industries that maintain archival records, such as public registers, cadastral records, and financial transaction repositories [8].

The two main challenges in public and academic debates about records' validity focus on their reliability and authenticity; two interconnected concepts that often overlap with integrity [9]. In the first case, record reliability begins with the process of creation, including conditions related to the creator and associated functions, as recognized by the ISO 15489 records management standard [10] and generally accepted ARMA recordkeeping principles [11]. According to standard 15489:2016, an accurate record is one whose contents can be considered reliable as a complete and precise representation of the transactions, activities, or events it verifies [10]. Similarly, authenticity depends on maintaining the identity and integrity of a record from the moment it is created onward [12]. As acknowledged by the standards above, ensuring integrity involves measures related to access control, user verification, fingerprint identification, and documentation demonstrating normal operation, routine maintenance, and the frequency of updates to recordkeeping information systems [10, 13].

According to Franks (2020) [14], this technology guarantees a reliable recording of data, such as ledgers related to transactions, agreements, events, and contracts, in an independent and verifiable manner. The digital signature in the blockchain is replaced by a series of letters and numbers (hash). Once a data set is logged in the ledger, altering or moving it becomes almost impossible. Each transaction (hash) must match the corresponding history log, making the blockchain a highly transparent platform [15].

The requirements for reliability and authenticity in blockchain systems are fulfilled by the following three main mechanisms:

(1) Incentive mechanism: Blockchain technology uses economic incentives to encourage honest behavior among participants, often through rewards like cryptocurrency tokens. These incentives aim to align individual actions with the collective goal of maintaining a trustworthy and secure system. Because participants understand that following the rules is financially beneficial, they tend to act independently while still adhering to the expected protocols. However, this mechanism faces criticism. Financial rewards can create ethical dilemmas, especially if individuals or coordinated groups exploit the system for personal gain. For example, so-called “51% attacks” — where an entity or coalition controls most of a network’s computational power — have happened in the past, notably against Bitcoin Gold (2018) and Ethereum Classic (2019). These attacks show that, while a single person likely can't compromise a blockchain from

home, well-funded organizations or state actors might be able to do so. Therefore, the resilience of blockchain is not absolute; it can be vulnerable to targeted manipulation depending on available computational resources, financial motivation, and intent. Ethereum's shift from proof-of-work to proof-of-stake in September 2022 shows an effort to decrease such vulnerabilities and strengthen the system.

(2) Record creation and keeping mechanism: this technology is designed to produce complete, definitive, and non-reproducible archival items using special encryption, thereby building a breach-resistant chain of proof of actions that occur.

(3) A decentralization mechanism: blockchain functions as a peer-to-peer distributed network, where participants typically act without the oversight of a central authority but instead operate autonomously while remaining coordinated through incentivization mechanisms. These incentives—often financial—raise ethical considerations, as the lack of supervision can blur the boundaries of responsible behavior. Although autonomy generally makes collusion more difficult, blockchain systems are not completely immune to coordinated manipulation. For example, a well-known vulnerability—the "51% attack"—happens when a single entity or a coalition controls the majority of the network's computational power, enabling it to alter the ledger and potentially validate fraudulent transactions. This challenges the idea that decentralization always guarantees integrity. However, under normal network conditions, the distributed nature of blockchain provides a solid basis for record validity and reduces many types of malicious activity [16, 9].

Blockchain systems utilize cryptographic file logs, rely on consent, and depend on distributive principles to finalize, complete, and stabilize records entered into the ledger [9]. Bhatia et al. (2020) [17] observed similar results in a recent study, which indicates that blockchain technology, when properly implemented, is a dependable solution for records management. It enables the recording of immutable transactions and offers independent control through digital documents that cannot be altered. Blockchain technology has been suggested as an effective solution for safeguarding privacy and security in managing records, transactions, and documents across various applications, such as payments, healthcare, and infrastructure developed for the Internet of Things (IoT) [18].

IV. Application of Blockchain in Records Management

The applications of blockchain technology in records management are a current research focus for many scholars, as this technology is increasingly viewed as a solution to recordkeeping issues where a reliable public ledger is needed. For example, Lemieux (2016) [3] uses blockchain applications in public identification services, title deed management, and financial transactions, arguing that this new technology can address longstanding problems related to information integrity and the reliability of active records. Franks (2020) [14], who analyzes case studies of blockchain applications in banking, healthcare, public services, and payment management, concludes that this technological solution aligns well with the fundamental principles of record management. At this point, it is important to note that blockchain applications, as discussed in more detail below, are often examined in relevant research literature in connection with "smart contracts" applications, i.e., digitized contracts with embedded IFTTT (if-this-then-that) code [19].

Among various blockchain applications in records management, those developed in healthcare stand out [20]. A limited but increasing number of studies have focused on this topic, highlighting blockchain's potential to improve patients' control over sensitive personal and medical data [21]. A study by Sunil & Sangamesh (2019) [22] describes specific uses of blockchain in healthcare, such as managing patients' medical histories, facilitating the pharmaceutical supply chain, and handling payments to healthcare providers. It argues that integrating blockchain into these functions provides important advantages in managing archival materials, including enhanced security, reliability, accessibility, and universal access. Harshini et al. (2019) [23] also introduce a human-centered record management model in healthcare using blockchain technology, emphasizing the need to implement smart contracts for exchanging medical data and increasing security in financial transactions between patients and healthcare providers.

Vaibhav et al. (2020) [24] confirm the previous need, arguing that implementing smart contracts in the healthcare industry significantly improves record management functions (e.g., insurance claims, clinical research, patient data security, pharmaceutical supply chain), leading to increased accuracy. Similarly, Sadiku et al. (2018) [25] contend that blockchain technology in health services is the right solution to enhance the quality of care provided to patients. Noh et al. (2017) [26] share similar findings, stating that blockchain platforms support the modern patient-centered healthcare approach. Specific blockchain applications in these functions are also documented in the literature. For example, Azaria et al. (2016) [27] analyzed the operation of MedRec, a new decentralized system for managing electronic patient records. This system gives patients access to a complete and unchangeable log of their records, while providers and healthcare organizations also have access. However, such shared access raises important ethical and legal concerns. For instance, insurance companies might use clinical data—such as a diabetes diagnosis—to enforce exclusion clauses or to increase premiums for related conditions like cardiovascular disease. This raises a critical question: is the sharing of clinical information truly in the patient's best interest, or does it mainly benefit insurers aiming to reduce financial risks?

Similarly, Medicalchain is another modern platform developed in the UK that uses encryption features (MedTokens) to handle payments and compensation in health services [28].

In addition to applications in healthcare, blockchain technology provides significant benefits in records management for public services [29]. For example, a study by Tasnim et al. (2018) [30] details a criminal record management platform designed to ensure maximum integrity and security of the data. By providing full access to authorities (law enforcement agencies and courts) and other users (e.g., airports, visa centers, police), this platform enhances capabilities for managing public criminal records, enabling prompt law enforcement and reducing the risk of corruption or breaches of criminal records in an environment of increased accountability.

The Vermont Digital Services (2019) [31] developed a blockchain platform for recording and managing land titles, which integrates previous electronic applications and allows responsible public bodies to control related transactions (e.g., sales, land repurposing), ensuring the reliability of active records. Similarly, a recent study by Thakur et al. (2020) [32] discusses the use of SAID technology to manage land ownership records in India, aiming to modernize the existing system by digitally connecting previously isolated services and improving the quality of property registration and transfer services. Comparable property management platforms are described both in the study by Lazuashvili et al. (2019) [33], focusing on the State of Georgia, and in a survey by Ramya et al. (2018) [34], covering Southeast Asian countries.

The potential of blockchain technology has been explored in other applications related to public administration, quality, and efficiency of public services, such as those related to handling and managing public certification documents (e.g., births and deaths), which can be made accessible to interested parties with the necessary security clearance [35]. Similar services have also been developed to record citizens' identities, property ownership, or migration flow data [36]. A study by Hyvärinen et al. (2017) [37] examines the application of blockchain technology to combat financial fraud or fraudulent waste of resources in public services, while another study by Elisa et al. (2018) [38] refers to respective applications offered by blockchain in identification services involving several governments, public and private entities.

Another area where blockchain technology and record management intersect is in finance, where suitable platforms can be used for activities such as transaction settlements, payments, and insurance claims [39, 40, 41], as well as in registration services (e.g., cadastre, civil register, tax register) [42, 43]. Recently, this new technology has become especially important in copyright registration services, where proving patent ownership and establishing registration priority are costly procedures for all parties involved [44]. Other applications can improve the effectiveness of e-voting services by securing them through data encryption functions [45], as well as record management related to donations and sponsorships to non-profit organizations [46].

V. Blockchain in Other Industries

Blockchain technology is directly used in supply chain management, helping to track products and enabling reliable process launches [47]. Shipping goods is another industry that benefits from improved records management by increasing transparency and security in maritime transport and related transactions [48]. Activities at ports and terminals (such as archiving and cargo availability information), customs authorities (like customs clearance of goods), intermediaries (such as archiving communications and transactions), and other bureaucratic procedures (including traceability) can see improvements in functionality, accuracy, and transparency thanks to these technologies [49]. Lastly, blockchain also impacts many areas of modern education, especially qualification certification services [50].

All these applications highlight the new possibilities offered by blockchain technology in records management, with the fundamental principle of ensuring maximum reliability and integrity for them [51].

VI. The Incompatibility of Blockchain and GDPR

However, it becomes clear that adopting legal personal data protection measures, such as the implementation of the GDPR in the EU, makes these applications problematic. The key innovation it introduces in e-government is not subject to central management and control functions [52]. Built on a peer-to-peer interaction framework, it is based on the principle of direct reciprocity between participants, allowing these functions to be performed within a single system without central mediators or third parties [53]. In such a system, transactions are recorded by any involved node, forming a chain where data is permanently stored and verifiable [21]. Indeed, in this system, all nodes in the network can record and control transactions, having direct access to the information in the blocks and their respective time sequences [54].

Blockchain technology is a secure database that uses asymmetric, complementary key encryption to protect data entered into the information chain [55]. The use of public and private keys along with hash functions enables the source of a specific message to be verified, ensuring its confidentiality, authenticity, and integrity [51].

Therefore, once validated by the nodes, the data entered cannot be altered or deleted, as it is recorded permanently. These features have historically conflicted with GDPR regulations, especially regarding the rights to rectification and erasure. However, recent advancements have proposed possible solutions. For example, the European Data Protection Board’s Guidelines 02/2025 highlight key compliance considerations for blockchain-based data processing, focusing on GDPR-compatible planning and accountability measures [56]. Moreover, technological innovations like chameleon hash functions have been introduced to allow data modification without compromising blockchain integrity, thereby supporting

GDPR's "right to be forgotten" [57]. Recent projects such as Olympus also investigate GDPR-compliant blockchain architectures using off-chain data storage and on-chain cryptographic verification, demonstrating that managing personal data under regulatory requirements is feasible. [58] These developments show a growing alignment between blockchain technology and data protection laws, indicating that practical legal and technical frameworks are starting to emerge.

The current regulatory framework was established between 2010 and 2014, and as a result, it does not account for emerging technologies such as blockchain, the Internet of Things (IoT), Artificial Intelligence (AI), or Smart Contracts [59]. Beyond this time limitation, skepticism among legislators has also arisen from the disruptive and decentralized nature of blockchain, which challenges traditional legal ideas of accountability, data ownership, and enforcement. Concerns about the opacity of consensus mechanisms, the potential for illegal use (e.g., money laundering or tax evasion), and the technical complexity of auditing distributed systems all contribute to hesitancy in adopting blockchain technology at the legislative level. Additionally, countries such as the United Kingdom and the United States have adopted data protection frameworks that reflect many of the GDPR's core principles, reinforcing a cautious regulatory approach toward blockchain implementations that could bypass centralized governance structures.

Indeed, in recent years, there has been intense research interest at both academic and practical levels regarding the relationship between blockchain and the GDPR, with their incompatibility attributed to two main reasons, as noted by a recent study conducted on behalf of the European Parliament [60]. The first reason concerns the fact that the GDPR is based on the premise that for each piece of personal data, there is at least one natural or legal person—the data controller—whom data subjects can approach to protect their rights under relevant EU data protection laws. In contrast, blockchain seeks information decentralization by replacing the central administrator with a network of different involved parties, making accountability for data use unclear. The second reason is that the GDPR enshrines the principle that personal data must be modifiable or erasable when necessary, as outlined in Article 16 (Right to Rectification) and Article 17 (Right to Erasure) of the Regulation [63]. Blockchain's immutability directly challenges these rights, creating a fundamental legal and functional incompatibility. However, blockchain makes such changes intentionally impossible to maintain data integrity and trust within the network [60].

The issues mentioned above have troubled many scholars and researchers, as discussed in the relevant literature. The conflict between blockchain and GDPR mainly revolves around three key points [61]. First, the "right to be forgotten" outlined in Article 17 of the GDPR requires entities holding personal data to delete it once the original purpose for collecting it has been fulfilled. This principle conflicts with one of blockchain's core features, which is the permanent storage of data and information entered into the network. Yaga et al. (2018) [62] explained that data is recorded on the blockchain in a permanent and unchangeable way, so removing it is not possible without "breaking" the chain. In other words, the architecture of this technology, which is based on cryptographic hash functions, does not allow modifying or tampering with data without disrupting its integrity and consistency [63].

According to Pizzetti (2017) [64], the immutability of the data recorded in this chain directly conflicts with the "right to be forgotten" introduced by the GDPR. The incompatibility between blockchain technology and data privacy is based on three fundamental assumptions.

(1) Data cannot be modified once inserted into a block, which conflicts with the right to delete and correct it according to article 17 of GDPR.

(2) Data is publicly accessible to each participant of the blockchain, a function that conflicts with the principles of confidentiality, accountability, and the designation of a central data processor.

(3) The data is stored indefinitely, which conflicts with GDPR principles related to purpose, necessity, and data minimization.

It becomes clear, then, that an organization that uses blockchain technology and chooses to comply with the data citizens' right to "be forgotten" faces a fundamental conflict with the core operating principles of this technology, undermining its credibility and validity [65].

The second point of incompatibility between blockchain and GDPR, as discussed in the relevant literature, relates to the fact that certain features of this technology conflict with "privacy by design" outlined in Article 25. Notably, Article 25 considers data protection as a set of measures that build in necessary guarantees of control and compliance with the regulation from the beginning when designing a data system [66]. Additionally, the inherent nature of blockchain requires storing data in the distributed ledger in a transparent and unchangeable manner, enabling each user to record a transaction and its associated value [67]. In this context, it has been argued that the transparent and publicly accessible nature of blockchain appears to present legal challenges. Under the current GDPR framework, data must be stored in a way that ensures, among other things, its confidentiality [68].

Given that personal data must be kept and processed discreetly, it goes without saying that it should only be accessible to authorized personnel. Although encryption and anonymization technologies can, to some extent, ensure compliance with these obligations, it is not yet clear whether this suffices to achieve full harmony between blockchain and GDPR [69]. A node containing personal data that may be visible to the public operates against the principle of availability; as such, data may be accessible to unauthorized users. Furthermore, if users can be identified from transaction data entries stored in a block, this conflicts with

the principle of confidentiality [70].

A foundational study by Biryukov et al. (2014) [71] demonstrated that users on the Bitcoin blockchain could be deanonymized through the analysis of pseudonymous addresses, even when such addresses exceeded 30 characters. This revelation exposed fundamental vulnerabilities in the blockchain's privacy assurances, especially within public, permissionless networks. These concerns are magnified in blockchain-based applications involving sensitive personal data, such as those in electronic health (e-health), where data confidentiality and user anonymity are crucial.

Recent research has reaffirmed and expanded on these concerns. Studies conducted as recently as 2023 continue to show that user identification through network-layer analysis remains feasible, indicating that the issue persists despite increased awareness and technical countermeasures. In response, new privacy-preserving frameworks have been proposed to protect sensitive information in healthcare systems.

For example, Alabdulatif et al. (2025) [73] introduced a blockchain-based authentication model using Ethereum smart contracts, blind signatures, and Proof of Authority (PoA) consensus to enhance the privacy, scalability, and efficiency of e-health systems. Likewise, other models incorporating self-sovereign identity (SSI), decentralized identifiers (DIDs), and attribute-based encryption (ABE) have been developed to enable granular, content-based access to encrypted medical data stored off-chain in decentralized file systems. These advancements highlight a growing focus on balancing blockchain's transparency with the strict privacy requirements imposed by data protection laws such as the GDPR.

The third point of incompatibility, which is the research focus of this review, concerns the distribution of data processing responsibility [74]. As Humbeeck (2019) [75] states, the fundamental principle of having a recognizable central entity that is legally responsible for data processing—embedded in the GDPR—and the core feature of blockchain technology that addresses this need are two conflicting perspectives that raise both legal and practical concerns. The decentralized nature of blockchain decision-making and data processing challenges the obligations placed on legal entities or individual persons by the current regulatory framework [76].

Indeed, the GDPR emphasizes data controllers as the main entities responsible for performing specific tasks and holding responsibilities for implementing necessary technical and organizational measures to protect personal data. However, the decentralized nature of blockchain makes it nearly impossible to identify who is accountable for these obligations under the GDPR. The core of this incompatibility mainly relates to how data should be protected [77]. In other words, the European legislature assumes that, in case of security breaches, regulatory authorities should hold a public or private entity accountable. Conversely, the very nature of blockchain removes the need for a "trusted third party," as trust is built collectively and there is no central authority managing the system responsible for storing and processing data [61].

The nodes participating in the blockchain's distributed ledger do not and cannot have full control over the functions within the system. In this context, the data controller defined by law is replaced by the blockchain's architecture and cryptographic functions [78]. While these may be more reliable for achieving secure and comprehensive data management than a legal or natural person, as required by the GDPR, they are practically difficult to hold accountable. Therefore, under this technological design, it is extremely challenging to identify the responsible "controller" under Article 4 of the Regulation [80], raising ethical concerns alongside legal ones. Given the limited influence of individual nodes, it would be unfair or even impossible to impose the GDPR obligations on data controllers [70], especially since most blockchain developers view hashing and anonymity as "impervious" doctrines of this technology [80].80].

VII. PROPOSALS

Reviewing academic literature shows ongoing conflicts between blockchain technology and the GDPR, especially regarding data erasure, accountability, and control. However, recent research is increasingly focused on solving these issues through legal and technological solutions. As mentioned earlier, efforts to make blockchain compatible with the GDPR include designating a legal entity—such as a Trusted Third Party (TTP)—to act as a data controller within the network [81]. This entity would be responsible for verifying the accuracy of personal data and ensuring GDPR compliance [82].

One area of research supports redesigning or adapting blockchain systems to better meet legal requirements, particularly concerning the right to be forgotten. Pollicino and De Gregorio (2017) [83] advocate for a compromise-based approach, while Dorri et al. (2019) [84] highlight that any data deletion process must preserve the integrity of the blockchain's structure. In this context, the concept of redactable blockchains—initially introduced by Ateniese et al. (2017) [85] using chameleon hash functions—has gained popularity. This enables selective data modification without compromising the cryptographic integrity of the chain.

Recent developments have tested different variations of this idea. For instance, Vukolić et al. (2024) [86] introduced updated chameleon hash functions to create GDPR-compliant blockchain designs while reducing the risk of misuse. Similarly, Olympus, a 2024 project by Ferrer et al. [87], uses hybrid off-chain storage with on-chain cryptographic proofs, enabling data to be erased from the system while maintaining blockchain auditability and integrity.

Legal scholars such as Pagallo et al. (2018) [88] have recognized that although these systems technically enable

data removal, implementation challenges still exist, especially if the redesign is attempted after a blockchain network is already in use [89]. Additionally, the continued existence of old copies of the blockchain remains an issue, even with architectures that can be modified [90].

To bypass on-chain limitations, a common design pattern involves storing personal data off-chain, with only the cryptographic hashes kept on-chain. Herian (2018) [76] endorses this approach as a GDPR-compliant strategy, and it is reflected in technical models by Bourka & Drogkaris (2018) [91] and Rieger et al. (2019) [2]. However, this also depends on a TTP, which some argue diminishes the decentralized nature of blockchain [89].

Addressing this concern, Eberhardt & Tai (2017) [92] and recently Ferrer et al. (2024) [87] proposed privacy-preserving off-chain architectures using zero-knowledge proofs, attribute-based encryption, and self-sovereign identity wallets, which minimize central control while improving compliance. These developments represent a merging of blockchain innovation with evolving data protection frameworks, showing that legal and technical interoperability is becoming more achievable.able.

VIII. Conclusions

The interaction between blockchain technology and the General Data Protection Regulation (GDPR) continues to present major challenges, especially regarding the storage and handling of personal data. While off-chain storage provides a possible solution by keeping personal data outside the immutable blockchain ledger, storing hash values on-chain that reference this data raises questions about whether these hashes qualify as personal data under GDPR. Currently, there is no clear consensus on this issue, leading to ongoing legal uncertainties [93, 94].

Recent advancements aim to bridge this gap. For example, the Olympus project showcases a GDPR-compliant blockchain system that uses off-chain storage for personal data while preserving on-chain cryptographic proofs to ensure data integrity and auditability [87]. This method aligns with the European Data Protection Board's latest recommendations [95], which offer guidance on personal data processing with blockchain, indicating that hybrid architectures present promising compliance solutions.

Furthermore, innovative frameworks like "Blockchain-enabled Trustworthy Federated Unlearning" have been introduced to fulfill the "right to be forgotten" in AI-integrated blockchain systems, allowing verifiable removal of user data contributions without compromising audit trails [96]. Such techniques provide a flexible way to enforce data subject rights even in decentralized settings.

In light of these developments, this paper proposes a mechanism that guarantees the right to be forgotten for data stored on-chain. The proposed system would use a hybrid approach, combining off-chain storage for personal data with on-chain references, and would include features to automatically assign and manage data controllers and processors. This design aims to uphold data protection principles while taking advantage of blockchain's inherent benefits, thereby supporting the development of legally compliant and technologically strong data management systems.

IX. References

[1] N. Al-Zaben, M. M. H. Onik, J. Yang, N. Y. Lee, and C. S. Kim, "General data protection regulation complied blockchain architecture for personally identifiable information management," in *Proc. IEEE Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Southend, UK, pp. 77–82, Aug. 2018, doi: 10.1109/iCCECOME.2018.8658586.

[2] A. Rieger, J. Lockl, N. Urbach, F. Guggenmos, and G. Fridgen, "Building a Blockchain Application that Complies with the EU General Data Protection Regulation," *MIS Quarterly Executive*, vol. 18, no. 4, Article 7, Dec. 2019. [Online]. Available: https://aisel.aisnet.org/misqe/vol18/iss4/7

[3] V. L. Lemieux, "Trusting records: Is blockchain technology the answer?," *Records Management Journal*, vol. 26, no. 2, pp. 110–139, Jul. 2016, doi: 10.1108/RMJ-12-2015-0042.

[4] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century*, P. Tasca, A. Aste, L. Pelizzon, and N. Perony, Eds. Cham: Springer, 2016, pp. 239–278, doi: 10.1007/978-3-319-42448-4_13.

[5] P. Vigna and M. J. Casey, *The Truth Machine: The Blockchain and the Future of Everything*. New York: St. Martin's Press, 2018.

[6] B. Markey-Towler, "Anarchy, blockchain, and utopia: A theory of political-socioeconomic systems organized using blockchain," *The Journal of the British Blockchain Association*, vol. 1, no. 1, pp. 1–13, Mar. 2018, doi: 10.31585/jbba-1-1-(1)2018.

[7] Hamilton, C., Harris, V., Taylor, J., Pickover, M., Reid, G., & Saleh, R. (2005). *Refiguring the Archive*. Dordrecht: Springer. https://doi.org/10.1007/1-4020-3089-6

[8] Duranti, L., & Michetti, G. (2012). Archival method. In A. Gilliland, S. McKemmish, & A. Lau (Eds.), *Archival Multiverse* (pp. 75–95). Victoria: Monash University Publishing.

[9] Lemieux, V. L. (2019). Blockchain and public recordkeeping: Of temples, prisons and the (re)configuration of power. *Frontiers in Blockchain*, 2, 5. https://doi.org/10.3389/fbloc.2019.00005

[10] International Organization for Standardization. (2001). *ISO 15489-1:2001—Information and documentation—Records management—Part 1: General*. Geneva: ISO. [Withdrawn; superseded by ISO 15489-1:2016].

[11] ARMA International. (2013). *Generally Accepted Recordkeeping Principles*. ARMA International. Retrieved from https://sosmt.gov/Portals/142/ARM/2015/notices/the-principles_executive-summaries_final.pdf

[12] [Duranti, L., & Rogers, C. (2014). Trust in records and data online. In J. Lowry & J. Wamukoya (Eds.), *Integrity in Government through Records Management: Essays in Honour of Anne Thurston* (pp. 203–216). Farnham: Ashgate.

[13] DLM Forum Foundation. (2011). *MoReq2010: Modular Requirements for Records Systems—Volume 1: Core Services & Plug-in Modules*. Brussels: Publications Office of the European Union. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/3e4c72c8-e802-4d73-bb1d-6cf3753d761c

[14] Franks, PC (2020). Implications of blockchain distributed ledger technology for records management and information governance programs. Records Management Journal (in press). Vol. 30 No. 3, pp. 287-299. https://doi.org/10.1108/RMJ-08-2019-0047, Issue publication date: 4 December 2020

[15] Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35(8), 2337–2354. https://doi.org/10.1016/j.tele.2018.10.004:contentReference[oaicite:0]{index=0}

[16] Lemieux, V. L., Hofman, D., Batista, D., & Joo, A. (2019). *Blockchain Technology & Recordkeeping*. ARMA International Educational Foundation. Retrieved from https://armaedfoundation.org/wp-content/uploads/2021/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf:contentReference[oaicite:1]{index=1}

[17] Bhatia, S., Douglas, E. K., & Most, M. (2020). Blockchain and records management: Disruptive force or new approach? *Records Management Journal*, 30(3), 277–286. https://doi.org/10.1108/RMJ-08-2019-0040OUCI+2IGI Global+2Ejournals+2

[18] Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27SCIRP

[19] Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007IDEAS/RePEc+2OUP Academic+2SCIRP+2

[20] Halamka, J. D., Lippman, A., & Ekblaw, A. (2017). The potential for blockchain to transform electronic health records. *Harvard Business Review*, 3(3), 2–5. Retrieved from https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

[21] Shrier, A. A., Chang, A., Diakun-Thibault, N., Forni, L., Landa, F., Mayo, J., & van Riezen, R. (2016). *Blockchain and Health IT: Algorithms, Privacy, and Data*. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Retrieved from: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

[22] Sunil, B., & Sangamesh, K. (2019). *Blockchain Technology for Securing Healthcare Records*. International Research Journal of Engineering and Technology, 6(4), 1804–1806. DOI not available.

[23] Harshini, V. M., Danai, S., Usha, H. R., & Kounte, M. R. (2019, April). *Health Record Management through Blockchain Technology*. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1411–1415). IEEE. https://doi.org/10.1109/ICOEI.2019.8862594 Webology+2OUCI+2OUCI+2

[24] Vaibhav, S., Manas, J., Raj, B., & Kishore, S. (2020). *Electronic Health Records Maintenance Using Blockchain*. International Research Journal of Engineering and Technology, 7(6), 4624–4627. DOI not available.

[25] Sadiku, M. N. O., Eze, K. G., & Musa, S. M. (2018). *Blockchain Technology in Healthcare*. International Journal of Advances in Scientific Research and Engineering, 4(5), 154–159. https://doi.org/10.31695/IJASRE.2018.32723 EurekaSelect+2ijasre.net+2ResearchGate+2

[26] Noh, S. W., Park, Y., Sur, C., Shin, S. U., & Rhee, K. H. (2017). *Blockchain-Based User-Centric Records Management System*. International Journal of Control, Automation, and Systems, 10(11), 133–144. https://doi.org/10.14257/ijca.2017.10.11.12MDPIPMC

[27] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). *MedRec: Using Blockchain for Medical Data Access and Permission Management*. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25–30). IEEE. https://doi.org/10.1109/OBD.2016.11

[28] Armstrong, S. (2018). *Bitcoin Technology Could Take a Bite Out of the NHS Data Problem*. BMJ, 361, k1996. https://doi.org/10.1136/bmj.k1996

[29] Navadkar, V. H., Nighot, A., & Wantmure, R. (2018). *Overview of Blockchain Technology in Government/Public Sectors*. International Research Journal of Engineering and Technology, 5(6), 2287–2292. DOI not available.

[30] Tasnim, M. A., Al Omar, A., Rahman, M. S., & Bhuiyan, M. Z. A. (2018, December). *CRAB: Blockchain-Based Criminal Record Management System*. In International Conference on Security, Privacy and Anonymity in Computation, Communication, and Storage (pp. 294–303). Springer, Cham. https://doi.org/10.1007/978-3-030-05345-1_25

[31] Vermont Agency of Digital Services. (2019). *Blockchains for Public Recordkeeping and Recording Land Records*. A White Paper of the Vermont State Archives and Records Administration Office of the Vermont Secretary of State. Vermont: Vermont League of Cities and Towns.

[32] Thakur, V., Doja, M. N., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on blockchain for implementation of land titling in India. *International Journal of Information Management*, 52, 101940. https://doi.org/10.1016/j.ijinfomgt.2019.04.013 OUCI+4pure.kfupm.edu.sa+4Cronfa+4

[33] Lazuashvili, N., Norta, A., & Draheim, D. (2019, September). Integration of blockchain technology into a land registration system for immutable traceability: A case study of Georgia. In *International Conference on Business Process Management* (pp. 219-233). Springer, Cham. https://doi.org/10.1007/978-3-030-30429-4_16

[34] Ramya, U. M., Sindhuja, P., Atsaya, R. A., Dharani, B. B., & Golla, S. M. V. (2018, July). Reducing forgery in land registry systems using blockchain technology. In *International Conference on Advanced Informatics for Computing Research* (pp. 725-734). Springer, Singapore. https://doi.org/10.1007/978-981-13-1580-0_64

[35] Hou, H. (2017, July). The application of blockchain technology in E-government in China. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCCN.2017.8038519

[36] Franciscon, E. A., Nascimento, M. P., Granatyr, J., Weffort, M. R., Lessing, O. R., & Scalabrin, E. E. (2019, May). A systematic literature review of blockchain architectures applied to public services. In *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 33-38). IEEE. https://doi.org/10.1109/CSCWD.2019.8791894

[37] Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. *Business & Information Systems Engineering*, 59(6), 441–456. https://doi.org/10.1007/s12599-017-0502-4IDEAS/RePEc+4

[38] Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, 26, 1–11. https://doi.org/10.1007/s11276-018-1866-y

[39] Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, 27(5), 53–57. https://doi.org/10.1002/jcaf.22179

[40] Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, 50(9), 14–17. https://doi.org/10.1109/MC.2017.3571042

[41] Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How blockchain can impact financial services–Expert interviewees' overview, challenges, and recommendations. *Technological Forecasting and Social Change*, 158, 120166. https://doi.org/10.1016/j.techfore.2020.120166

[42] Miraz, M. H., & Donald, D. C. (2018, August). Application of blockchain in booking and registration systems of securities exchanges. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)* (pp. 35–40). IEEE. https://doi.org/10.1109/iCCECOME.2018.8658513

[43] Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, 491, 151–165. https://doi.org/10.1016/j.ins.2019.04.005

[44] Gürkaynak, G., Yılmaz, İ., Yeşilaltay, B., & Bengi, B. (2018). Intellectual property law and practice in the blockchain realm. *Computer Law & Security Review*, 34(4), 847–862. https://doi.org/10.1016/j.clsr.2018.05.027

[45] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software*, 35(4), 95–99. https://doi.org/10.1109/MS.2018.2801546

[46] Lee, J., Seo, A., Kim, Y., & Jeong, J. (2018). Blockchain-based one-off address system to guarantee transparency and privacy for a sustainable donation environment. *Sustainability*, 10(12), 4422. https://doi.org/10.3390/su10124422

[47] Galvez, J.F., Mejuto, J.C., & Simal-Gandara, J. (2018). Future challenges on the use of blockchain for food traceability analysis. *TrAC Trends in*

Analytical Chemistry, 107, 222–232. https://doi.org/10.1016/j.trac.2018.08.011

[48] Loklindt, C., Moeller, M.P., & Kinra, A. (2018). How blockchain could be implemented for exchanging documentation in the shipping industry. In *International Conference on Dynamics in Logistics* (pp. 194–198). Springer, Cham. https://doi.org/10.1007/978-3-319-74225-0_27SpringerLink

[49] Jabbar, K., & Bjørn, P. (2018). Infrastructural grind: Introducing blockchain technology in the shipping domain. In *Proceedings of the 2018 ACM Conference on Supporting Groupwork* (pp. 297–308). https://doi.org/10.1145/3148330.3148345 dl.acm.org+2dl.eusset.eu+2dl.acm.org+2

[50] Chen, G., Xu, B., Lu, M., & Chen, N.S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1), 1–10. https://doi.org/10.1186/s40561-017-0050-xProQuest+3ThaiJo2.1: Thai Journal Online+3SpringerOpen+3

[51] Lemieux, V.L., & Sporny, M. (2017). Preserving the archival bond in distributed ledgers: A data model and syntax. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1437–1443). https://doi.org/10.1145/3041021.3053896 DOI+2OUCI+2De Gruyter Brill+2

[52] Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology*, 25(3), 179–195. https://doi.org/10.1093/ijlit/eax003

[53] Sakho, S. S., Zhang, J., Kiki, M. M., Bonzou, A. K., & Essaf, F. (2019). Privacy protection issues in blockchain technology. *International Journal of Computer Science and Information Security*, 17(2), 23–39.

[54] Sutton, A., & Samavi, R. (2017). Blockchain-enabled privacy audit logs. In *Proceedings of the 16th International Semantic Web Conference (ISWC)* (pp. 645–660).

[55] Biswas, S., Sharif, K., Li, F., Nour, B., & Wang, Y. (2018). A scalable blockchain framework for secure transactions in IoT. *IEEE Internet of Things Journal*, 6(3), 4650–4659. https://doi.org/10.1109/JI

[56] [European Parliament and Council of the European Union, 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 (General Data Protection Regulation), Official Journal of the European Union, L119, 4 May 2016, pp. 1–88.

[57] Mantelero, A. (2016). Right to be forgotten and public registers – A request to the European Court of Justice for a preliminary ruling. *European Data Protection Law Review*, 2(2), 231–235. https://doi.org/10.21552/edpl/2016/2/10

[58] Ferrer, A. L., Alchieri, E., Kharouf, R., Pimenta, M., & Melo, C. (2024). Olympus: A Model and Implementation for GDPR-Compliant Blockchain. *International Journal of Information Security*, 23. https://doi.org/10.1007/s10207-023-00782-z

[59] Hofman, D., Lemieux, V. L., Joo, A., & Batista, D. A. (2019). The margin between the edge of the world and infinite possibility: Blockchain and archival discourse. *Records Management Journal*, 29(1/2), 240–257. https://doi.org/10.1108/RMJ-12-2018-0045

[60] Finch, M. (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* Study for the European Parliamentary Research Service. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[61] Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*, 38, 105431. https://doi.org/10.1016/j.clsr.2020.105431

[62] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. National Institute of Standards and Technology. NISTIR 8202. https://doi.org/10.6028/NIST.IR.8202

[63] Di Ciommo, F. (2017). Privacy in Europe after Regulation (EU) No. 2016/679: What will remain of the right to be forgotten? *Italian Law Journal*, 3(2), 623–646. [Online]. Available: https://www.theitalianlawjournal.it/privacy-in-europe-after-regulation-eu-no-2016679/

[64] Pizzetti, F. (2017). Privacy e blockchain: la protezione dei dati personali nella catena di blocchi. Rivista di diritto dei media, 2(2), 1–20

[65] Herian, R. (2018). *Regulating Blockchain: Critical Perspectives in Law and Technology*. London: Routledge.

[66] Berberich, M., & Steiner, M. (2016). Blockchain technology and the GDPR—How to reconcile privacy and distributed ledgers. *European Data Protection Law Review*, 2(4), 422–448. https://doi.org/10.21552/EDPL/2016/4/10

[67] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, Jan–Feb, 118–127. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain

[68] Finck, M. (2018). Blockchains and data protection in the European Union. *European Data Protection Law Review*, 4(1), 17–35. https://doi.org/10.21552/EDPL/2018/1/6

[69] Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, 12(1), 156–174. https://doi.org/10.1080/17579961.2020.1729523

[70] Buocz, T., Ehrke-Rabel, T., Hödl, E., & Eisenberger, I. (2019). Bitcoin and the GDPR: Allocating responsibility in distributed networks. *Computer Law & Security Review*, 35(2), 182–198. https://doi.org/10.1016/j.clsr.2019.02.002

[71] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 15–29). https://doi.org/10.1145/2660267.2660379

[72] Daniels, J., Sargolzaei, S., Sargolzaei, A., Ahram, T., Laplante, P. A., & Amaba, B. (2018). The Internet of Things, Artificial Intelligence, Blockchain, and Professionalism. *IT Professional*, 20(6), 15–19. https://doi.org/10.1109/MITP.2018.2876925

[73] Alabdulatif, A., Khalil, I., & Alzahrani, A. (2025). Blockchain-based privacy-preserving authentication and access control for e-health systems. *Future Generation Computer Systems*, [In Press]. https://doi.org/10.1016/j.future.2025.02.012

[74] Manski, S., & Manski, B. (2018). No gods, no masters, no coders? The future of sovereignty in a blockchain world. *Law and Critique*, 29(2), 151–162. https://doi.org/10.1007/s10978-018-9225-zInternet Policy Review+4Academia+4ORCID+4

[75] Van Humbeeck, A. (2019). The blockchain-GDPR paradox. *Journal of Data Protection & Privacy*, 2(3), 208–212. https://doi.org/10.69554/EYOF8218HSTalks

[76] Herian, R. (2018). Regulating disruption: Blockchain, GDPR, and questions of data sovereignty. *Journal of Internet Law*, 22(2), 1–16.

[77] Schwerin, S. (2018). Blockchain and privacy protection in the case of the European general data protection regulation (GDPR): A Delphi study. *The Journal of the British Blockchain Association*, 1(1), 3554. https://doi.org/10.31585/jbba-1-1-(10)2018

[78] Mattila, J. (2016). The blockchain phenomenon – The disruptive potential of distributed consensus architectures. *ETLA Working Papers*, No. 38. The Research Institute of the Finnish Economy. https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdfEconPapers+2IDEAS/RePEc+2EconStor+2

[79] Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7SCIRP+1Dokumen+1

[80] Baldwin, J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications*, 4(1), Article 1. https://doi.org/10.1057/s41599-018-0065-0SSRN+8Internet Policy Review+8The Crypto Syllabus+8

[81] Henderson, A., & Burnie, J. (2018). Putting names to things: Reconciling cryptocurrency heterogeneity and regulatory continuity. *Journal of International Banking and Financial Law*, 33(2), 83–86.

[82] Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain access privacy: Challenges and directions. *IEEE Security & Privacy*, 16(4), 38–45. https://doi.org/10.1109/MSP.2018.3111245ResearchGate+2

[83] Pollicino, O., & De Gregorio, G. (2017). Privacy or Transparency? A New Balancing of Interests for the 'Right to Be Forgotten' of Personal Data Published in Public Registers. *Italian Law Journal*, 3(2), 647–668. theitalianlawjournal.it+2theitalianlawjournal.it+2SSRN+2

[84] Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). MOF-BC: A Memory-Optimized and Flexible Blockchain for Large-Scale Networks. *Future Generation Computer Systems*, 92, 357–373. https://doi.org/10.1016/j.future.2018.10.002

[85] Ateniese, G., Magri, B., Venturi, D., & Andrade, E. R. (2017). Redactable Blockchain – or – Rewriting History in Bitcoin and Friends. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 111–126). IEEE. https://doi.org/10.1109/EuroSP.2017.37BibBase

[86] Vukolić, S., Jain, A., & Oprea, A. (2024). Chameleon Hash Functions for GDPR-Compliant Blockchains. *Journal of Cybersecurity*, 9(1). https://doi.org/10.1093/cybsec/tyaf002
[87] Ferrer, A. L., Alchieri, E., Kharouf, R., Pimenta, M., & Melo, C. (2024). Olympus: A Model and Implementation for GDPR-Compliant Blockchain. *International Journal of Information Security*, 23. https://doi.org/10.1007/s10207-023-00782-z
[88] Pagallo, U., Bassi, E., Crepaldi, M., & Durante, M. (2018). Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure. In M. Palmirani (Ed.), *Legal Knowledge and Information Systems: JURIX 2018* (pp. 81–90). IOS Press.
[89] Ibáñez, L.-D., O'Hara, K., & Simperl, E. (2018). On Blockchains and the General Data Protection Regulation. *EU Blockchain Observatory and Forum*. European Parliament+3King's College London+3Blockchain+3
[90] Wirth, C., & Kolain, M. (2018). Privacy by Blockchain Design: A Blockchain-Enabled GDPR-Compliant Approach for Handling Personal Data. In *Proceedings of the 1st ERCIM Blockchain Workshop 2018*.
[91] Bourka, A., & Drogkaris, P. (2018). Recommendations on Shaping Technology According to GDPR Provisions. *European Union Agency for Network and Information Security (ENISA)*.
[92] Eberhardt, J., & Tai, S. (2017). On or Off the Blockchain? Insights on Off-Chaining Computation and Data. In F. de Paoli, S. Schulte, & E. B. Johnsen (Eds.), *Service-Oriented and Cloud Computing* (pp. 3–15). Springer. https://doi.org/10.1007/978-3-319-67262-5_1SpringerLink
[93] Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Ni Loideain, N., & Svantesson, D. J. B. (2018). Blockchain versus data protection. *International Data Privacy Law*, 8(2), 103–104. https://doi.org/10.1093/idpl/ipy008
[94] Hristov, P., & Dimitrov, W. (2019). The blockchain is a backbone of GDPR compliant frameworks. *Calitatea*, 20(S1), 305.
[95] European Data Protection Board (EDPB). (2025). Guidelines 02/2025 on the Use of Blockchain for Personal Data Processing. [Online]. Available: https://edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf
[96] Zhang, Y., Chen, J., Liu, X., & He, B. (2024). Blockchain-enabled trustworthy federated unlearning for GDPR compliance. *arXiv preprint arXiv:2401.15917*. https://arxiv.org/abs/2401.15917

X. AUTHORS

Nikos Kareklas holds an MSc in Information Science from the CITY University of London, England (School of Mathematics, Computer Science and Engineering) and is a graduate of the Department of Library Sciences and information systems of the Technological Educational Institute of Athens. From 2016 to 2023, he served as a laboratory collaborator in the Department of Archives, Library, and Information Systems at the University of West Attica. Since 2019, he has been a Ph.D. candidate in the same department, researching the use and value of new technologies in Records Management, which is his area of expertise. He successfully defended his Ph.D. thesis in 2025. He has built a successful professional career as an Information Manager on numerous innovative projects in Greece, including the modernization and upgrade of the Elefsis Refinery, which remains the largest private industrial investment in Greece to this day. For many years, he was the Director of the Records Management Department at WWW, one of the few companies in Greece dedicated to professionally managing archive material. Since 2019, he has been the Managing Director of GreenFence-MetalLogic, a company specializing in confidential data destruction and precious metals refining. In 2021, he received an honorary distinction at the Business Elite Awards 40 Under 40, in recognition of his exceptional professional skills and leadership. His current research interests focus on integrating new technologies such as Blockchain and Artificial Intelligence into Records Management, as well as implementing GDPR in Greek companies and developing a new model for processing active documents.

Artemis Chaleplioglou is an Assistant Professor of Health Information Science in the Department Archival, Library & Information Studies at the University of West Attica. She is a faculty member of the Information Management Laboratory at the University of West Attica. She was a post-doctoral researcher at Ionian University, Department of Archives, Library Science, and Museology from 2018 to 2022, and she served under an academic scholarship in the Department of Archival, Library, and Information Studies at the University of West Attica from 2020 to 2023. She is a council member of the European Association of Health Information Libraries (EAHIL). She is the Editor-in-Chief of the Journal of Hospital Librarianship, published by Taylor & Francis, Informa UK (https://www.tandfonline.com/journals/whos20). She is a peer reviewer for academic journals in Information Science and Informatics, such as Scientometrics, JOLIS, BMC Bioinformatics, and others. Her research has been published in international peer-reviewed journals and conferences. Her research interests include: Information Science, Librarianship, Health Libraries, Semantic Web, and Bibliometrics.