LUISS

Master of Science in Law, Digital Innovation and Sustainability

Chair of Data Protection Law

The GDPR's Right to Erasure and Blockchain Technology: Towards (In)compatibility?

Simone Garibaldi
631673
CANDIDATE

Prof. Filiberto E. Brozzetti
SUPERVISOR

Prof. Anna Berti Suman
CO-SUPERVISOR

Academic Year 2024/2025

Table of Contents

1. Introduction…. 4

2. Right to Erasure and Blockchain Technology 8

2.1 Setting the Context 8

2.1.1 The GDPR and the Right to Erasure: Legal Foundations 8

2.1.2 Origins, Functioning and Core Features of Blockchain Technology 11

2.2 Structural Tensions Between GDPR and Blockchain Technology 16

2.2.1 The Immutability of Blockchain and the Right to Erasure 16

2.2.2 Other Conflicts: Identification of Controllers and Territorial Scope in Decentralized Ledgers 18

2.3 The 2024 Spanish Data Protection Supervisory Authority Proof of Concept 22

2.3.1 The "*Equívocos*" of Blockchain Technology According to the AEPD 22

2.4 Reconciling Law and Technology 25

2.4.1 Blockchain Technology as "Originally Anarchic" and "Alegal" 25

2.4.2 A Dynamic Perspective 27

3. Technical Adaptations to Implement the Right to Erasure in Blockchain Technology 29

3.1 The AEPD Proposal 29

3.1.1 The Proof of Concept Implementation 29

3.1.2 Proof of Authority, Decentralization, and Replicability of the Proof of Concept 31

3.2 The Almaviva GiottoChain Case 34

3.2.1 The Project: Notarization Service in Public Blockchain 34

3.2.2 Data Protection in GiottoChain and the Right to Erasure Compliance 36

3.2.3 The European Blockchain Sandbox Initiative 39

3.3 Possible Technical Solutions for Blockchain Compliance with Article 17 GDPR 44

3.3.1 Mutable Blockchain Infrastructures and Chameleon Hashes 44

3.3.2 Off-Chain Data Storage and Key Destruction 46

3.3.3 Zero-Knowledge Proof Technologies 48

4. Finding Compatibility. 51

4.1 Regulatory Sandboxes and the Importance of Dialogue and Experimentation 51

4.1.1 Overview and Global Expansion of Regulatory Sandboxes 51

4.1.2 Regulatory Sandboxes: Objectives and Experimental Traits 52

4.2 Regulatory Enforcement or Compromise? 56

4.2.1 The EDPB "Guidelines 02/2025 on the Processing of Personal Data Through Blockchain Technologies": Between Openness and Caution 57

4.2.2 A Flexible and Pragmatic Regulatory Approach 58
5. Conclusions 60
Bibliography 64

Chapter 1
Introduction

Data have become a fundamental pillar of the global economy, and their importance continues to grow. Once primarily a driver of growth through efficiency and innovation, data are now collected, structured, and exchanged to create economic value in what can be called a "data economy" and no longer a "data-driven economy"[1]. Data, defined as information originating from and related to various fields and derived primarily from digital technologies[2], have been metaphorically described as the new "black gold" of the twenty-first century[3]. The economic power of data lies in their transformation into a crucial asset that drives innovation, disrupts industries, and creates new markets, offering businesses a competitive advantage across sectors[4]. However, unlike "black gold", oil, the amount of data is not a finite resource. In fact, the global volume of data generated every year grows exponentially. In 2024, the total amount of data generated, stored, duplicated, and utilized worldwide reached 149 zettabytes[5] (equivalent to one sextillion bytes), and projections indicate that by 2025, this figure will rise to 181 zettabytes[6].

The pervasive digitalization of everyday life has resulted in the widespread collection and utilization of data. Technologies, such as the Internet, and more recently Artificial Intelligence (AI), Internet of Things (IoT) sensors, and blockchain play a central role in the data economy we live in today. As these technologies advance and the exploitation of data and personal data (data through which it is possible to identify persons) increases, regulations have evolved to address both the increasing legitimate use and potential misuse of such information. A key area of focus in this regard is data protection, which entails the fundamental concept of protecting the integrity of the identity of people. Data protection varies globally in both approach and implementation. In Europe, the experience of totalitarian regimes in the 20th century has contributed to a heightened collective awareness of the importance of safeguarding personal data[7], leading the European Union (EU) to actively develop data protection

[1] Andrea Sestino, Adham Kahlawi, and Andrea De Mauro, "Decoding the Data Economy: A Literature Review of Its Impact on Business, Society and Digital Transformation", *European Journal of Innovation Management* 28, no. 2 (2025), p. 298.
[2] *Ivi* p. 299.
[3] Lawrence Texeira, "The New Black Gold: How Data Became the Most Valuable Asset in Tech", *Medium*, February 12, 2024. https://medium.com/@lawrenceteixeira/the-new-black-gold-how-data-became-the-most-valuable-asset-in-tech-9e4541262ddf.
[4] OECD, *Going Digital to Advance Data Governance for Growth and Well-being*, (Paris: OECD Publishing, 2022), p. 16.
[5] "Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025", Statista, accessed February 2025, https://www.statista.com/statistics/871513/worldwide-data-created/#statisticContainer.
[6] *Ibidem*
[7] Hannah Bloch-Wehba, "Confronting Totalitarianism at Home: The Roots of European Privacy Protections", *Brooklyn Journal of International Law*, Vol. 40 (2015), p. 751.

strategies over the last years, culminating in the adoption of Regulation 2016/679, known as the General Data Protection Regulation (GDPR).

Data's strategic importance as an infrastructural resource is widely acknowledged at the international level[8], and various initiatives have been launched to enable cross-border data sharing[9]. However, rising protectionist trends are hindering these efforts[10], as such initiatives would require significant liberalization of the sector and the establishment of a shared data governance framework, an objective that increasingly appears unrealistic.

Furthermore, the importance of digitalization and the associated concepts of digital and data sovereignty within the growing realm of data geopolitics is reflected in the strong emphasis placed by the EU and its Commission President, Ursula von der Leyen, since the beginning of her first mandate in 2019[11]. The focus on the digital transition, alongside sustainability, remained central throughout the mandate as evidenced by the numerous laws adopted on the subject, such as the Digital Services Act, the Digital Markets Act, the Data Act, the Data Governance Act, and the Artificial Intelligence Act, among others. The EU strategy sought to govern the digital phenomenon, acknowledging its significance while reacting to innovations often originating in other countries[12].

In this context of digital regulation, the protection of citizens' data, the unique "EU's one and only digital asset"[13], is ensured through the fundamental principles enshrined in the GDPR, but challenges arise from the interaction with certain emerging technologies. The complex interplay between innovation and law, particularly between innovative technology and data protection law, is evident in numerous cases. These lead to the central theme of this work: the challenging compatibility between the data protection rights conferred to EU citizens by the GDPR, specifically the right to erasure, and a technology that, while no longer at the forefront of novelty and excitement, having been somewhat eclipsed by the rise of Artificial Intelligence (AI), remains highly relevant and potentially valuable, such as blockchain (thereby also referred to as Distributed Ledger Technology, or DLT).

[8] OECD, *Going Digital to Advance Data Governance for Growth and Well-being*, pp. 15-16.
[9] OECD, *Fostering Cross-Border Data Flows with Trust*, (Paris: OECD Publishing, OECD Digital Economy Papers, 2022).
[10] Martina F. Ferracane, "The Costs of Data Protectionism". In *Big Data and Global Trade Law*, edited by Mira Burri, (Cambridge University Press, 2021), p. 64.
[11] Filiberto E. Brozzetti, "EU Digital Sovereignty: How Long Will the "Brussels Effect" Last?", *Rivista Internazionale Di Filosofia del Diritto*, 2(2024), p. 345.
[12] *Ivi* pp. 349-350.
[13] *Ivi* p. 350.

Specifically, blockchain's inherent immutability feature, stemming from the original nature of the technology itself[14], appears to be in direct tension with the right to erasure enshrined in Article 17 of the GDPR[15], which assumes that data subjects can request and obtain the deletion of their personal data in certain data processing scenarios. This contradiction frames the central research question of this thesis: whether and to what extent blockchain technology and the GDPR can be compatible with respect to the right to erasure, from both a legal and technical perspective.

The issue is complex and difficult to solve, despite extensive academic examination[16]. The intersection of regulatory and policy-making frameworks, digital and technical perspectives, innovative experimental aspects, and the relationship between regulators and firms applying blockchain technology reveals a complicated scenario, whose importance has also been recently acknowledged by EU authorities. Indeed, the writing of this thesis took place alongside important publications by national and supranational authorities, which simultaneously supported and challenged the ongoing research, highlighting both the complexity of the topic and its contemporary relevance.

This thesis is structured as follows: Chapter 2, titled "Right to Erasure and Blockchain Technology", will provide an overview of the context. This includes an introduction to the GDPR's right to erasure and its legal foundations, alongside an explanation of blockchain technology, covering its origins and functionality. The chapter will also present the tensions between regulation and blockchain, with a primary focus on the challenge posed by DLT's immutability to comply with the right to erasure. Furthermore, other conflicts will be analyzed and exposed: the complicated allocation of data processing responsibilities in DLT infrastructure, and the international transfer issue, among others. Specifically, section 2.3 will discuss a recent development, the 2024 Proof of Concept from the Spanish Data Protection Supervisory Authority, which offered a technical proof of compliance for a blockchain infrastructure in relation to the right to erasure. Section 2.4 will provide a discursive overview of the importance of reconciling technology and law, examining the "anarchic" and "alegal" features of DLTs.

"Chapter 3 - Technical Adaptations to Implement the Right to Erasure in Blockchain Technology" will focus on a more technical analysis, providing a practical examination of the AEPD Proof of Concept and assessing the replicability of the adopted measures in other contexts, and examining a significant

[14] David van de Giessen, "Blockchain and the GDPR's Right to Erasure", (Bachelor's essay, University of Twente, 2019), p. 2.
[15] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, Version 1.1, April 8, 2025, p 12.
[16] Rahime Belen-Saglam, Enes Altuncu, Yang Lu, and Shujun Li, "A systematic literature review of the tension between the GDPR and public blockchain systems", *Blockchain: Research and Applications* 4, (June 2023), p. 2.

case study: the GiottoChain project developed by the Italian digital company Almaviva. This blockchain project, designed for the notarization of digital assets, participated in the first cohort of the European Blockchain Sandbox in 2023. The relevance of the GiottoChain case lies in both its approach to data erasure and its relationship with EU regulators within the practical sandbox process, aspects analyzed in section 3.2, thanks to insights offered by Almaviva. The Chapter will also offer an overview of some of the most promising technical mechanisms for achieving compliance between Article 17 GDPR and DLTs. The examined tools are: the chameleon hash techniques that render blockchains mutable, the practice of storing data off-chain and destroying cryptographic keys, which permits the decryption of the hashes stored as proof of existence, and the Zero-Knowledge Proof technologies, which enable privacy-preserving verification of data without revealing personal information.

"Chapter 4 - Finding Compatibility" will focus primarily on regulatory and governance perspectives. It will explore the opportunities arising from sandbox experiences, important tools to enhance dialogue between firms and regulators, and to eventually experiment both in terms of innovative products and connected legislations. Furthermore, section 4.2 will provide an analysis of the European Data Protection Board (EDPB) "Guidelines 02/2025 on processing of personal data through blockchain technologies", published in April 2025. The "posture" of the EDPB as expressed in the document will be examined, alongside the consideration of the potential for EU authorities to assume a more flexible and pragmatic regulatory approach towards emerging technologies. Such an approach would require careful attention in avoiding stifling innovation, balancing the compliance requirements with the dynamic specificity of unconventional technologies, such as blockchain. Finally, Chapter 5 will present the concluding remarks of this thesis, synthesizing the key findings and reflecting on the challenges and opportunities emerging from the complex and conflicting relationship between blockchain technology and the GDPR's right to erasure.

The research primarily relies on authoritative academic and legal sources, as well as publications from national and European authorities. Given the contemporary nature of the topic, most sources are recent, and literature will probably be subject to evolution over time. Moreover, a practical approach has been adopted, including qualitative interviews conducted as part of the GiottoChain case study, to enrich the analysis with valuable perspectives. By examining the compatibility between the right to erasure and blockchain, the thesis aims to offer a contribution to the ongoing dialogue around balancing innovation with regulation, providing practical insights that may support responsible and effective governance of emerging technologies in an evolving digital landscape.

Chapter 2
Right to Erasure and Blockchain Technology

2.1 Setting the Context

2.1.1 The GDPR and the Right to Erasure: Legal Foundations

On April 27, 2016, "Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" was published in the Official Journal of the European Union (EU). This regulation, commonly referred to as the General Data Protection Regulation (GDPR), entered into force on May 25, 2018, replacing Directive 95/46/EC, also known as the Parent Directive. The legislator aimed to switch from a prescriptive to a substantive and pragmatic approach to data protection. One of the main objectives was to effectively address the numerous technological advancements that arose over the twenty years of the Parent Directive. The Internet, above all, was still in its "infancy" stage when the initial norm was enacted[17]. In fact, over the years, countless data processing methods have been developed, along with the proliferation of a connected myriad of data controllers, the entities that define the purposes and methods of processing personal data. Data protection needed a new approach based on the accountability principle to give data subjects control over their data[18]. Moreover, the choice of adopting a Regulation instead of a Directive was legally significant. Both are EU secondary legislative acts, but while regulations are directly applicable in all EU Member States, directives establish binding objectives but allow Member States the discretion to determine how to achieve them[19]. This decision aimed to address inconsistencies in the implementation of data protection strategies across Member States, ensuring greater harmonization at the EU level, and also facilitating the free movement of personal data in the European Union[20].

The GDPR, complying with Article 8 of the Charter of Fundamental Rights of the European Union, aims to grant data subjects greater control over their personal data by establishing several rights, some

[17] "The History of the General Data Protection Regulation", European Data Protection Supervisor, accessed February 2025, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
[18] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 1
[19] "Types of EU Law", European Commission, accessed February 2025, https://commission.europa.eu/law/law-making-process/types-eu-law_en.
[20] Michèle Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?", *Panel for the Future of Science and Technology (STOA)*, European Parliamentary Research Service (EPRS), July 2019, p. I.

of them inherited from the 1995 Directive and others new. Among the latter, Article 17 of the GDPR defines the right to erasure, also referred to as the right to be forgotten.

The article states that:
"1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

The article further explains the controller's obligation to notify third parties when personal data have been made public:
"2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

Article 17 concludes by defining some considerations for which the right to erasure may not be exercised:
"3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) 1. for the establishment, exercise or defence of legal claims."

The GDPR's right to erasure plays a key role in enhancing informational self-determination by empowering data subjects to request the deletion of their personal information from a data controller, provided that one of the specified legal grounds is met[21]. However, this right is not absolute; it is both conditional and subject to the specific limitations listed in the third paragraph of the article.

The recognition and development of the right to erasure were significantly shaped by legal precedents. A key moment in this evolution came in 2014, before the GDPR's approval, with the *Google Spain v. AEPD and Mario Costeja Gonzalez* judgment. The case revolved around the request of a Spanish citizen, Mr. Costeja, to have online articles from the 1980s that damaged his reputation removed from Google. The European Court of Justice (ECJ) acknowledged that the Directive did not explicitly recognize a "right to be forgotten", as the deletion of data could only apply to processing activities incompatible with the Directive's provisions[22]. However, the ECJ ruling established that individuals have the right to request the delisting of links that redirect to lawfully published personal data when its continued accessibility is irrelevant, excessive, or outdated in light of data protection principles[23]. Significantly, the Court's ruling affirmed what would later become a central pillar of the GDPR: the individual's control over personal data and their deletion, emphasizing the right to data protection[24].

It is also essential to identify in *Google Spain v. AEPD and Mario Costeja Gonzalez* a central raised issue that will be one of the key focuses of this work, namely the role of technology (in this specific case, big search engines containing links to personal information) in the interactions with the law. At the time of the ruling, many media and academics debated its implications, particularly with regard to the impact on legislative updates, the improvement of technology use, and the creation of a safer and

[21] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?", p. 75.
[22] Orla Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja González", *Modern Law Review* 78, no. 3 (2015), p. 528.
[23] *Ivi*, p. 522.
[24] *Ivi*, p. 533.

more balanced cyberspace[25]. There was significant skepticism regarding the practical implementation of the right to be forgotten, as the notion of the Internet as a permanent repository of digital footprints was deeply rooted, and the technology was seen by many as difficult to change or to regulate[26]. However, this did not hinder the evolution of legal principles, ultimately leading to the adoption of the GDPR and the codification of Article 17 within it.

While the GDPR aimed, and succeeded, at revolutionizing and modernizing the European data protection framework, conflicts and tensions still exist, particularly with emerging technologies entering the field. Among these, blockchain technologies present significant conflicts with some of the GDPR's main principles, particularly the right to erasure.

2.1.2 Origins, Functioning and Core Features of Blockchain Technology

A blockchain is a digital Distributed Ledger Technology (DLT) that, as can be easily inferred by its name, consists of a chain of blocks. Each block is identified by a cryptographic hash and contains a set of data and the hash of the previous block, establishing the chain link between blocks[27] (Figure 1). The hash is the output of a hashing algorithm, "a function that compresses a string of arbitrary input to a string of fixed length"[28].

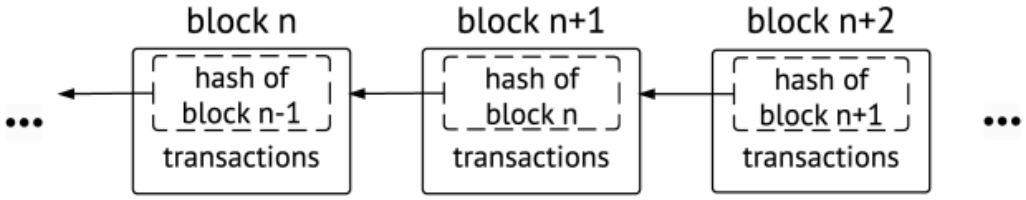

Figure 1 - Blockchain Structure. Source: Konstantinos Christidis and Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", IEEE Access 4 (2016): 2296.

The blockchain data structure is distributed, meaning there is no central database containing all the data[29]. Instead, the ledger is replicated and shared among all participants, commonly referred to as

[25] Julia Powles, "What Did the Media Miss with the Right to Be Forgotten Coverage?", *The Guardian*, May 21, 2014, https://www.theguardian.com/technology/2014/may/21/what-did-the-media-miss-with-the-right-to-be-forgotten-coverage.
[26] Andrew Smith, "Roll Up for Digital Whack-a-Mole: Europe Can't Enforce the Right to Be Forgotten", *The Conversation*, May 20, 2014, https://theconversation.com/roll-up-for-digital-whack-a-mole-europe-cant-enforce-the-right-to-be-forgotten-26726.
[27] Konstantinos Christidis and Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", *IEEE Access* 4 (2016), p. 2293.
[28] Rajeev Sobti and Geetha Ganesan, "Cryptographic Hash Functions: A Review", *IJCSI International Journal of Computer Science Issues* 9, no. 2 (2012), p. 461.
[29] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 1

"nodes" or "peers". In order to achieve the necessary agreement on a single data value or a single state of the network among distributed agents, these "peer-to-peer" architectures work on a consensus mechanism[30]. There are different types of consensus mechanisms, chosen by developers depending on the type of different blockchain[31].

The idea of building a digital distributed protocol to create consensus between uncoordinated parties was already a topic of discussion in the 1980s[32]. However, the first systematic conceptualization of blockchain technology, which preceded its real-world implementation, is attributed to Satoshi Nakamoto, an anonymous individual or group of developers, who published the paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* in 2008. The project was conceived to create Bitcoin, a trustless payment system relying on DLT, also named "cryptocurrency", for processing electronic transactions. The purpose was to eliminate the need for financial institutions, toward which the 2008 financial crisis had generated significant distrust. Nakamoto wrote: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party"[33].

The Bitcoin cryptocurrency was also designed to solve the double-spending problem, a fundamental challenge in digital currencies where a unit of value could be spent more than once. Traditional electronic payment systems rely on a central authority to verify transactions and prevent fraudulent duplication, while Bitcoin introduced a decentralized approach, leveraging blockchain technology to ensure that once a transaction is confirmed, it becomes irreversible and immutable[34]. Satoshi Nakamoto's proposed solution relied on a decentralized network where transactions are, still today, validated through a Proof-of-Work (PoW) consensus mechanism, ensuring security without the need for a trusted intermediary. The PoW system, simplifying, requires computational resources from "miners", nodes who dedicate their processing power to solving cryptographic puzzles in order to add new blocks to the ledger, thereby securing the network and confirming transactions[35].

Since the emergence of Bitcoin, numerous blockchain systems have been developed, featuring diverse technological variations and applications. Beyond cryptocurrency exchange, blockchain is now utilized in various sectors, including, among others, education, healthcare, and the Internet of Things

[30] Christidis and Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", p. 2293.
[31] *Ibidem.*
[32] Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem", *ACM Transactions on Programming Languages and Systems* 4, no. 3 (1982): p. 382.
[33] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", October 31, 2008, p. 1.
[34] Lewis Popovski and George Soussou, "A Brief History of Blockchain", *Legal Tech News*, May 14, 2018, p. 2.
[35] Christidis and Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", p. 2294.

(IoT)[36]. An important development in the "crypto-world" was Ethereum, a decentralized platform designed to run smart contracts (defined as computerized transaction protocols that automatically execute the terms of a contract[37]), established in 2013, and which is the most well-known DLT, together with Bitcoin. This highlights the importance of considering blockchain not as a singular technology, but rather as a class of technologies that share fundamental core features while evolving to serve different purposes[38]. Blockchains are not only limited to the cryptocurrency sector; they have a wide range of applications across various industries, and personal data are often involved in DLT processes.

Most blockchains contain personal data in various forms: they can be directly embedded in blocks, transactions, or operations related to smart contracts, stored off-chain in connection with DLT usage, or maintained by individual nodes in replicas or temporary databases[39]. In fact, the transactions occurring in blockchain may often contain personal data and metadata ("data about data" that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource[40]), which, even if hashed, are considered pseudonymized but not anonymized[41] (for the distinction between pseudonymization and anonymization, see section 2.2.1). Additionally, most blockchain systems use a two-step verification process with asymmetric encryption, where each peer has a public key, functioning similarly to a username, and a private key, serving as a password for authentication and security[42]. The public key, which is visible on the public ledger, may be considered personal data, in accordance with the "online identifier" definition contained in Recital 30 of the GDPR, and drawing an analogy with a 2016 ECJ decision regarding Internet Protocol (IP) addresses (judgment of 19 October 2016, *P. Breyer v. Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779)[43]. Furthermore, personal data in DLTs may not be directly stored on the ledger but can be shared with third parties or referenced externally. The overall presence of personal data in DLTs requires compliance with the GDPR.

[36] Belen-Saglam, Altuncu, Lu, and Li, "A systematic literature review of the tension between the GDPR and public blockchain systems", p. 2.
[37] Alexander Savelyev, "Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law", *Information & Communications Technology Law*, 26(2), (2016), p. 7.
[38] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?", p. I.
[39] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, (November 13, 2024), p. 23.
[40] Jenn Riley, *Understanding Metadata*, for National Information Standards Organization (NISO), (Baltimore, MD: NISO Press, 2017), p. 1.
[41] Agencia Española de Protección de Datos and European Data Protection Supervisor, *Hash Functions as Personal Data Pseudonymisation Techniques,* (November 4, 2019), p. 26.
[42] *Ivi*, p. 26.
[43] Aurelie Bayle, Mirko Koscina, and David Manset, "When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry", *IEEE/WIC/ACM International Conference on Web Intelligence (Wil)*, December 2018, p. 2.

Four main features of blockchain technology can be identified: decentralization, immutability, scalability, and a limited degree of privacy[44]. While decentralization and, in a certain way, also immutability, are widely recognized as core properties, it remains debatable if scalability and privacy limitations can be referred to all blockchain systems. These four characteristics are briefly summarized as follows.

1) Decentralization has already been examined, but it is important to emphasize that it is the fundamental underlying concept behind DLT. It ensures that data integrity is maintained collectively by all nodes, with trust distributed among participants rather than relying on a central authority[45]. There are however practices that reduce the decentralization, which is almost never an absolute characteristic (in depth in section 2.2.1).

2) Immutability is closely related to the design of blockchain, and it implies that once data is added in a block, and the nodes have agreed upon that, it is not possible, most of the time, to modify that data. More about the immutability concept is offered in the subsequent section, the 2.2.1.

3) Scalability refers to the challenges that arise in blockchains with a large number of participants, particularly in terms of throughput, propagation time of information, and the amount of data stored[46]. Scalability depends largely on the consensus algorithm used and the intended application of the blockchain.

4) Privacy limitations emerge primarily due to blockchain's data inherent transparency, which is one of its foundational principles. However, privacy constraints are not uniform across all blockchain systems. The level of privacy is influenced by factors such as data encryption, hashing mechanisms, private key management, and the architecture of the blockchain itself, meaning whether the blockchain is public (permissionless) or private (permissioned)[47]. In public blockchains, anyone can participate as a node, whereas in private blockchains, access is restricted to a selected group of participants, for instance the employees of a specific company[48]. The most used and famous blockchains, such as Bitcoin or Ethereum, are public and do not require any authorization to participate. These types are the ones for which the compatibility with some aspects of the GDPR is more problematic, as

[44] Fabian Knirsch, Andreas Unterweger, and Dominik Engel, "Implementing a Blockchain from Scratch: Why, How, and What We Learned," *EURASIP Journal on Information Security* 2019, no. 2 (March 2019), p. 2.
[45] *Ibidem.*
[46] *Ibidem.*
[47] *Ibidem.*
[48] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, p. 17.

highlighted in 2018 by the EU Blockchain Observatory & Forum, stating that: "Public, permissionless blockchains represent the greatest challenges in terms of GDPR compliance"[49].

[49] Tom Lyons, Ludovic Courcelas, and Ken Timsit, "Blockchain and the GDPR", by *The European Union Blockchain Observatory And Forum*, (October 16, 2018), p. 16.

2.2 Structural Tensions Between GDPR and Blockchain Technology

2.2.1 The Immutability of Blockchain and the Right to Erasure

In addressing the interplay between blockchain technology and the GDPR's right to erasure, it is necessary to clarify the precise meaning of "erasure", as Article 17 of the GDPR does not provide a formal definition. According to the Oxford Dictionary, erasure is "the act of removing or destroying all signs of something"[50], a meaning that could suggest a restrictive interpretation, implying the complete destruction of data by controllers.

However, past sentences and indications from national and supranational regulators have adopted in the years a more flexible interpretation of the practical implications of the right to erasure, allowing for "alternatives to the outright destruction of data"[51]. In the *Google Spain v. AEPD and Mario Costeja Gonzalez* judgment (for more details see 2.1.1) the delisting of information from research results was considered an erasure[52]. Similar decisions had been previously taken in the 2012 Opinion on Cloud Computing by the Article 29 Working Party, the former EU advisory board on data protection, replaced in 2018 with the European Data Protection Board (EDPB). The Opinion considered hardware destruction, demagnetization, and overwriting as methods to ensure data erasure[53], not yet explicitly governed at the time of the 1995 Directive. Another consideration was raised by a sentence of the Austrian Data Protection Authority, the *Datenschutzbehörde* (DSB), which in December 2018 recognized anonymization of the data as a means to realize the erasure[54]. This decision referenced to Recital 26 of GDPR, which states that anonymized data falls outside the scope of the GDPR. At this stage, it is important to clarify the definition of anonymization and its distinction from pseudonymization. Anonymization refers to the process of irreversibly transforming data so that the data subject can no longer be identified. In contrast, pseudonymization is a reversible process that modifies data to prevent immediate attribution to a specific data subject but allows re-identification if using additional information.

[50] Oxford Learner's Dictionaries, s.v. "erasure," accessed February 2025, https://www.oxfordlearnersdictionaries.com/definition/english/erasure
[51] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" p. 76.
[52] *Ivi*, p. 75.
[53] Article 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing*, WP 196, adopted July 1, 2012, pp. 20-21.
[54] Datenschutzbehörde, *Decision DSB-D123.270/0009-DSB/2018*, December 5, 2018.

Having examined the various applications and interpretations of the right to erasure, it is essential to emphasize that it must be applied to all processing activities involving personal data (except the limitation cases listed in paragraph 3 of Article 17), regardless of the technology used, as established by the principle of technological neutrality outlined in Recital 15 of the GDPR. Among the numerous technologies used in data processing activities, DLTs are one of the most problematic in terms of right to erasure compliance. The immutability feature (cited in section 2.1.2), which stands behind the very initial concept of the "append-only" distributed ledgers, seems to make by design blockchain incompatible with Article 17 GDPR, as well as with Article 16 GDPR, which defines the "right to rectification". In fact, any change to a block would be immediately noticeable to all network participants of a DLT, as it would disrupt the cryptographic linkage between blocks[55]. This would require altering all subsequent blocks, and a new consensus by all the participants on the new modified chain. There appears to be a trade-off between immutability and data integrity or trust within the network[56]. In fact, if data in blocks could be easily altered, both data integrity and the trust of chain participants may be compromised. On this, it is important to anticipate that there are discrepancies in the perception of immutability as an intrinsic property of DLT, as some regard it as a "desired goal that some infrastructures try to achieve"[57], rather than a codified and always-present feature. However, the European Data Protection Board (EDPB) in paragraph 50 of "Guidelines 02/2025 on processing of personal data through blockchain technology" strongly affirms the difficulty of mutating the conditions of data in DLTs: *"[…] once stored on a blockchain, the data will stay on the blockchain with no practical possibility of deletion or modification in most cases. Even though it is technically possible to modify a blockchain, such modifications are very hard to put in place as it requires that all nodes update their copy of the chain (or to delete their copy) and agree upon the change. This undermines the principles of consistency and tamperproof processing, which are the core of most blockchains design*"[58].

The challenge of applying the right to erasure in blockchain technology is determined by technical factors and governance design[59]. The two aspects are interconnected, yet distinct. The technical challenges are inherent to the design of many DLTs, which makes modifying or erasing data highly difficult, if not practically impossible, due to mechanisms of consensus protocols (e.g., Bitcoin's PoW,

[55] Belen-Saglam, Altuncu, Lu, and Li, "A systematic literature review of the tension between the GDPR and public blockchain systems", p. 2.
[56] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?", p. II.
[57] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, p. 18.
[58] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p 12.
[59] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" p. 75.

described in section 2.1.2). On the other hand, governance design pertains to the management of the information system by developers and key stakeholders, shaping how data are controlled and whether alternative solutions to deletion can be implemented[60].

To solve the difficulties of applying the right to be forgotten in blockchains, some technical solutions have been proposed over the years. Building mutable blockchain infrastructures, chameleon hashes, storing data off-chain, destroy the cryptographic linkages, and zero-knowledge proofs are some of the possibilities investigated (see Chapter 3). The governance challenge must also be carefully addressed, especially in those DLTs that adopt a decentralized and automatized governance structure.

In summary, to ensure effective compliance with Article 17 of the GDPR, it should be made possible to erase personal data stored in a distributed ledger technology (DLT), regardless of how "erasure" is defined. While this possibility is still widely considered difficult to implement, recent technical proposals, above all the 2024 Proof of Concept by the AEPD, in detail in section 2.3, and the 2025 EDPB recommendation have sought to address what appears to be a significant incompatibility between blockchain technology and Article 17 of the GDPR. Before delving into the analysis of possible solutions to this current incompatibility, it is necessary to first briefly outline two other key tensions in the relationship between GDPR and DLTs.

2.2.2 Other Conflicts: Identification of Controllers and Territorial Scope in Decentralized Ledgers

The challenges of applying the GDPR's principles to DLT extend beyond the conflict between blockchain's immutability and the right to erasure. At least two additional key issues must be considered for a comprehensive understanding of the situation: the identification of controllers in DLTs and the territorial scope of data processing activity.

The GDPR is based on the identification of certain key actors: above all the data subject, the data controller, and, if present, the data processor. The controller is defined in Article 4(7) GDPR as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […]*". The Regulation assumes

[60] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 5.

that every processing activity must have a data controller to whom data subjects can address to enforce their rights under the law[61]. The controller must therefore be accountable for data processing.

However, blockchains are inherently decentralized technologies designed to replace a central authority with many different players[62]. This creates an overarching challenge in clearly identifying the data controller and in establishing the assignment of responsibilities and accountability arising from the data processing activity. This is particularly true in the case of public blockchains, where all the peers may add transactions to the ledger without the control of any central authority. In these cases, every peer could be possibly considered a controller because of his actions[63]. In the case of private or permissioned blockchains the situation is typically more transparent, and the controller can be more easily identified[64]. In these cases, the nodes may act as data processors operating on behalf of the controller, who is generally the company that owns the DLT[65].

Moreover, the issue of controllership in public blockchain technology is complex and must be assessed on a case-by-case basis, as the system's architecture and governance framework can vary, influencing the identification of those who determine the purposes of processing activities[66]. Generally, diverse actors may be considered as data controllers in DLTs. The *Commission nationale de l'informatique et des libertés* (CNIL), the French data protection supervisory authority, released an opinion in September 2018 in which the issue was discussed. The CNIL defined as controllers the participants of the blockchain, specifically those "who have the right to write on the chain and who decide to send data for validation by the miners"[67]. More precisely, the CNIL identifies as controllers: (i) natural persons processing data for commercial or professional purposes, (ii) legal entities registering personal data on the blockchain, and (iii) groups of entities that collectively decide to conduct processing operations on a blockchain for a common purpose[68]. For example, miners in Proof-of-Work blockchains are not considered controllers by the CNIL because they do not define the purposes of transactions and of the processing activities but, in some cases, they are considered processors[69]. At

[61] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" p. II.
[62] *Ivi*
[63] Bayle, Koscina, and Manset, "When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry", p. 2.
[64] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p 40.
[65] European Commission, *European Blockchain Sandbox - Best Practices Report - 1st Cohort, Part B*, June 2024, p. 19.
[66] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" p. 45.
[67] Commission Nationale de l'Informatique et des Libertés, *Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, September 2018, p. 1.
[68] *Ivi*, p. 3.
[69] *Ibidem.*

the same time, the Opinion does not consider "natural persons who enter personal data on the blockchain, that do not relate to a professional or commercial activity" as data controllers "pursuant to the purely personal or household activity exclusion set out in Article 2 of the GDPR"[70].

CNIL's pronouncement leaves some ambiguity in defining controllers within public DLTs, especially regarding the possible overlap of the data controller and data subject and the reduced possibility for the actors to comply with the GDPR because of their limited control over the data[71]. Moreover, the literature reflects a lack of consensus on the identification of controllers in public DLTs, emphasizing the fact that the issue remains open and needs to be assessed case-by-case and requires further clarification by the EDPB[72]. To gain a more comprehensive understanding of the topic, it is recommended to refer to Chapter 4 of Finck (2019).

As previously discussed in section 2.1.2 the material scope of the GDPR is broad but somewhat ambiguous when applied to blockchain networks, in which data processing activities are inherently decentralized. Similarly, assessing the territorial scope of the GDPR in relation to DLTs presents significant challenges. According to Article 3 of GDPR, the regulation applies to the processing of personal data carried out within the European Economic Area (EEA) and extends extraterritorially to data processing activities conducted outside the EEA when they target or monitor individuals within the EU. This extraterritorial reach, which guarantees comprehensive data protection for European citizens regardless of where their data is processed, is linked to the so-called Brussels Effect, an influential concept developed by Professor Anu Bradford. It refers to the EU's ability to set a global regulatory agenda on certain issues, prompting other countries to replicate its regulatory efforts to some extent.

However, when considering blockchain networks, which operate beyond traditional jurisdictional boundaries, the territorial aspect introduces significant difficulties[73]. Transactions on public, permissionless blockchains occur simultaneously across multiple jurisdictions, with copies of the distributed ledger stored and maintained by nodes in various parts of the world. This raises uncertainties regarding which national Data Protection Authorities (DPAs) have the competence to

[70] *Ivi*, p. 2.
[71] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" p. 52.
[72] Ivi, p. 50.
[73] Bayle, Koscina, and Manset, "When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry", p. 2.

enforce GDPR obligations on blockchain participants[74]. Additionally, identifying an "establishment" within the EU, as required by Article 3(1) GDPR, becomes particularly challenging in blockchain ecosystems that rely on decentralized governance structures, such as Decentralized Autonomous Organizations (DAOs), rather than traditional legal entities with a fixed presence. In these cases "a functional approach ought to be adopted to determine where relevant activity for the specific processing in question was carried out"[75].

Having briefly examined two of the main tensions between DLTs and EU data protection law, it is evident that ensuring their harmonious coexistence presents significant challenges. These tensions, along with the conflict between immutability and the right to erasure, are not necessarily exhaustive; for instance, the principle of data minimization (defined in Article 5 of GDPR) can also be considered. It requires limiting the processing of personal data to what is strictly necessary and that may also be difficult to reconcile with the progressive accumulation of personal data within blockchain ledgers. However, the priority is to make evident that there must be an effort to let technology, in particular blockchain, comply with the law. The question that arises is from where this effort should primarily originate: should the burden fall on the technology itself, requiring developers and participants to design blockchain systems that align with EU legal data protection standards? Or should the law adapt to a certain extent in order to accommodate the unique characteristics of blockchain, requiring regulators to rethink existing frameworks?

The interplay between technology and legal frameworks has never been more interconnected. The challenge lies also in determining how the EU can assert its regulatory authority over emerging technologies while ensuring that innovation is not hindered in the process. The next section examines how a Supervisory Authority of a Member State managed to provide a technical solution to solve the challenge for DLTs to comply with Article 17 GDPR.

[74] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" p. 9.
[75] *Ibidem.*

2.3 The 2024 Spanish Data Protection Supervisory Authority Proof of Concept

On November 13, 2024, the Spanish Data Protection Supervisory Authority, *Agencia Española de Protección de Datos* (AEPD), released a paper titled "*Prueba de concepto Blockchain y el derecho de supresión*", a Proof of Concept (PoC) regarding the viability of building blockchain structures in compliance with the GDPR's right to erasure. Probably for the first time in Europe, the document represents the choice of a national authority to intervene in an active, functional, and documented manner in order to ensure compliance with the GDPR for data processing activities related to emerging technology such as blockchain. The AEPD paper seeks to demonstrate the feasibility of implementing the right to erasure in DLTs that were not originally designed to allow for it, providing detailed technical proof. Simultaneously, it encourages developers to integrate data protection strategies by design, in accordance with Article 25 of the GDPR.

The AEPD paper, released only in Spanish, is structured into three main sections. The first provides a contextual overview, explaining the technological and legal framework while addressing the "*equívocos*" related to blockchain, the misconceptions and common cognitive biases surrounding the technology. The second focuses on the proof of concept, detailing the technical steps necessary to ensure compliance with the right to erasure in blockchain systems. The final section presents and analyzes the results of the proof of concept. Alongside the document, the AEPD has also released a demonstrative video on their YouTube channel that illustrates the technical details of the PoC[76].

The technical details of the AEPD PoC will be discussed later in section 3.1. For now, it is essential to understand the foundations of the Spanish Authority's work and the contextual framework in which it was developed. This paper challenges the spread belief that the immutable nature of blockchain technology is fundamentally incompatible with the mutability and erasure requirements set out in the EU GDPR, as described in section 2.1.3.

2.3.1 The "*Equívocos*" of Blockchain Technology According to the AEPD

The AEPD provides an analysis of ten ambiguities ("*equívocos*") related to distributed ledger technology and its relationship with data protection principles. The most important *equívoco* is about the immutability feature of blockchain technology. The AEPD does not consider immutability as an intrinsic property of DLT but rather as a design objective or a requirement desired by certain

[76] Agencia Española de Protección de Datos, "Derecho al olvido y Blockchain: Prueba de concepto", video, November 13, 2024, https://www.youtube.com/watch?v=H7gnoI3B7SY.

blockchain infrastructures[77]. The immutability of DLT is not absolute because there are some scenarios in which the possibility of erasing or modifying data is permitted.

In fact, the AEPD states that it is possible for peers to agree on data erasure in a way that does not create inconsistencies in the chain. This is more probable to happen in a blockchain that operates with particular and unusual consensus mechanisms. However, the document also emphasizes that erasing data is easier to achieve in private blockchains, where governance systems are also more straightforward to manage. The paper also cites cyberattacks, block pruning, and project abandonment as scenarios in which the erasure of data may be accomplished. To summarize, while immutability in blockchains is not absolute, it appears to be more than just a desired characteristic for many infrastructures as the AEPD sustains. It is, in fact, a real fundamental characteristic, particularly in widely used public blockchains, which are to a certain extent based on it, and that render the modification of data particularly onerous, difficult, or even impossible[78].

The Spanish Authority highlights additional ambiguities in common perceptions of blockchain, particularly regarding its decentralization and the supposed absence of a governance structure. Decentralization, in fact, is not absolute across all DLT infrastructures, mainly due to the presence of miner or validator pools, who, even in large public blockchains, consolidate and exert significant decision-making power. For instance, in 2023, in Bitcoin five mining pools controlled 82% of the total mining power, posing a risk of cartel formation and undermining the decentralization of the network[79].

Regarding the governance structure, while most DLT projects operate under unconventional and often incomplete frameworks, they still possess governance mechanisms[80]. Decisions are typically made by founders, key developers, and influential community members, reflecting the centralization tendencies described earlier. When nodes and participants disagree on the state of the chain or advocate for changes to fundamental aspects, governance mechanisms can facilitate the implementation of such changes, sometimes resulting in the splitting of the chain into two or more separate entities, through a process known as “hard fork”. One of the most notable examples of a hard fork is the so-called “The Merge” of Ethereum which occurred in September 2022, in which the DLT transitioned from Proof of Work (PoW) to Proof of Stake (PoS) consensus mechanism[81]. This change was done to reduce the

[77] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, p. 18.
[78] Finck, “Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?” p. II.
[79] Simona Ram, “How Centralized Is the Bitcoin (BTC) Mining Sector?”, *DailyCoin*, February 7, 2023. https://dailycoin.com/bitcoin-mining-pool-sector-how-centralized-is-it/.
[80] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, p. 19.
[81] “The history of Ethereum”, Ethereum.org, last modified February 2025, https://ethereum.org/en/history/#paris.

computing demand of DLT, enhancing also the sustainability of the technology, and implementing its security and scalability[82].

The AEPD identified also other minor *equívocos*, most of which share two key aspects already present in the previously discussed points: the involvement of responsible individuals in the operation of DLT projects and the gap between real-world applications of blockchains, and the "ideal model", which many projects see as an unreachable goal towards the DLT must tend. The lack of control of data subjects over their personal data is described not as a limit of the blockchain technology itself, but rather as a problem related to how the DLTs are structured right now, which leads to incompatibilities with the GDPR. "If they [the developers] had considered compliance objectives from the design stage, the appropriate management mechanisms would have been implemented. And this is independent of whether we are dealing with any type of Blockchain infrastructure"[83].

[82] "Proof-of-Stake vs Proof-of-Work", Ethereum.org, last modified January 2024, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/pos-vs-pow/.
[83] Agencia Española de Protección de Datos (AEPD), *Prueba de concepto: Blockchain y el derecho de supresión*, p. 21.

2.4 Reconciling Law and Technology

Technology is playing an increasingly central role in people's daily lives and in the global economy. As a fundamental asset, it requires a carefully balanced regulatory approach, safeguarding the rights of those affected by its use while avoiding excessive restrictions that could hinder innovation, thereby stifling economic growth and competitiveness. The digital transition, in fact, necessitates a legal strategy, as already recognized in 2019 in the EU with the "A Europe fit for the digital age" policy plan implemented by the Commission President Ursula Von Der Leyen[84], but which did not have the intended impact, as many scholars and commentators agree, being overly defensive and inflexible[85].

However, without delving into a macro-geopolitical analysis level, it is important to state that the relationship between law and technology is inherently evolving and complex. This complexity arises from the challenges that emerging technologies pose to the legal boundaries set by regulators. Meanwhile, technology evolves independently of external factors, including jurisdictional constraints.

Blockchain technology exemplifies the difficulty of aligning legal imperatives with technological architectures. This section explores the importance of reconciling law with emerging technologies like blockchain, which, in its permissionless form, naturally conflicts with traditional regulatory approaches. The central question remains whether the law should dictate the design of DLTs or, alternatively, adapt to the technology through interpretative flexibility and evolving regulatory frameworks that reflect its constantly changing nature.

2.4.1 Blockchain Technology as "Originally Anarchic" and "Alegal"

The inherent nature of permissionless blockchains makes it challenging to interact within existing legal frameworks. The decentralization and disintermediation in these systems were intentionally designed by Nakamoto in 2008 as a means to bypass both economic and jurisdictional constraints, driven by an anarchic impulse that was central to the origins of DLTs[86]. Bitcoin was revolutionary precisely because it sought to challenge the state's monopoly over the financial sector, embodying what some anarchists regarded as a utopian ideal[87].

[84] Ursula von der Leyen, *Political Guidelines for the Next European Commission 2019-2024*, (Brussels: European Commission, 2019), p. 13.
[85] Henrique Schneider, "Europe's Innovation Problem: Trying to Regulate the Future", *GIS Reports*, December 2, 2024, https://www.gisreportsonline.com/r/innovation-regulation/.
[86] Brendan Markey-Towler, "Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using Blockchain", *The JBBA* Vol. 1, Issue 1, (March 2018), p. 15.
[87] *Ibidem.*

However, the anarchic ethos surrounding blockchain technology has gradually diminished as it has become increasingly widespread and integrated into state apparatuses. Rather than remaining a tool of "financial insurrection", blockchain has even been adopted by some governments as both a legal financial instrument and a store of value. A notable example is El Salvador, which in 2021 became the first country to recognize Bitcoin as legal tender. Although the country reversed this decision in 2025, it continues to maintain significant Bitcoin holdings as a reserve asset, as is also the case for other states, such as Bhutan[88]. Similarly, in March 2025, U.S. President Donald Trump, a fervent crypto-enthusiast, declared his ambition to establish the United States as "the Bitcoin superpower of the world and the crypto capital of the planet"[89].

This evolution highlights how the anarchic origins of blockchain technology have, in many cases, transformed into a more institutionalized framework. Yet, blockchain retains characteristics that remain difficult to encapsulate within conventional legal boundaries. The resistance to regulation has led some authors to describe blockchain as "alegal"[90]. The concept of alegality, developed by Hans Lindahl[91], refers to actions or phenomena that, at a given moment, "exceed the intelligibility of the law and cannot be reduced to the legal/illegal binary"[92]. Alegal acts or technologies exhibit a particular form of "strangeness"[93], making them difficult to categorize within the scope of legal orders, as in the case of permissionless blockchain technology.

The issue of alegality of DLTs has been explored by De Filippi, Mannan, and Reijers (2022). The authors delineate two primary approaches policymakers could adopt in response to the inherent alegal characteristics of blockchain technology: either by extending the scope of existing legal provisions to encompass blockchain within the legal framework or by narrowing the law's reach, thereby excluding certain activities from legal regulation[94]. These two approaches reaffirm the fundamental choice between prioritizing the supremacy of law or that of technology. However, it is crucial to consider whether a middle ground can be realistically achieved.

---

[88] Leo Schwartz, "Two small countries bet on Bitcoin—and it's paying off big time", *Fortune Crypto*, November 15, 2024, https://fortune.com/crypto/2024/11/15/el-salvador-bitcoin-holdings-500-million-bhutan-bukele/.
[89] David Yaffe-Bellany, "At Crypto Summit, Trump Says U.S. Will Be 'the Bitcoin Superpower'", *The New York Times*, March, 7, 2025, https://www.nytimes.com/2025/03/07/technology/trump-crypto-summit.html.
[90] Primavera De Filippi, Morshed Mannan, and Wessel Reijers, "The alegality of blockchain technology", *Policy and Society*, 41(3), (2022), p. 358.
[91] Hans Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-Legality*, (Oxford Academic, 2013).
[92] De Filippi, Mannan, and Reijers, "The alegality of blockchain technology", p. 360.
[93] Lindahl, *Fault Lines of Globalization: Legal Order and the Politics of A-Legality*, p. 157.
[94] De Filippi, Mannan, and Reijers, "The alegality of blockchain technology", p. 367.

2.4.2 A Dynamic Perspective

The digital revolution generated by the advent of the Internet posed numerous challenges that were difficult to address from a legal and regulatory compliance perspective. Lawmakers faced a significant challenge in regulating a global digital network. To tackle this issue, innovative strategies were adopted, such as initially refraining from directly regulating the behavior of individual Internet users and instead focusing on controlling gateways and Internet service providers[95]. Through the concerted efforts of governments and regulatory authorities, the Internet was integrated into existing legal orders, leading to amendments in certain legal provisions. A similar challenge arose with blockchain technology, presenting a regulatory conflict that is probably even more complex.

The alegality of DLTs, their ability to operate beyond traditional legal boundaries, has been, in some aspects, addressed by regulators, particularly in areas such as Anti-Money Laundering (AML) provisions and Know Your Customer (KYC) obligations imposed on cryptocurrency exchanges[96]. While these regulatory efforts have, to some extent, curtailed the decentralization objectives of many permissionless DLTs, their implementation remains challenging and, at times, difficult to enforce[97].

However, the challenge posed by blockchain technology in complying with legal frameworks, particularly in relation to the GDPR's right to erasure, represents a promising area for what Professor Giuseppe D'Acquisto describes as "an important experimental laboratory for addressing and resolving tensions between rights and technologies"[98]. In other words, the tensions offer an opportunity for reflection on an increasingly pressing issue, that needs to be addressed through a "dynamic dialogue between law and technology"[99]. Such an approach requires a multidisciplinary perspective on emerging technologies while ensuring the protection of fundamental rights and maintaining the centrality of the individual.

In the case of the conflict between blockchain and the GDPR's right to erasure, a "static and paralyzing"[100] opposition between law and technology risks leading to legal uncertainty. This could either result in difficulties in applying the law or, as is often the case, the almost complete disregard

[95] *Ibidem.*
[96] *Ivi* p. 365.
[97] *Ivi* p. 367.
[98] Giuseppe D'Acquisto, "Blockchain e GDPR: verso un approccio basato sul rischio", *Federalismi.it*, n. 2, (2021), p. 65.
[99] *Ibidem.*
[100] *Ibidem.*

for regulatory provisions. A notable example is the right to erasure within large permissionless blockchain networks, such as Bitcoin, where compliance remains today largely unaddressed.

In summary, regulators must be ready to intervene in a dynamic manner to reconcile legal frameworks with technological developments, considering the evolving nature of regulatory objectives. This can be pursued, for example, by seeking to govern technological processes through regulatory-technical guidance, as demonstrated by the approach of the AEPD in relation to the GDPR's right to erasure, where technical imperatives suggestions were derived from legal compliance requirements (in detail in section 3.1). A strict and severe regulatory approach to blockchain, where applied, could however have adverse effects on governance oversight, as participants in blockchain projects may choose to relocate to more lenient jurisdictions[101].

Concurrently, regulators should remain open to more innovative and nuanced approaches capable of addressing these challenges with greater adaptability. One such approach is the implementation of regulatory sandboxes: controlled environments in which stakeholders directly involved in the development and use of emerging technologies can test their solutions while benefiting from temporary exemptions from specific regulatory obligations[102]. Sandboxes (analyzed deeply in section 4.1: Regulatory Sandboxes and the Importance of Dialogue and Experimentation) offer a valuable opportunity to better understand the technologies and the legal complexities they encounter while fostering interdisciplinary and multi-stakeholder dialogue. Such frameworks are likely to benefit both regulators and innovators, who can be seen as complementary actors rather than opposed in the development of responsible innovation.

In recent years, the European Union has established several regulatory sandboxes, including the European Blockchain Sandbox, launched in 2023 with the primary aim of establishing a "pan-European framework for regulatory dialogues to increase legal certainty for innovative blockchain technology solutions"[103]. In the following chapter, which adopts a more technical perspective on the compatibility between the right to erasure and distributed ledger technologies, a case study involving a participant in this sandbox initiative will be examined in detail.

[101] De Filippi, Mannan, and Reijers, "The alegality of blockchain technology", pp. 367-368.
[102] De Filippi, Mannan, and Reijers, "The alegality of blockchain technology", p. 368.
[103] "European Blockchain Sandbox", European Commission, accessed March 2025, https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en.

Chapter 3
Technical Adaptations to Implement the Right to Erasure in Blockchain Technology

This chapter will focus on a technical and practical perspective regarding the compatibility between the GDPR's right to erasure and blockchain technology. While an in-depth computer engineering analysis of the various specific technical strategies falls outside the scope of this work, it remains essential to provide an overview of the most recent mechanisms that could facilitate compliance, also considering the connected governance aspects of the proposed solutions.

The chapter will examine the solution proposed by the Spanish Supervisory Authority through its Proof of Concept, and will analyze as case study the GiottoChain project, developed by the Italian company Almaviva, which participated in the European Blockchain Sandbox. The final section will provide a comprehensive analysis of the most promising technical methods for adapting DLTs to the requirements of Article 17 of the GDPR.

3.1 The AEPD Proposal

3.1.1 The Proof of Concept Implementation

The Spanish Data Protection Supervisory Authority (AEPD) released in November 2024 a Proof of Concept aimed at reconciling the right to erasure with blockchain technology, as introduced in section 2.3. In the document, the AEPD offered a detailed use case of data cancellation related to the activity of a private user inside a blockchain infrastructure. The operation consists of the erasure of the address of an account through overwriting either the account address itself or the transaction signature from which the address can be derived[104].

The PoC is implemented on a private blockchain based on Ethereum version 1.13.15 (April 2024), which works on a particular type of consensus mechanism named Proof of Authority (PoA), specifically a configuration called *clique*. The process of data erasure can be divided into five procedures (as described by Figure 2): 1) the individuation of the data to be modified; 2) the generation of a new version of the blockchain through an hard fork (a splitting of the DLT, as already described

[104] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, p. 27.

in section 2.3.1); 3) the distribution of the new version; 4) the technical strategy for the consensus on the new version; and 5) the organizational measures to be adopted for the blockchain management.

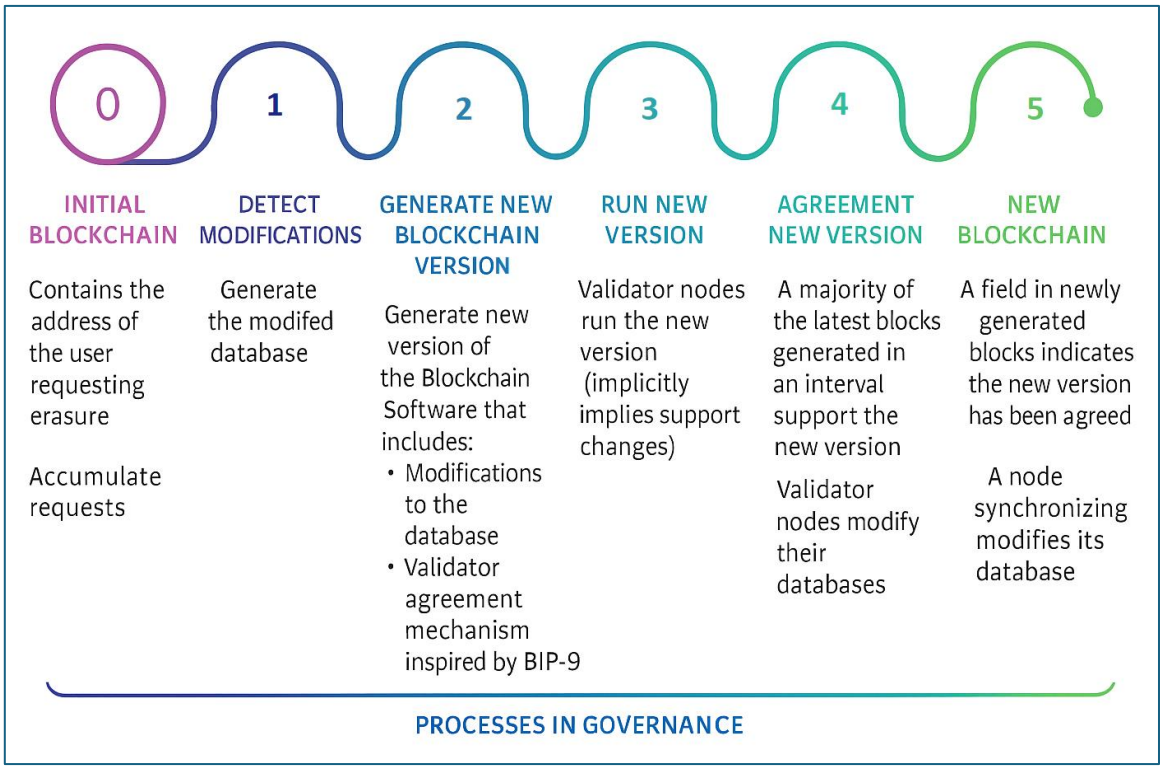

Figure 2 – Phases of the PoC. Source: Adapted and translated from Figure 10 of Agencia Española de Protección de Datos, "Prueba de concepto: Blockchain y el derecho de supresión" (2024).

As a first step, the PoC implements a mechanism to identify the data related to the user concerned. The detection process must locate all the blocks containing transactions linked to the user's activity, including all the interactions with smart contracts. This is done through an auxiliary node, avoiding influencing the ledger before the hard fork, which copies the blockchain database and analyzes it to find the data that need to be erased. The modifications are then stored in a file that will be used to update the blockchain through a hard fork.

Once the concerned data have been identified, the Ethereum source code (the set of programming instructions that define the platform's functionalities) is modified to include the necessary changes. First, the code is updated to introduce new functions that allow the nodes to reach an agreement, following the logic of the Bitcoin Improvement Proposal BIP-0009 mechanism. These functions also enable the modification of each node's local database. Once these modifications are completed, the software is compiled and made available to all participating nodes. At this stage, the validator nodes update their software, and the new blocks generated include an indicator that signals the change. When, within a predetermined interval, the majority of blocks contain this indicator, consensus is

considered to have been reached. The validator nodes then proceed to update their local databases by replacing the relevant data. This marks the occurrence of the hard fork.

From that moment on, any node wishing to synchronize with the network must update its software to the new version. Otherwise, it will no longer be able to synchronize, given that the network has undergone a structural change due to the hard fork. If synchronization takes place after consensus has been reached, the node will update its database by detecting the indicator in the most recent block. If synchronization occurs beforehand, the update will be automatically applied as soon as consensus is achieved.

3.1.2 Proof of Authority, Decentralization, and Replicability of the Proof of Concept

The AEPD undoubtedly had a valuable intuition in developing the Proof of Concept, shedding light on a pressing issue. However, certain aspects of the initiative make it difficult to consider this as a replicable model or a definitive reference point for ensuring blockchain-GDPR compliance with regard to the right to erasure. Even the authors, in the conclusion of the PoC, emphasize that the work constitutes a laboratory experiment not intended for commercialization, but rather aimed at encouraging developers of such projects to adopt strategies that support data protection compliance by design[105].

The reduced transferability of the AEPD model to other context is mainly due also to the fact that the blockchain infrastructure in which the PoC operated is an example of a DLT that, to some extent, deprecates decentralization, an element that was central to the original concept of blockchain and remains fundamental in most of the widely used blockchain systems today (in depth in section 2.2). Decentralization is mainly constrained through the consensus mechanism employed by the DLT: the Proof of Authority (PoA).

PoA is derived from the Proof of Stake (PoS) consensus mechanism, which is the underlying consensus mechanism in the Ethereum infrastructure. Created to mitigate the energy consumption derived from the computational power requested by Bitcoin's Proof of Work, PoS, simplifying, determines the next eligible block to be appended to the chain on the basis of the current stakes held by the accounts (the probability of being designated as a validator increases proportionally with the

[105] *Ivi* pp. 53-54.

amount of stake held)[106]. The stakeholders agree to lock part of their stake to become validators, and they receive a fee when they participate in the validation of new blocks. Instead, in Proof of Authority infrastructures, the validators are not chosen according to their stake amount but rather are selected through their reputation on the network[107]. Nodes must disclose their real identities and link them with their on-chain ID to apply to be validators.

While Proof of Authority is an efficient consensus mechanism for private DLTs, even more than PoW or PoS[108], it clearly departs from the more traditional models and diverges significantly from the original idea (or ideal) of blockchain. In fact, PoA is a consensus mechanism used almost exclusively for permissioned DLTs, as can be inferred from its functioning, which stands in contrast to the decentralization principle. The very idea of having small groups of predetermined validators, who in practice hold authority over decisions concerning the ledger, is fundamentally opposed to the principles of distribution, decentralization, and the anarchic features that were, and in some public blockchains still are, central.

Back to the Spanish Supervisory Authority's Proof of Concept, it is undeniable that the solution offered to comply with the right to erasure has been posed in a controlled environment with a relatively centralized ledger. While it is important to acknowledge the uncommon effort made by a public authority to govern and propose a solution to a complex technical issue, and although the AEPD stated that the aim was to integrate compliance by design into the technology itself[109], it remains challenging to affirm that the PoC is replicable across a wide range of blockchains, particularly public, decentralized ones operating under different consensus mechanisms, which are the majority. For private blockchains, it could represent a viable option; however, the hard fork mechanism remains subject to debate due to the time delays that it may involve in executing data erasure[110]. In the APED document, it is stated that the hard fork-based data erasure mechanism developed would comply with the timeframe set out in Article 12, paragraph 3 of the GDPR[111]. The provision requires data controllers to act on data subject requests within one month of receipt, with the possibility of extending

[106] Peng Zhang, Douglas C. Schmidt, Jules White and Abhishek Dubey, "Consensus mechanisms and information security technologies", in *Role of Blockchain Technology in IoT Applications*, ed. Shiho Kim, Ganesh Chandra Deka, Peng Zhang (Academic Press, 2019).
[107] *Ibidem.*
[108] *Ibidem.*
[109] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión*, p. 27.
[110] Xin-Yu Li, Jing Xu, Ling-Yuan Yin, Yuan Lu, Qiang Tang and Zhen-Feng Zhang, "Escaping from Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting", *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 5, (2023), p. 2.
[111] Agencia Española de Protección de Datos, *Prueba de concepto: Blockchain y el derecho de supresión, p. 32.*

the period to up to three months in cases of particular complexity. The timing of the erasure is undoubtedly a relevant element in the technical implementations of the data erasure process.

In conclusion, the AEPD's Proof of Concept represents a valuable contribution to the ongoing debate about reconciling blockchain technology with data protection requirements, in particular with the right to erasure. This is also confirmed by the use of the AEPD PoC as a reference in the recent EDPB guidelines document published in April 2025[112]. The Spanish Authority's effort demonstrates that technical adaptations are possible within controlled, permissioned environments. However, its reliance on a relatively centralized infrastructure and the use of a consensus mechanism such as Proof of Authority, far from the decentralization that characterizes most public blockchains, presents concerns in considering the PoC as a replicable or scalable solution. Rather, it should be viewed as a targeted experiment with limited generalizability, useful more as a stimulus for further innovation in compliance with Article 17 GDPR than as a regulatory or technical model.

While the AEPD PoC offers a significant step towards reconciling blockchain with data protection, the GiottoChain project provides real-world insights into the challenges of the topic. As explored in the following case study, the project presents a practical and comprehensive application of data handling procedure mechanisms within GDPR compliance.

[112] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, Version 1.1, April 8, 2025, pp. 9, 14, 20.

3.2 The Almaviva GiottoChain Case

This section is dedicated to analyzing, as a case study, the GiottoChain project. A common misconception is that blockchain technology is solely confined to the world of cryptocurrencies. However, as previously discussed, blockchain technology is used for a variety of purposes across different sectors. The GiottoChain project, developed by the Italian company Almaviva since 2018, stands as a virtuous example of an innovative and practical application of blockchain technology in a context that extends beyond the crypto-world.

The significance of the project lies in its configuration, in the data protection framework developed, particularly with regard to the compliance with the right to erasure, and in its participation in the first cohort of the European Blockchain Sandbox. These aspects are thoroughly examined here thanks to the kind support of Almaviva staff, who agreed to be interviewed to provide insights and details on the project. I want to express my sincere gratitude to Geltrude Amodio, Head of DLT Solutions & Token Platform, Emanuele D'Agostini, Head of Game Changing Technologies Lab, and Gianluigi Mascia, Head of Digital Compliance & RegTech, for their availability and assistance in supporting this study.

3.2.1 The Project: Notarization Service in Public Blockchain

Figure 3 - GiottoChain Logo. Source: "Notarizzazione Blockchain", Almaviva, accessed April 2025, https://notarizzazione.almaviva.it/

GiottoChain is an innovative initiative that enables the notarization of documents and assets on the blockchain. The notarization process is traditionally aimed at ensuring the accuracy of an activity between parties or at verifying the authenticity of a document through a trusted central authority, such as a notary, who attests to the truthfulness and correctness of the event[113]. The use of blockchains in the notarization field, a sector that is often reluctant to innovation, is extensively researched and

[113] Tonino Palmisano, Vito Nicola Convertini, Lucia Sarcinella, Luigia Gabriele, and Mariangela Bonifazi, "Notarization and Anti-Plagiarism: A New Blockchain Approach", *Applied Sciences* 12, no. 1: 243, (2022), p. 1.

explored, as DLTs have the potential to replace the trusted authority in certain practices[114]. In particular, the authority figure can be replaced in fixed-date notarization practices, such as those offered by the GiottoChain service. These practices involve authenticating the existence of a document and confirming the date of its creation (or, more precisely, the date of its "blockchain-notarization") in an unequivocal manner[115]. Fixed-date notarization does not certify the genuineness of the content of the notarized asset but guarantees the integrity of its existence in a secure and verifiable way[116].

GiottoChain offers a notarization service for any digital asset on public blockchain infrastructures, "certifying them and guaranteeing integrity, paternity, against fraudulent usage"[117]. The service is offered as a "Software-as-a-Service" (SaaS), facilitating for clients to adopt it through a model that mirrors the Web 2.0 approach. However, it is, in fact, a product that aligns closely with the decentralization principles of Web 3.0.

The notarization process is conducted on stable public blockchains, specifically Ethereum and Bitcoin. The decision to run the project on these types of DLTs rather than on a private blockchain, which probably would have been easier to manage in certain aspects, demonstrates a commitment to the decentralization and disintermediation of the notarization experience. This approach is inherently linked to the original features and purposes of blockchain, as discussed in sections 2.2 and 2.4.

To provide a general and simplified overview of how GiottoChain works, clients wishing to notarize digital assets (e.g. presentations, press releases, or other types of documents) can contact Almaviva or reach the service through various marketplace platforms. Almaviva offers to clients, most of whom are public entities, a flexible and modular experience, providing the blockchain nodes that support the process. The digital assets are hashed, processed through additional algorithms, and subsequently notarized through blockchain transactions. The hash (the concept is explained in section 2.1.2) serves as an "immutable digital fingerprint", meaning that even a single bit change in the original document would result in a completely different hash value[118]. Each transaction recorded on the blockchain inherently attests to its immutability and non-repudiation, ensuring the information in the ledger remains unchanged. This notarization service guarantees the authenticity and integrity of the digital

[114] Shinya Haga, and Kazumasa Omote, "Blockchain-Based Autnomous Notarization System Using National eID Card", *EE Access*, vol. 10, (2022), p. 87477.
[115] *Ivi* p. 87478.
[116] *Ivi* p. 87479.
[117] "Notarizzazione Blockchain", Almaviva, accessed April 2025, https://notarizzazione.almaviva.it/.
[118] *Ibidem.*

asset by assigning a timestamp and an identifiable owner to each transaction[119]. Customers receive a receipt confirming the notarization process. The technology used to generate these receipts is Chainpoint 2.0, an open standard that allows for verifying and certifying the integrity of data on a blockchain by creating the secure timestamp that proves the data existed at a specific moment in time and could not be altered.

As an extremely innovative project, particularly within the Italian and European contexts, GiottoChain offers interesting opportunities to explore the relationship between such a novel approach and data protection practices. It is crucial to investigate whether personal data is involved in the notarization process, the role of Almaviva in this context, and how the project ensures compliance with the right to erasure.

3.2.2 Data Protection in GiottoChain and the Right to Erasure Compliance

The data protection issue in GiottoChain is complex, but it provides an opportunity to explore how DLTs can be compliant with the GDPR. Although the system was developed well before the release of the EDPB's "Guidelines 02/2025 on the processing of personal data through blockchain technologies," in some ways, it aligns with similar conclusions for what concerns the right to erasure topic.

Firstly, it is important to underline that, in most cases, GiottoChain does not process personal data, as it primarily serves public bodies and private firms. In these contexts, data related to individuals are excluded from the operations and therefore the situation falls outside the scope of the GDPR, as defined by Art. 2 of the GDPR. However, the system can potentially be used by private individuals to notarize personal data, but the customers' intentions must be previously disclosed to the company, and an agreement on the presence of personal data must be established. In such cases, which are the focus of this scrutiny, Almaviva would be considered as the processor of the personal data, while the customer of GiottoChain would act as the data controller, solely determining the purposes of the processing activity (for more about the identification of controllers in DLTs, see section 2.2.2). The client, and thus the controller in this case, chooses to manipulate his own data through blockchain infrastructure, while Almaviva provides the technical instruments to process the data. In this way, the Italian company would have the obligations, accordingly with Art. 28 GDPR, to respect the instructions of the controller without acting autonomously in the processing activity.

[119] European Commission, *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part A*, December 2023, p. 37.

This definition of the roles is well delineated in paragraph 11.2 of the General Terms and Conditions of GiottoChain (that must be approved by the customers before starting the contractual relationship): "*The Client remains the sole and exclusive owner of the processing of all data collected, processed, handled, processed, stored and communicated using and during the use of the Product, assuming all liability law in this regard and undertaking to hold harmless the Supplier and the Almaviva Group all claim, action, process, penalty, payment or other injury resulting from the processing of personal data operated by the Client or on its behalf. In the event that the Client should call on the Supplier in order to execute its ownership and/or responsibility process, the Client and the Supplier will provide to stipulate an ad hoc agreement concerning the processing of personal data, drafted according with Article 28 of European Union Regulation 2016/679 – General Protection Regulation, with the attribution of the role of additional responsible and/or responsible to the Supplier.*[120]"; and in paragraph 11.3: "*During the term of the Contract, should it become necessary for the Supplier to process personal data on behalf of the Client, as data controller, the Parties undertake to cooperate in order to ensure compliance with the applicable legislation on the protection of personal data, appointing, by way of example but not limited to, the Supplier as data processor, pursuant to Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council.*[121]"

Furthermore, Almaviva does not have any direct contact with personal data, if they are present. In fact, the data are transformed into hashes using SHA-256 algorithms directly by the client on their hardware and then transmitted to Almaviva in hash form. Hashes are widely considered, also by the EDPB/Article 29 Working Party since 2014[122], as pseudonymized data (more in depth in sections 2.1.2 and 2.2.1), but still remain unintelligible to almost everyone. Hence, Almaviva processes the hash using aggregation procedures to make it inseparable from a set of information that generates "noise" before being inserted into the blockchain through transactions. This ensures that only the client can establish a connection between what ends up on-chain and the off-chain data.

In these cases, even if the controller is the customer itself, and Almaviva is the processor, in the event of a request for erasure of the hashed-pseudonymized data, what can be assured is the deletion of the off-chain data, which would allow for the indirect identification of the data subject, thereby rendering the on-chain stored data completely anonymous. This is, as previously mentioned, the "preferred" solution of the EDPB, outlined in paragraph 64 of the Guidelines: "*[…] It might be possible,*

[120] Almaviva, *GiottoOnChain General Terms and Conditions (SaaS)*, last modified May 11, 2023, p. 6.
[121] *Ivi* p. 6-7.
[122] Article 29 Data Protection Working Party, *Opinion 5/2014 on Anonymisation Techniques*, April 10, 2014, p. 20.

depending on the type of blockchain and the way transactions are recorded, to modify off-chain data so that the data subjects involved in the transaction are no longer identifiable with reference to data remaining on the chain. Such modification will likely preclude any use of the data stored on the chain for the original specified purposes beyond the maintenance of the blockchain structure. This means that the "anonymised transaction" would have lost all its semantics, but still exists to allow the verification of integrity for other, remaining transactions"[123].

Additionally, there may be further customers' personal data off-chain, which have been collected for the GiottoChain project but not directly embedded into the notarization service. Almaviva processes these additional data outside the scope of the decentralized service itself (e.g., contact information). In these cases, the application of the right to erasure would be carried out by simply deleting the off-chain data.

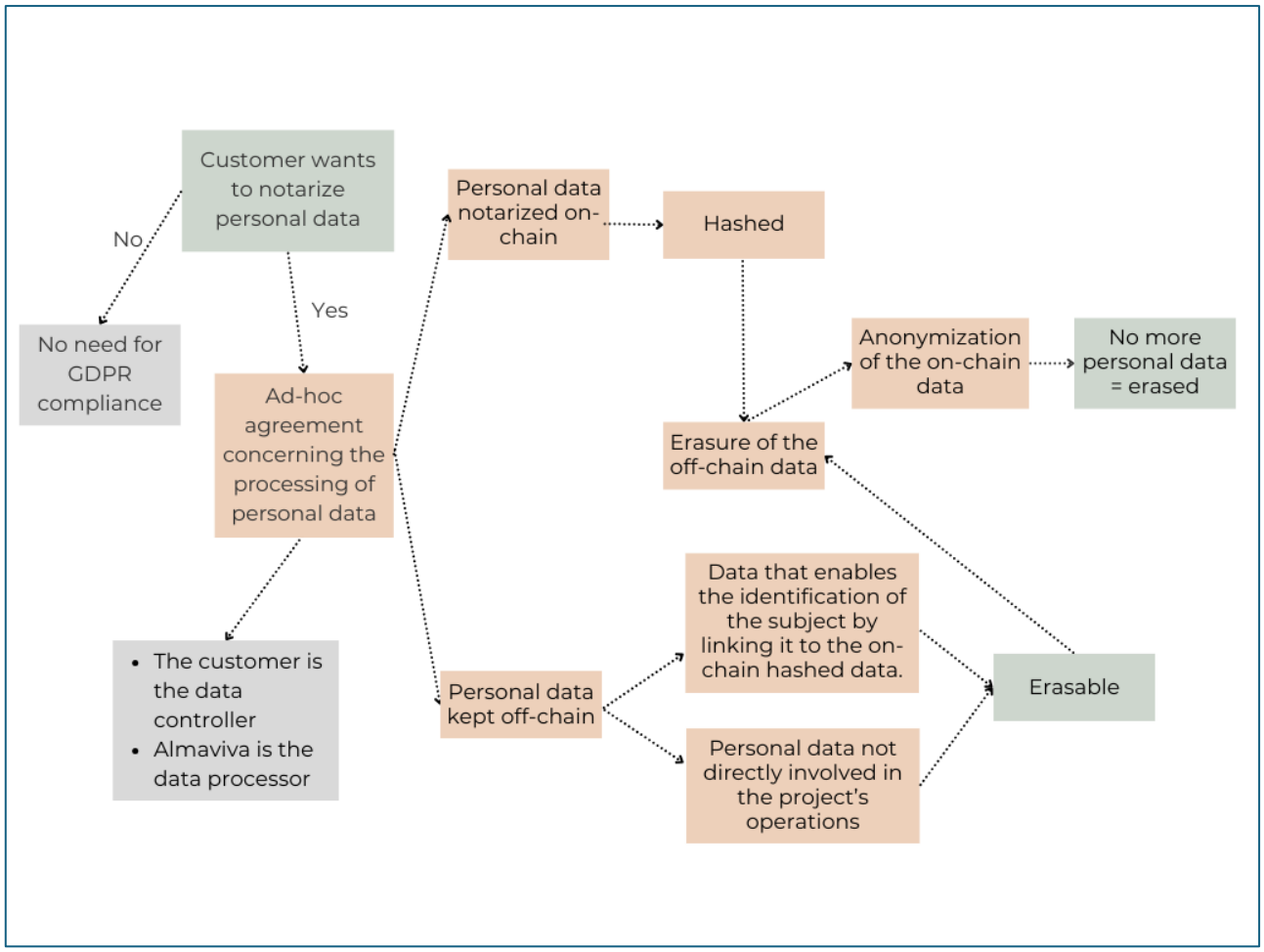

Figure 4 - Flowchart illustrating the simplification of the personal data handling process and GDPR's right to erasure compliance in GiottoChain. Source: Author's elaboration.

[123] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, Version 1.1, April 8, 2025, p. 20.

This mechanism (see the flowchart in Figure 4), described and implemented in the GiottoChain project, demonstrates a commitment to personal data protection by design and by default, as prescribed by Article 25 of the GDPR and stressed by the recent EDPB Guidelines[124]. Although the issue was particularly challenging due to the legal uncertainties it entailed, especially in the early stages of GiottoChain's development in 2018, over the years, through data protection assessments, experimentation, and careful legal analysis of the case, the project eventually received qualification from the *Agenzia Per l'Italia Digitale* (AgID) (whose responsibility for qualifications have now been delegated to the National *Agenzia per la Cybersicurezza Nazionale* (ACN)[125]). The AgID qualification also included a data protection assessment and enabled Almaviva's notarization solution to be marketed even before participating in the European Blockchain Sandbox initiative, in which GiottoChain joined the first cohort. The sandbox itself, an interesting and innovative project within the European Union framework, is explored in the following paragraph.

3.2.3 The European Blockchain Sandbox Initiative

The European Blockchain Sandbox initiative responds to the call contained in the 2020 European Union Council document, *"Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-friendly, Future-proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age"*, in which the Council urged the European Commission to foster innovation through experimentation and to implement regulatory sandboxes in cooperation with Member States[126]. The Commission promptly responded to this request by establishing the European Blockchain Sandbox, within the scope of the European Blockchain Services Infrastructure (EBSI), following an open call in 2022 for the creation of the leading consortium. It led to the involvement of the law firm Bird & Bird, its consulting arm OXYGY, blockchain experts, and independent academics.

The project was officially launched on February 14, 2023, with an open call for use case applications suitable for the sandbox, specifically innovative decentralized technology solutions. Notably, one of the selection criteria for the use cases was the maturity of the business development, alongside their

[124] *Ivi* p. 16.
[125] "Oggi il Processo di Qualificazione Cloud per la PA Passa ad ACN", Agenzia per l'Italia Digitale, January 19, 2023, https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/01/19/oggi-il-processo-qualificazione-cloud-pa-passa-ad-acn.
[126] European Union Council, *Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age*, December 23, 2020, paras. 14-15, p. 3.

legal and regulatory relevance and their alignment with EU policy priorities[127]. The characteristic of being near, or already at, the commercialization stage of the DLTs, and the importance of this factor in the selection for the first cohort of the sandbox, already indicates an approach oriented towards helping regulators to better understand the technology rather than the establishment of an environment primarily devoted to experimentation, also regarding early-stage products. The inclusion of Almaviva's GiottoChain, a product already certified by the AgID Italian authority and already actively in commerce, further highlights this approach.

Nineteen use cases were selected, originating from all EU regions and with applications relevant to different industries (as highlighted in the chart in Figure 5)[128]. At the same time, different national authorities were selected to participate in the subsequent dialogue meetings on the basis of their interest in the use case applications. For companies with less experience in blockchain-related matters, experts on the subject were made available. Almaviva, however, chose not to rely on this support, instead providing the authorities and consortium experts with a fully functional demo of GiottoChain that pragmatically explained and showcased the application use, the functioning of the aggregation algorithms, and the overall technical aspects of the project.

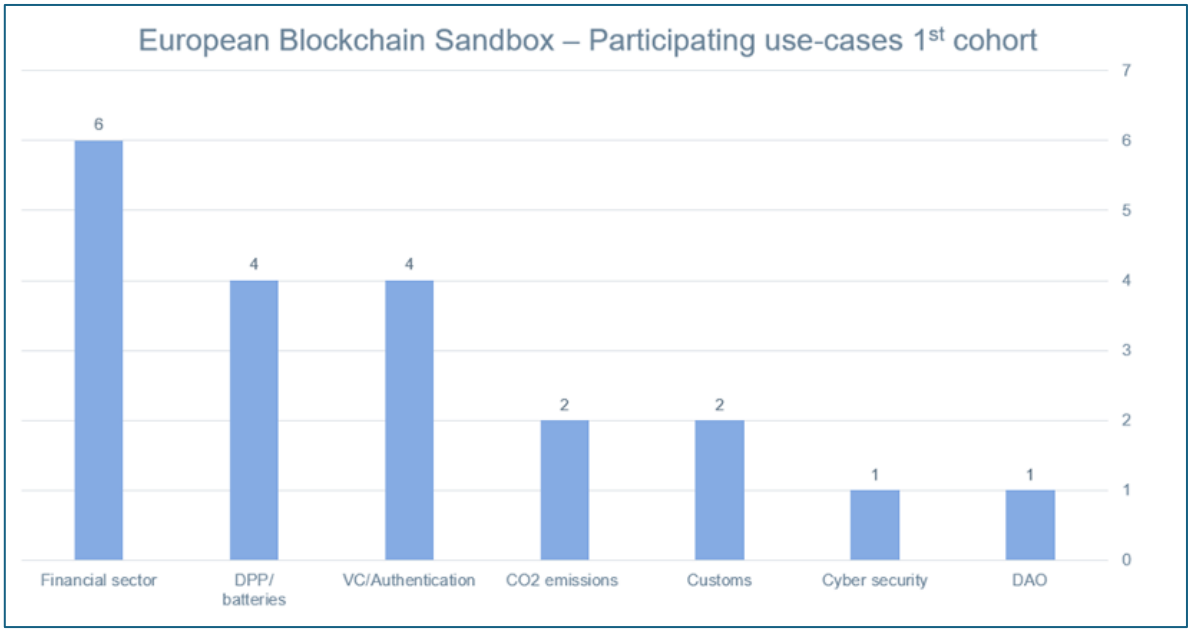

Figure 5 - Bar chart illustrating the distribution of participating use cases in the European Blockchain Sandbox's first cohort. Source: European Commission, European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part A, Abstract and Executive Summary, December 2023, p. 9.

[127] European Commission, *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part A, Abstract and Executive Summary*, December 2023, p. 8.
[128] *Ivi*, pp. 8-9.

For the sandbox, several dialogues were held by Almaviva, also with the participation of the Italian Data Protection Supervisory Authority, the "*Garante per la Protezione dei Dati Personali*". According to the firm-side participants, the dialogues were productive for Almaviva, and the exchanges appeared to be reciprocal. The *Garante* gained a deeper understanding, particularly of the technical aspects and the use case, while the company expanded its knowledge, especially regarding specific measures and updates. Almaviva's experts viewed the experience of engaging with the authorities positively, also due to an effective organizational structure of the sandbox.

The regulator's focus on understanding the specific characteristics of the use cases is central to the sandbox, as highlighted in the second best practices report (part B) produced during the sandbox's operation[129]. The recognition of the structural differences within blockchain technology, depending on its specific use, has led to the need for an in-depth understanding of the various possible applications.

Part B of the "Best Practices Report", written in collaboration with all the cohort participants, also includes a dedicated chapter on data protection compliance. The report recommends DLTs' data protection compliance by design and by default, as outlined in Article 25 of the GDPR, emphasizing the importance of integrating this concept from the very beginning of the decentralized product's development[130]. In this way, the document anticipated the approach that would later be adopted in the EDPB's 2025 Guidelines[131]. Additionally, the best practices from the first cohort reaffirm the pseudonymized, rather than anonymized, nature of encrypted and hashed personal data, given their persistent linkability to off-chain personal data[132]. However, the presence of adequate encryption measures or privacy-enhancing technologies, determined on a case-by-case basis, which render the data highly unintelligible, is considered a method of reducing the risk of re-identification of the data subject, and consequently, is viewed as a facilitative measure for GDPR compliance[133].

The best practices report also emphasizes the importance of assessing data protection roles within blockchain technologies. The conclusion it reaches is similar to what is outlined in the GiottoChain case: *"*[1] *If the DLT provider does not process any personal data but only develops and sells software*

[129] European Commission, *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part B, Abstract and Executive Summary*, December 2023, p. 9.
[130] European Commission, *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part B,* December 2023, p. 16.
[131] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p. 16.
[132] European Commission, *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part B,* pp. 16-17.
[133] *Ivi* p. 19.

but the customer decides how the software is used without any involvement by the DLT provider and the DLT provider cannot see which data is used (including which data is stored) and also does not have the keys to decrypt the data, and does not have a say in who is processing the data, then the DLT provider would likely be neither a controller nor a processor under GDPR, but only a mere technology provider. [2] *This could be different if the DLT provider (and not the customer) would determine the settings and thereby determine essential means or if it would receive diagnostic/telemetry data for its own purposes. In that case, the DLT provider could qualify as a controller or a joint controller.* [3] *If the DLT provider would be able to view personal data (e.g. see or store user accounts or diagnostic/telemetry data) for support purposes on behalf of the customer, the DLT provider could qualify as a data processor for this data processing"*[134].

The GiottoChain case seems to largely fall under the third formulation [3], although the first [1] also has some points of contact with the practical reality of the service provided. However, the definition of a simple technology provider appears too restrictive given the scope of Almaviva's involvement in managing the service. The role of the processor thus seems appropriate, even though Almaviva, contrary to what is defined in [1], cannot view any of the notarized personal data, apart from their unintelligible hashed version (for further details, see the previous section, 3.2.2).

Regarding the compliance with the right to be forgotten under Article 17 GDPR, the European Blockchain Sandbox documents highlight the problematic nature of the issue, which must still be addressed through a case-by-case assessment[135]. However, the issue is briefly approached and "solved" through the disconnection of the link between on-chain hashes and the off-chain data that may permit the reverse engineering, thereby anonymizing the data in the ledger[136]. What is outlined by the sandbox reports is very much aligned with Almaviva's approach and the way in which data deletion requests should practically be handled within GiottoChain. This reflects the collaborative nature of the drafting of the best practices document. Nonetheless, in the paper is noted that such an off-chain storage solution would require an external architecture to manipulate the data in order to anonymize the on-chain data[137]. This would, in turn, necessitate another infrastructure (non-decentralized), implying the need for an additional risk assessment system[138].

[134] *Ivi* p. 20.
[135] *Ivi* p. 22.
[136] *Ibidem.*
[137] *Ibidem.*
[138] *Ibidem.*

In conclusion, the experience gained so far by the first cohort of the European Blockchain Sandbox (the initiative is still ongoing and possibly subject to future developments) seems quite effective in providing a dialogue platform between companies with innovative DLT projects and regulatory authorities. This is evident in the cases related to data protection discussed here, which anticipated by a few months some of the conclusions that the EDPB only reached in April 2025. This does not imply that the sandbox documents necessarily inspired or influenced the EDPB in drafting the Guidelines, but the alignment of conclusions in certain areas suggests that the sandbox has likely contributed to the development of effective and forward-looking best practices.

Nonetheless, it is also important to briefly reflect on the non-standard and unconventional nature of the European Blockchain Sandbox. While usually a sandbox is a mechanism to establish a controlled environment for early-stage companies to experiment with new technologies and business models, benefiting from temporary exemptions from legal requirements in that controlled environment[139], it must be noted that the European Blockchain Sandbox does not offer regulatory exemptions for experimentation[140]. This characteristic likely makes the initiative an atypical thematic sandbox, functioning more as a multistakeholder dialogue development environment rather than a space where practical innovation, especially in terms of private sector technological advancements, is actively pursued. These aspects are, however, primarily addressed later in this research, in the section dedicated specifically to regulatory sandboxes as innovation projects for both regulatory and technological development.

[139] De Filippi, Mannan, and Reijers, "The alegality of blockchain technology", p. 368.
[140] "Frequently Asked Questions", European Blockchain Services Infrastructure, European Commission, FAQ no. 64, https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Frequently+Asked+Questions.

3.3 Possible Technical Solutions for Blockchain Compliance with Article 17 GDPR

This concluding section explores the major technical solutions available for blockchain compliance with the GDPR's right to erasure, focusing on previously examined approaches and promising methods highlighted in the 2025 EDPB Guidelines. The possibilities examined are the development of mutable blockchain projects, such as the AEPD's Proof of Concept (PoC), discussed in section 3.1.1, and the practice of off-chain data storage.

Mutable DLTs can be realized through several technologies embedded in the ledger structure, such as chameleon hashes. Additionally, the practice of storing data outside the chain in decentralized contexts, coupled with the potential destruction of decryption keys, offers another valuable approach. This method is illustrated through the GiottoChain case study, specifically discussed in section 3.2.2, and is strongly endorsed by the EDPB Guidelines of April 2025[141]. Finally, a brief overview of zero-knowledge proof technology will be provided, as it is an interesting and current area of study that could serve as a privacy-enhancing solution within DLT environments.

The section is intentionally not deeply technical, as this is not the ultimate goal of the research. However, the delineation of the various aspects is made possible through the thorough review of papers and documents, which are used as references and may provide a more profound understanding of the issue.

3.3.1 Mutable Blockchain Infrastructures and Chameleon Hashes

Deprecating the immutability feature of DLTs allows for updating and removing data from the decentralized ledger through technical methods. The Proof of Concept of the Spanish Data Protection Supervisory Authority provides a feasibility study of a mutable blockchain through the establishment of governance processes that include hard forks. The PoC, as described in section 3.1.2, was developed in a controlled environment within a permissioned blockchain, and it utilized a consensus mechanism, Proof of Authority, which facilitated an effective governance process. This process covered all steps, from identifying the data to its deletion and the hard-forking phase. Regarding the replicability and scalability of the AEPD solutions, doubts remain, as discussed in section 3.1.2.

[141] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, pp. 13,14,20.

However, the establishment of redactable DLT infrastructures is not limited to the use of hard forks in relatively centralized environments. For instance, projects are exploring the use of chameleon hashes, cryptographic functions that allow for rewriting blocks of information under specific constraints[142]. The concept was already pioneered by Krawczyk and Rabin in 1997 in the context of digital signatures[143], and has more recently been adopted for the purposes of redactable blockchain technology[144].

Incorporating chameleon hashes into the blockchain framework allows for rewriting or updating blockchain content without compromising the integrity of the entire ledger. Chameleon hashes rely on a secret "trapdoor" key, a secret key used in cryptography that allows someone to reverse a cryptographic operation, such as decrypting or modifying data, in an otherwise secure system[145]. Only those who know the secret key can access or alter the data. Thus, if the key is known, the hash can be rewritten to match a new set of data. The very concept is well-simplified by Ateniese et al. (2017): "The best way to grasp the concept of a redactable blockchain is to think of adding a lock to each link of the hash chain (see Figure [6]): Without the lock key it is hard to find collisions and the chain remains immutable, but given the lock key it is possible to efficiently find collisions and thus replace the content of any block in the chain. With the knowledge of the key, any redaction is then possible: deletion, modification, and insertion of any number of blocks. Note that if the lock key is lost or destroyed, then a redactable blockchain reverts to an immutable one"[146].

[142] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 5.
[143] Hugo Krawczyk, and Tal Rabin, "Chameleon Hashing and Signatures", *Theory Of Cryptography,* (October 1997).
[144] Bill Buchanan, "Chameleon Hashes", *Medium*, December 22, 2022. https://medium.com/asecuritysite-when-bob-met-alice/chameleon-hashes-c9e969a91ccb.
[145] *Ibidem.*
[146] Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, and Ewerton Andrade, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends", *IEEE EuroS&P*, (April 2017), p. 3.

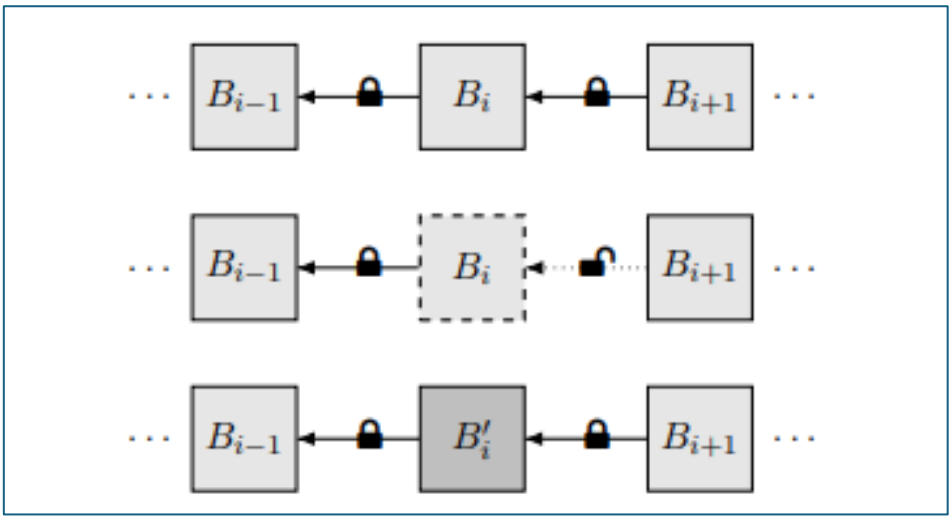

Figure 6 - Redaction operations on a redactable blockchain. Source: Giuseppe Ateniese, Bernardo Magri, Daniele Venturi, and Ewerton Andrade, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends", IEEE EuroS&P, May 2017.

This chameleon hashes mechanism ensures, in theory, that blockchain content can be modified in specific cases, such as when personal data needs to be erased under GDPR compliance. The system also ensures that only authorized entities with the trapdoor key can perform such redactions, preventing unauthorized changes to the blockchain[147]. However, this allocation of responsibilities and authorities for the key management, similar to other solutions previously examined, could be viewed by some as a "betrayal of the decentralization principle"[148]. Additionally, this solution could be more easily implemented in a private DLT environment, while for public blockchains, it presents more complexity.

Nonetheless, introducing technical characteristics to make blockchains mutable is an interesting way to comply with the right to erasure, despite the cost of implementation and the challenges involved in applying this solution to already developed blockchains[149]. While the idea holds promise, especially in contexts that require data flexibility, it also raises concerns about maintaining the core principles of decentralization and security, as well as the recurrent issue regarding whether "the value of blockchain lies when it becomes editable"[150].

3.3.2 Off-Chain Data Storage and Key Destruction

[147] *Ibidem.*
[148] Ugo Pagallo, Eleonora Bassi, Marco Crepaldi, Massimo Durante, "Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure", in *Legal Knowledge and Information Systems*, IOS Press, (November 2019).
[149] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 5.
[150] Henry Chang, "Blockchain: Disrupting Data Protection?", *Privacy Law & Business International Report*, (November 2017), p. 3.

Another possible solution for achieving compliance with the right to be forgotten in blockchain infrastructures is off-chain data storage. This option, strongly recommended in the EDPB's April 2025 Guidelines, involves storing only the hashes of data on-chain, while the actual data is securely stored outside the blockchain, which acts as "access control point"[151]. The data is, therefore, as suggested by the EDPB in paragraph 54, to be considered as stored in the DLT in a manner that serves as a proof of existence: *"Whenever it is necessary to store personal data on the blockchain, it is better to store the data in a form which is primarily intended to function as a proof of existence18 (e.g. by use of a pointer, a cryptographic commitment or a hash generated from a keyed hash function, etc.) on the blockchain, with the data that should be used to verify the proof being kept outside of the blockchain (such as, for example, on the data controller's information system). This must be done ensuring a high level of confidentiality"*[152].

The GDPR obviously applies to both off-chain data, which must be handled separately appropriately and in compliance with the data subject's rights, and the hash of the data stored on-chain (this situation is very similar to the case study on the GiottoChain project discussed in section 3.2)[153]. The GDPR applies to the hash as well, since, as mentioned multiple times, it is considered pseudonymized data, due to the reversibility of the process. However, while it is still possible to reverse the hash, retrieving the original off-chain data from it is highly complex[154].

Off-chain storage allows for the anonymization of the hash by deleting the off-chain data, for which the hash serves as proof of existence. Alternatively, the key responsible for linking on-chain and off-chain data can be destroyed, making the linkage impossible. The irreversible anonymization of data, obtained through the elimination of the possibility of reconnecting on-chain and off-chain data, would be considered as data erasure, thus complying with Article 17 GDPR.

While this architecture is certainly promising and theoretically simpler to implement compared to other solutions, it undoubtedly presents some disadvantages. The most significant one is that off-chain data still needs to be handled separately, requiring an additional storage system[155]. This introduces another layer of data processing activity in a separate external infrastructure, which must be carefully assessed to minimize risks to individuals' data protection rights as outlined in the GDPR. Additionally, off-chain data storage may also lead to increased vulnerabilities in terms of security and potential data

[151] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 4.
[152] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p. 13.
[153] *Ivi* p. 12.
[154] *Ibidem.*
[155] *Ibidem.*

breaches, and may also increase the operational complexity of managing two or more different systems dedicated to data processing[156].

Furthermore, the off-chain storage system previously described could, in many cases, be viewed as a negation of the blockchain system itself and would only be reasonable in certain applications. However, as seen and documented in the GiottoChain project (discussed in detail in section 3.2.2), such applications do indeed exist.

Off-chain data storage does not fully leverage the benefits of decentralization, such as transparency, disintermediation, and the inherent security of the system[157]. Moreover, this approach is more feasible in permissioned private blockchains or those based on consortiums than in permissionless DLTs. Another concern is the potential presence of indirect personal data traces left on-chain during the hashing process, in the form of wallet keys or similar identifiers[158].

Nevertheless, it is important to reiterate that the solution described here is both interesting and potentially effective, particularly for ensuring compliance between blockchain technology and the right to erasure. However, this is contingent on proper implementation and adaptation to the specific use case. The process could also be facilitated by complementing it with cryptographic techniques, such as the zero-knowledge proof that will be briefly examined in the next section.

3.3.3 Zero-Knowledge Proof Technologies

A promising tool for blockchain-GDPR compliance is represented by zero-knowledge proof (ZKP) technologies. These innovative cryptographic methods are based on the concepts already introduced in 1985 by Goldwasser et al. in the paper "The Knowledge Complexity of Interactive Proof-Systems"[159]. ZKPs "allow one party to prove to another that a statement is true without revealing any additional information"[160]. This means that the verification of the information occurs without disclosing the underlying data, including personal data.

---

[156] Andries van Humbeeck, "The Blockchain-GDPR Paradox", *Journal of Data Protection & Privacy*, 2(3), (2019).
[157] *Ibidem.*
[158] van de Giessen, "Blockchain and the GDPR's Right to Erasure", p. 6.
[159] Daljit Singh, "Exploring Blockchain with Zero Knowledge Proof Uses", *Debut Infotech*, January 6, 2025, https://www.debutinfotech.com/blog/zero-knowledge-proof-uses.
[160] Patrizio Germani, Michelangelo Amoruso Manzari, Riccardo Magni, Paolo Dibitonto, Fabio Previtali, and Emanuele D'Agostini, "Building Trustworthy AI Systems: AI Inference Verification with Blockchain and Zero-Knowledge Proofs", *6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, (2024), p. 1.

In the context of many DLTs, in which the transparency is also directed towards the users' credentials, implementing zero-knowledge proof systems may provide the infrastructure with enhanced privacy and security, while maintaining transaction confidence, and importantly, securing the decentralization principle[161]. As D'Acquisto explains, by using ZKPs before storing the data on-chain, the data can be transformed into "new IT objects", specifically in the form of cryptographic commitments that are only usable within the blockchain, with no possibility of making them interoperable in other contexts[162].

The properties of ZKP cryptographic systems thus also allow for compliance with Article 17 of the GDPR. The innovative ZKP cryptography offers data subjects the possibility of being less identifiable, promoting anonymization and, consequently, "erasure through invalidation"[163]. This is made possible through a combination of the previously described operations of off-chain personal data storage and on-chain storage of only hashes manipulated with ZKP techniques[164]. Zero-knowledge proofs, in fact, not only enhance the confidentiality level but also may prevent the reconnection of on-chain data to external identifiers, thus achieving the objective of the right to be forgotten.

The solution of applying zero-knowledge proof architectures to blockchains in order to comply with GDPR requirements is also positively mentioned by the EDPB in the 2025 Guidelines. Specifically, paragraph 24 of the Guidelines explains how ZKPs are one of the cryptographic solutions to hide the identities of DLT participants, transforming the ledger into a "zero-knowledge blockchain": *"The initial concept of blockchain includes transactions where the identities of the parties involved are visible to all. Some blockchains provide ways of hiding those identities to most people reading the chain using advanced cryptographic tools. While zero knowledge proofs are only one of the cryptographic solutions used for this, the blockchains using such tools are often called "zero knowledge blockchains"*[165].

The adoption of zero-knowledge blockchain structures is definitely considered important by the EDPB. In fact, in the 2025 Guidelines, the authority also recommends considering ZKPs in the

[161] Singh, "Exploring Blockchain with Zero Knowledge Proof Uses".
[162] D'Acquisto, "Blockchain e GDPR: verso un approccio basato sul rischio", p. 64.
[163] Dave Zein, Wiktor Pinkwart, Catarina Silva, Geoffrey Goodell, Harris Niavis, Jonathan Heiss, Jörn Erbguth, Sharmin Chougule, Sophoclis Stephanou, and Stéphanie Attias, "Leveraging Zero-Knowledge Proofs for GDPR Compliance in Blockchain Projects", *INATBA Position*, (October 2024), pp. 5-6.
[164] *Ibidem.*
[165] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p. 8.

evaluation of blockchain data processing activities, indirectly encouraging the widespread adoption of such cryptographic techniques[166].

In conclusion, ZKPs are undoubtedly a promising method for blockchains to become more responsive to data protection requirements, including the right to erasure. Moreover, the compatibility of ZKPs with the decentralization principle and their potential application to public DLTs is a significant development, highlighting the importance of continued research and implementation in real-life use cases.

[166] *Ivi* p. 11.

Chapter 4
Finding Compatibility

After having analyzed both the legislative and technical aspects that make the compatibility between blockchain technology and the right to erasure difficult, it is crucial to explore how such compatibility could be facilitated and achieved, and by which actors. This chapter is therefore divided into two parts: the first revisits the concept of regulatory sandboxes, viewing them both as a tool for dialogue between legislators and innovators and as a mechanism for facilitating and incubating the innovation process itself. The following section will address the tensions between the key actors involved in the compatibility of emerging technologies and regulation. This section seeks to address whether it is more beneficial to pursue and adopt a compromise position between regulation and innovation, or if regulation should take a more authoritative enforcement role when it deals with complex issues, such as the blockchain/right to erasure compliance.

4.1 Regulatory Sandboxes and the Importance of Dialogue and Experimentation

4.1.1 Overview and Global Expansion of Regulatory Sandboxes

Although there is no widely accepted definition of regulatory sandboxes, Ranchordás and Meoli consider them as "regulatory tools allowing businesses to test and experiment with new and innovative products, services or businesses under supervision of a regulator for a limited period of time"[167]. In fact, the sandbox instrument is a relatively new practice, having been adopted only since the mid-2010s to address the regulatory challenges associated with the digital transformation[168]. The first experiences with regulatory sandboxes took place as part of the 2014 "UK's Global FinTech Policy", a project initiated by the United Kingdom Financial Conduct Authority to "advance effective competition in the interests of consumers"[169]. While currently sandboxes remain primarily used in the FinTech sector, their application has also expanded to various other industries, including green finance, telecommunications, energy, healthcare, and more[170].

[167] Sofia Ranchordás, and Roberta Meoli, "Regulatory Sandboxes for Sustainable Finance", *SSRN Electronic Journal*, (December 2024), p. 252.
[168] Angela Attrey, Molly Lesher and Christopher Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age,* OECD Going Digital Toolkit Notes, No. 2, OECD Publishing, (Paris, 2020), p. 6.
[169] Sofia Ranchordás, "Experimental Lawmaking in the EU: Regulatory Sandboxes", *University of Groningen Faculty of Law Research Paper Series*, No. 12, (2021), p. 3.
[170] *Ivi* p. 266.

As data shows, the adoption of regulatory sandboxes is expanding globally. In 2020, the World Bank Group (WBG) reported 73 sandboxes in 57 jurisdictions[171]. More recently, the Centre for Competition Policy (CCP) Regulatory Sandbox Portal tracks 199 sandboxes across 92 countries[172], underscoring the increasing adoption of these tools worldwide. Most of these experiences are conducted in developed countries, with three countries alone (the United States of America, Singapore, and the United Kingdom) accounting for 25% of the world's sandboxes[173].

The European Union has been encouraging the implementation of regulatory sandboxes since 2020[174]. Recommendations from the European Council have been adopted by EU institutions, leading to the publication of papers that outlined the specifics of European sandboxes, particularly in the fields of innovation and technological transition[175]. This has also resulted in practical examples of thematic sandboxes, such as the European Blockchain Sandbox. Furthermore, the topic is addressed in detail in the EU's AI Act, specifically in Article 57, which establishes a framework for the creation and operation of AI regulatory sandboxes within the EU, with the purposes of designing, testing and developing AI solutions in a controlled environment, under the supervision of the relevant authorities[176].

4.1.2 Regulatory Sandboxes: Objectives and Experimental Traits

Regulatory sandbox practices, which Ranchordás refers to as "experimental legal regimes"[177], are also primarily aimed at creating a supportive environment for both innovators and regulators. The objectives of sandboxes can vary: while some focus mostly on fostering innovation, others are more concerned with ensuring compliance with regulations and reducing the uncertainty that often arises in the context of emerging technologies. In this regard, the WBG provides a non-exhaustive categorization of sandboxes based on their objectives, which are often transversal.

---

[171] "Key Data from Regulatory Sandboxes across the Globe", World Bank Group, last modified November 1, 2020, https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe.
[172] "Portal On Regulatory Sandboxes", Center for Competition Policy, Accessed May 2025, https://competitionpolicy.ac.uk/research-projects/portal-on-regulatory-sandboxes/.
[173] Raphael Markellos, Sean Ennis, Bryn Enstone, Anastasios Manos, Dimitrios Pazaitis, and Dimitrios Psychoyios, "Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies", *SSRN Electronic Journal*, (March 2024), p. 12.
[174] European Union Council, *Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age*, December 23, 2020, paras. 14-15, p. 3.
[175] Venizols Efthymiou, Nikos Hartziargyrou, Mark McGranaghan, Marco-Robert Schulz, Jochen Kreusel, Ricardo Almeida Henriques, Andrei Morch, Dagmar Jarásová, Rad Stanev, Aris Dimeas, Athanase Vafeas, Michele de Nigris, Iva Maria Gianinoni, Rainer Bacher, Mahboubeh Hortamani, and Shafi Khadem, "Regulatory Sandboxes - Policy Report drafted by WG5's Regulatory Sandboxes Task Force", *ETIP SNET*, Publications Office of the European Union, (2023).
[176] *Artificial Intelligence Act*, art. 57, "AI Regulatory Sandboxes", https://artificialintelligenceact.eu/article/57/.
[177] Ranchordás, "Experimental Lawmaking in the EU: Regulatory Sandboxes", pp. 1-2.

According to this classification, there are: 1) Policy-focused sandboxes, used for evaluating regulations or policies; 2) Innovation or product-focused sandboxes, aimed at encouraging innovations and specific innovative products, including market entry; 3) Thematic sandboxes, focused on a specific theme, policy, or product with the objective of accelerating adoption (this is the case of the European Blockchain Sandbox, described in section 3.2.3); and 4) Cross-border sandboxes, which support firms' cross-border operations while fostering regulatory cooperation[178]. These varying aims are frequently embedded in a broader context of enhancing dialogue between actors who may not often interact on such issues, fostering mutual learning, and collaboration, facilitating knowledge transfer, and thus helping regulators in understanding new technologies[179].

It is also important to consider that regulatory sandboxes not only offer a controlled environment for testing innovations but can also assist policymakers' decisions, leading to legislative changes[180]. Conducting tests, regulators can gather data that highlights the need for legislative updates. For example, the Capital Markets Authority (CMA) of Kenya used its regulatory sandbox to refine guidelines for debt-based crowdfunding; in Brazil, the LIFT initiative of the Central Bank employed its sandbox to assess regulatory risks and identify necessary changes[181]. According to a survey conducted by the WBG and the Consultative Group to Assist the Poor (CGAP) think tank, around 50% of authorities reported making regulatory adjustments based on live-testing results, demonstrating how sandboxes can drive regulatory evolution and better align the legal framework with the needs of emerging markets[182].

However, regulatory sandboxes are implemented differently across various contexts and by different stakeholders, varying in terms of objectives, participation conditions, and other factors. One of the consolidated assumptions about this practice is its limited (both temporally and spatially) waiver of regulatory requirements for a circumscribed group of actors focused on a specific issue. This characteristic, aimed at offering regulatory flexibility[183], is also recognized by many institutional actors, as evidenced also by the definition contained in a paper published by the Organisation for

[178] Mandepanda Sharmista Appaya, Helen Luskin Gradstein, and Mahjabeen Haji Kanz, *Global Experiences from Regulatory Sandboxes*, World Bank Group, Fintech Note No. 8, (Washington DC, 2020), p. 6.
[179] Dirk Zetzsche, Ross P. Buckley, Douglas W. Arner, and Janos Nathan Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", *European Banking Institute Working Paper Series,* no. 11, (2017), p. 51.
[180] Appaya, Gradstein, Kanz, *Global Experiences from Regulatory Sandboxes*, p. 26.
[181] *Ibidem*.
[182] *Ibidem*.
[183] Zetzsche, Buckley, Arner, and Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", p. 51.

Economic Co-operation and Development (OECD) in 2020: "A regulatory sandbox refers to a limited form of regulatory waiver or flexibility for firms, enabling them to test new business models with reduced regulatory requirements"[184]. In this way, the sandbox creates a "safe space" for firms to innovate in a controlled environment, in which regulatory authorities observe, dialogue, and eventually intervene[185].

As previously described in section 3.2.3, there are also cases of regulatory sandboxes, particularly within the European Union, where the principle of limited waiver or suspension of certain regulations within a controlled environment has not been applied. In the case outlined in Chapter 3, specifically the 2023 European Blockchain Sandbox and, more notably, the experience of the first cohort where Almaviva participated with the GiottoChain project, the sandbox was implemented as a platform for active dialogue between innovative companies and startups. However, there was no possibility for companies to benefit from existing regulatory derogations[186], thus limiting the experimental scope of the initiative and excluding a fundamental recognized feature of the sandbox tool.

Regarding individual EU member states, a notable example is LBChain, a thematic regulatory sandbox launched by the Bank of Lithuania (BOL), which focuses on fintech firms and blockchain startups.[187]. It provides both regulatory and technological support directly from experts backed by the financial institution. The goal of LBChain is to offer companies the opportunity to gain new knowledge, conduct blockchain-oriented research and tests, and to adapt blockchain-based services[188], with a focus on innovation and business development more than on regulatory aspects.

In conclusion, considering the proven effectiveness of many sandbox experiences and the growing global adoption of these solutions, it would be preferable that the EU, as is already occurring, continues to expand the implementation of these tools, although in a more flexible manner. A more experimental approach, or what Zetzsche et. al refer to as "structured experimentalism"[189], could therefore yield multiple positive outcomes. Among these, there could be: economic growth, stimulating competition, and the attraction of talent and developers in the tech field[190]. If addressed

[184] Attrey, Lesher and Lomax, "The role of sandboxes in promoting flexibility and innovation in the digital age", p. 7.
[185] *Ibidem.*
[186] "Frequently Asked Questions", European Blockchain Services Infrastructure, European Commission, Accessed May 2025, FAQ no. 64, https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Frequently+Asked+Questions.
[187] Appaya, Gradstein, Kanz, *Global Experiences from Regulatory Sandboxes*, p. 24
[188] "LBChain", Lietuvos Bankas, Accessed May 2025, https://www.lb.lt/en/lbchain.
[189] Zetzsche, Buckley, Arner, and Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", p. 64.
[190] Appaya, Gradstein, Kanz, *Global Experiences from Regulatory Sandboxes*, p. 35.

more proactively and flexibly, the approach could lead to less uncertainty and, consequently, greater development, also implementing legislative changes.

Thematic DLTs' regulatory sandboxes, with controlled environments for testing innovative DLT products, with potential regulatory suspensions or relaxations, could involve the innovative technologies described in section 3.3, such as zero-knowledge proofs and chameleon hashes. This would help to understand how best to implement the protection of personal data and related rights, such as the right to erasure. It seems, therefore, that to facilitate this to happen, regulators must foster even greater openness, engaging in constructive dialogues with developers, startups, and firms, but also implementing flexible experimentation and research from both a technological and legislative standpoint.

4.2 Regulatory Enforcement or Compromise?

In summary, the emerging and innovative blockchain technology poses significant challenges in terms of compliance with some data protection rights outlined in the EU's GDPR. In particular, as previously discussed, what raises concerns is compliance with the right to be forgotten (Article 17 of the GDPR), which allows data subjects to request and obtain, under certain conditions, the deletion of their data by data controllers. This possibility of erasure is made very complicated, if not impossible in certain situations, by the very characteristics of many DLT configurations, especially public and non-permissioned blockchains, which feature immutability and append-only traits (in-depth in section 2.2.1).

In Chapter 3, after describing a notable practical case study, some possible technical solutions to the problem were outlined. These solutions, which include cryptographic commitments, chameleon hashes, and zero-knowledge proofs, can be, however, in some cases, difficult for blockchains to implement, costly, or challenging to integrate into already operational and advanced DLT systems. The question is then if regulators, in addition to suggest and promote the application of these technologies (as also recommended in the EDPB Guidelines 02/2025[191]), could further assist technology developers and the technology itself by finding workable compromises between the current regulations and the innovative component of the regulated material, in this case, the blockchain itself. Such an approach, however, would require a partial disregard of, or at least flexibility towards, current GDPR norms, which stand in stark contrast to an authoritative enforcement approach of the rights granted by the GDPR and the resulting compliance requirements.

The issue thus becomes crucial in terms of the approach adopted by European regulators, in terms of flexibility, openness, and even experimentation, given the contradictions and "rough edges"[192], as defined by D'Acquisto, between law and technology. While apparently, in recent years, there has been little openness in this regard, and, particularly in some cases like the AI Act, a reluctance to truly understand what was being regulated, following instead the objective of "being the first to regulate"[193], it is also true that recently something is changing, at least in the data protection field. Exemplary cases in this way include national authorities like the AEPD, which has taken the lead in the blockchain-

[191] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p. 8.
[192] D'Acquisto, "Blockchain e GDPR: verso un approccio basato sul rischio", p. 65.
[193] Media2000, "AI Act, Filiberto Brozzetti (Luiss): Qual è l'obiettivo strategico che l'UE si propone?", last modified March 14, 2024. https://www.media2000.it/ai-act-filiberto-brozzetti-luiss-qual-e-lobiettivo-strategico-che-lue-si-propone/.

GDPR compliance process, with the drafting in November 2024 of the PoC document, engaging in a detailed and technical discussion to contribute to the topic. This input was also acknowledged by the EDPB, which, in its Guidelines published a few months later, refers to the work of the Spanish authorities multiple times.

4.2.1 The EDPB "Guidelines 02/2025 on the Processing of Personal Data Through Blockchain Technologies": Between Openness and Caution

Specifically regarding the "Guidelines 02/2025 on the processing of personal data through blockchain technologies", it is essential to analyze them both in terms of their content and the posture adopted by the European Data Protection Board. The guidelines have long been strongly advocated by many. In fact, there have been calls since 2019 for regulatory guidance on certain elements of the GDPR in relation to blockchain infrastructures, in order to enhance legal certainty within the GDPR framework[194].

The document, finally made public in April 2025 during the drafting of this research work, is undoubtedly interesting from several perspectives. First and foremost, the recognition of the challenge that blockchain technologies pose in relation to the GDPR, and particularly to the right to erasure, is clearly defined[195]. It is therefore significant how the EDPB, in drafting the guidelines, repeatedly discourages the use of blockchain technologies for storing personal data, due to the risks that the technology itself may pose to individuals' rights and freedoms during data processing activities[196].

Despite this pronounced rejection of blockchain as a potential repository for personal data, in its various applications, which often require such storage, the EDPB also provides practical advice for those wishing to use DLT solutions[197]. Among the solutions proposed, there are innovative technical tools, such as the already mentioned zero-knowledge proofs, cryptographic commitments, data hashing, and the storage of data outside the chain with proof-of-existence in-chain (more in-depth in section 3.3). Additionally, there are procedural practical aspects that are recommended. These include the EDPB's emphasis on considering the principles of compliance by design and by default, as well

[194] Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?", p. 102.
[195] European Data Protection Board, *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*, p. 2.
[196] *Ivi* pp. 2,3, 11, 18, 19, 21.
[197] *Ivi* p. 12.

as the conduct of Data Protection Impact Assessments (DPIA), fundamental and specifically detailed for blockchain use cases[198].

This dualism in the EDPB's guidelines, strong discouragement and almost aversion towards the use of DLT technology on one hand, and a proactive approach offering recommendations for organizational, technical, and governance combinations for compliance on the other, is particularly interesting. It certainly reflects the role of enforcement authority within European regulation and also reveals a good degree of realism in addressing the complicated and multifaceted issue of blockchain compliance with European law. It also shows insightful technical understanding and openness in this regard, though this is always counterbalanced by the continuous discouragement of the technology itself, which is seen as a threat to data protection and is deemed preferable not to be used for such purposes, in favor of less risky alternatives.

4.2.2 A Flexible and Pragmatic Regulatory Approach

It is crucial to advocate for greater awareness among regulators regarding digital compliance with data protection in blockchain technologies. Since the EDPB Guidelines specifically target DLT solutions that are still in development[199], where implementing data protection by design measures is possible, and recognizing that private or permissioned blockchains are considered more easily solvable than public blockchains[200], it becomes evident that, particularly for large public and non-permissioned DLTs, which are widely used, such as those dedicated to the development of cryptocurrencies, a legislative gap remains. This gap concerns the application of certain GDPR rights, including the right to erasure.

Therefore, it would be desirable, and it is the responsibility of European lawmakers, to resolve the previously mentioned incompatibility between law (GDPR) and technology (blockchain). To do so, legislators may adopt stringent enforcement mechanisms, or alternatively, they could find compromises that facilitate compliance for DLT solutions that, by their very nature, are otherwise impossible to reconcile. While adopting a severe approach may hinder innovation processes, regulatory flexibility should instead entail a relative interpretation of the law, considering the pragmatic effectiveness of the GDPR application in the specific context, and ultimately, it may

[198] *Ivi* p. 16,18,19.
[199] *Ivi* p. 6.
[200] *Ivi* p. 10.

produce socially beneficial effects. The aim would be to avoid "purely formal GDPR compliance"[201] when applying the individual rights enshrined in the regulation.

Such a flexible approach towards law interpretation (realistically difficult to be implemented and accepted) would also align with the general simplification and "slashing" of regulation in the tech and sustainability sectors, which seems to have gained traction during the second European legislative term of the Commission President Ursula von der Leyen[202]. Many believe this could also lead to a forthcoming revision of certain aspects of the GDPR, seen as "untouchable" for a long time[203]. In this regard, a revision could represent a great opportunity for regulators to pragmatically modify certain "rigid" regulatory positions towards emerging technologies such as blockchain, possibly also introducing partial exemptions if well justified[204].

This position of regulatory simplification of EU legislation has also been shared by Mario Draghi, former President of the European Central Bank and former Prime Minister of Italy, who, in his September 2024 report focused on the future of European competitiveness, warned against the risk of overregulation, particularly the overlap between AI and data protection regulation[205]. He also criticized the EU's stance towards the tech sector, which complicates the economic behavior of companies and market players, ultimately hampering innovation[206].

This discussion remains embedded in the "dynamic" perspective discussed in section 2.4.2, where it has been stated that the static nature of the law should not compromise technological and innovative development. Without "yielding" to technology, the law should ethically safeguard individual rights, always seeking, through a risk-based approach, to assess the risks and benefits arising from the regulatory stance and adjusting accordingly. In doing so, relating to data protection, there must also be always present the idea of data protection not as an absolute right, but as a right that "must be considered in relation to its function in society and be balanced against other fundamental rights", as defined in Recital 4 of the GDPR.

[201] D'Acquisto, "Blockchain e GDPR: verso un approccio basato sul rischio", p. 63.
[202] Ellen O'Regan, "Europe's GDPR privacy law is headed for red tape bonfire within 'weeks'", *Politico*, April 3, 2025, https://www.politico.eu/article/eu-gdpr-privacy-law-europe-president-ursula-von-der-leyen/.
[203] *Ibidem*.
[204] Anisa Mirchandani, "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR", *Fordham Intellectual Property, Media, and Entertainment Law Journal,* Vol. 29, XXIX, no. 4, (2019), pp. 1240-1241.
[205] Mario Draghi, *The Future of European Competitiveness – Part B: In-depth analysis and recommendations*, (Bruxelles: European Commission, September 2024), p. 79.
[206] Mario Draghi, *The Future of European Competitiveness – Part A: A competitiveness strategy for Europe*, (Bruxelles: European Commission, September 2024), p.8.

Chapter 5
Conclusions

This thesis has explored the complex and conflicting relationship between blockchain technology and the GDPR's right to erasure. The legal foundations of the right to erasure, defined by Article 17 of the GDPR, have been outlined, together with an introduction to the blockchain technology features, in particular its immutability. The structural characteristic of the block's concatenation in a Distributed Ledger Technology, in fact renders most of the blockchain configurations inherently immutable, and thus incompatible with the possibility for data subjects to request the deletion of their personal data recorded on the DLT.

Blockchains, which serve a wide range of purposes, often retain various forms of personal data (such as information contained within blocks, metadata from transactions, public keys, etc.), raising challenges not only under Article 17 but also with respect to the allocation of responsibilities in data processing scenarios, international transfers, and broader compliance issues. The decentralized and disintermediated nature of blockchain, foundational to its design, introduces significant tensions with stringent data protection regulations. As a technology born as "anarchic" and "alegal", blockchain resists easy integration into established legal frameworks. This is particularly evident in public or permissionless blockchains, where regulatory alignment proves especially difficult, whereas private or permissioned configurations offer more flexibility.

Despite this, several approaches have been proposed to solve, or at least, to mitigate, the incompatibility between blockchain technology and the GDPR's right to be forgotten. These solutions can be grouped into technical solutions, to be implemented alongside governance mechanisms, and broader regulatory approaches aimed at reconciling the tension. Among the technical solutions explored are: hard-forking chains (as illustrated by the Spanish Data Protection Authority in its 2024 Proof of Concept); the use of chameleon hashes to introduce mutability into DLTs; off-chain storage of personal data with on-chain hashes serving as proof-of-existence; and the deployment of cryptographic commitments. While this list is not exhaustive, it highlights the most promising tools, which, however, are often costly, complex to implement, or unsuitable for certain blockchain applications. These methods, whose technical aspects have been discussed in a simplified manner, given the mostly legal nature of the work, nonetheless offer valuable opportunities for potential paths forward.

Among the various solutions, the off-chain storage of personal data appears to be the most effective in many cases. However, this solution can be seen as a circumvention rather than a resolution of the core issue, as it avoids the problem by storing only cryptographic hashes on-chain. Nevertheless, it remains a significant and viable option for certain DLT configurations, as illustrated in the case study on the data protection framework adopted by the GiottoChain project developed by the company Almaviva.

In fact, the data protection framework examined in GiottoChain has been found to be aligned with the off-chain storage approach outlined by the European Data Protection Board in its "Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies", published in April 2025. While this convergence is noteworthy, it is important to clarify that GiottoChain has not processed personal data, either in the past or currently. The proposed safeguards are in place and ready to be applied if needed, but so far, the notarization of digital assets has not involved data falling under the scope of the GDPR.

At a macro level, regulatory sandboxes, extensively examined in this thesis, represent a viable tool for regulators. In practice, sandboxes can serve multiple purposes, ranging from experimental incubators for innovation to platforms for the development of emerging technologies, and even as instruments for assessing or revising existing legislation in the tech sector[207]. This last aim is particularly relevant given the forward-looking nature of technological innovation, which often challenges the rigidity of current regulatory frameworks.

Through the GiottoChain case study, which participated in the first cohort of the European Blockchain Sandbox, a concrete illustration of the sandbox approach has been provided. The EU initiative offered notable advantages (and continues to offer, since it is still working for the second cohort), particularly for the enhancement of the crucial dialogue between regulators and firms, but it also presents certain shortcomings. Most notably, the European Blockchain Sandbox lacks a truly experimental mandate from a regulatory perspective, as it does not foresee any limited exemptions from applicable rules. This limits its potential to fully explore in depth the interactions between law and blockchain technologies. Nevertheless, the overall experience remains positive and promising for future configurations, especially when regulatory sandboxes are designed as practical tools for genuine exchange and openness, including on the side of regulatory authorities. The current momentum in the

[207] Appaya, Gradstein, Kanz, *Global Experiences from Regulatory Sandboxes*, p. 6.

EU, together with Article 57 of the AI Act, suggests a likely future increase in the use of regulatory sandboxes, ideally supported by a flexible and receptive environment.

Such a shift in the regulatory approach would also be beneficial for addressing the incompatibility between blockchain and Article 17 of the GDPR. At a time when the European Union appears to be revisiting the over-regulatory stance of the first von der Leyen mandate, moving instead toward a framework of simplification, reduction, and possibly revision of digital regulations[208], a more open and constructive posture from EU authorities could only be advantageous for the core issue discussed in this research work.

In this regard, it is worth underlining that, while this thesis focuses on the European Union regulatory data protection framework, very few non-EU jurisdictions offer a comparable right to erasure. In the United States, data protection laws are highly fragmented and sectoral and do not recognize a general right to deletion. The California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), provide a limited right to delete data, but with broad exemptions and significantly less enforceability than the GDPR[209]. Similarly, frameworks in countries such as Japan (Act on the Protection of Personal Information, APPI)[210] or Singapore (Personal Data Protection Act, PDPA)[211] tend to prioritize business certainty and innovation over strict individual rights. While the absence of certain data protection rights, such as the right to erasure, in non-EU jurisdictions does not, from the European Union's perspective, constitute a shortcoming, it nonetheless represents an objective reality that must be duly acknowledged and carefully balanced.

Back to the EU, although still perhaps premature or difficult to implement in practice, a progressively more pragmatic interpretation of the GDPR, based on a risk-based approach, could help to resolve or at least support compliance in complex scenarios such as the blockchain–right to erasure conflict. This ultimately raises the question of whether it is possible to interpret the GDPR in light of technological specificities, despite its principle of technology neutrality (Recital 15 GDPR), by adopting more practical principles. For instance, it may be worth reflecting on the differing purposes and expectations

[208] O'Regan, "Europe's GDPR privacy law is headed for red tape bonfire within 'weeks'"
[209] Glenn A. Brown, "Consumers' "Right to Delete" under US State Privacy Laws", *Privacy World*, on Squire Patton Bogs, March 3, 2021, https://www.privacyworld.blog/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/.
[210] Tomoki Ishiara, "Japan", in *The Privacy, Data Protection and Cybersecurity Law Review – Fifth Edition*, edited by Alan Charles Raul, (Law Business Research, 2018), p. 222.
[211] Yuet Ming Tham, "Singapore", in *The Privacy, Data Protection and Cybersecurity Law Review – Fifth Edition*, edited by Alan Charles Raul, (Law Business Research, 2018), p. 288.

surrounding data deletion in bilateral relationships with respect to disintermediated environments such as the DLT ones, where data governance often follows a collective logic[212].

It should be noted that, in this context, a push, not in terms of interpretative flexibility, but rather in terms of encouraging the adoption of innovative technical components, has emerged in recent months from the EDPB's Guidelines on blockchain and the GDPR. Despite adopting a highly cautious stance and at times even discouraging the use of blockchain as a repository for personal data, the EDPB nonetheless recommends several innovative and promising techniques. Among these are the already mentioned zero-knowledge proofs and cryptographic commitments, as well as off-chain data storage combined with the deletion of cryptographic keys linked to on-chain hashes. This openness toward potential technical solutions to solve the legal-technical incompatibilities is a solid perspective for future progress in this area.

In conclusion, it is important to acknowledge the significant incompatibilities between blockchain technologies and data protection, particularly regarding the right to erasure enshrined in Article 17 of the European Union's GDPR. These incompatibilities are especially pronounced and virtually incontrovertible in public or permissionless configurations of DLTs. However, some methods exist that can act as mitigators or corrective measures to address these conflicts. Such methods may be technical, implemented within the infrastructure by developers and recommended by the authorities, or legal and regulatory, involving interpretative flexibility, possible exemptions, or simply a pragmatic and adaptable approach by the relevant authorities. While the issue remains complex and difficult to resolve, what should be encouraged, alongside further technical research, is a progressively more open, propulsive, and flexible balanced stance from European authorities towards emerging technologies and innovation, recognizing the numerous benefits that a thriving digital innovative market can bring to the European economy.

[212] D'Acquisto, "Blockchain e GDPR: verso un approccio basato sul rischio", pp. 63-64.

Bibliography

Agencia Española de Protección de Datos (AEPD) and European Data Protection Supervisor (EDPS). *Hash Functions as Personal Data Pseudonymisation Techniques*. Adopted November 4, 2019. https://www.edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en.

Agencia Española de Protección de Datos (AEPD). *Prueba de concepto: Blockchain y el derecho de supresión*. Adopted November 13, 2024. https://www.aepd.es/guias/nota-tecnica-blockchain.pdf.

Agencia Española de Protección de Datos. "Derecho al olvido y Blockchain: Prueba de concepto". November 13, 2024. Video, 16 min., 17 sec. https://www.youtube.com/watch?v=H7gnoI3B7SY.

Agenzia per l'Italia Digitale (AgID). "Oggi il Processo di Qualificazione Cloud per la PA Passa ad ACN". Last modified January 19, 2023. https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/01/19/oggi-il-processo-qualificazione-cloud-pa-passa-ad-acn.

Almaviva. *GiottoOnChain General Terms and Conditions (SaaS)*. Last modified May 11, 2023. https://d7umqicpi7263.cloudfront.net/eula/CsFKnDO4qK-k308FW0dBHJJz8wOv3DDc0AzgvzYoYn4.

Almaviva. "Notarizzazione Blockchain". Accessed April 2025. https://notarizzazione.almaviva.it/.

Appaya, Mandepanda Sharmista, Helen Luskin Gradstein, and Mahjabeen Haji Kanz. *Global Experiences from Regulatory Sandboxes*. World Bank Group, Fintech Note No. 8, (Washington DC, 2020). https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912001605241080935/global-experiences-from-regulatory-sandboxes.

Article 29 Data Protection Working Party. *Opinion 5/2014 on Anonymisation Techniques*. Adopted April 10, 2014.

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Article 29 Data Protection Working Party. *Opinion 05/2012 on Cloud Computing*. Adopted July 1, 2012. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Ateniese, Giuseppe, Bernardo Magri, Daniele Venturi, and Ewerton Andrade. "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends". *IEEE EuroS&P*, (April 2017): 111-126. https://doi.org/10.1109/EuroSP.2017.37.

Attrey, Angela, Molly Lesher, and Christopher Lomax. *The role of sandboxes in promoting flexibility and innovation in the digital age*. OECD Going Digital Toolkit Notes, No. 2, OECD Publishing, (Paris, 2020). https://www.oecd.org/en/publications/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age_cdf5ed45-en.html.

Bayle, Aurelie, Mirko Koscina, and David Manset. "When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry". *IEEE/WIC/ACM International Conference on Web Intelligence (Wil)*, (December 2018): 788-792. https://doi.org/10.1109/WI.2018.00133.

Belen-Saglam, Rahime, Enes Altuncu, Yang Lu, and Shujun Li. "A systematic literature review of the tension between the GDPR and public blockchain systems". *Blockchain: Research and Applications* 4, (June 2023): 1-23. https://doi.org/10.1016/j.bcra.2023.100129.

Bloch-Wehba, Hannah. "Confronting Totalitarianism at Home: The Roots of European Privacy Protections". *Brooklyn Journal of International Law*, Vol. 40 (2015): 748-790. https://brooklynworks.brooklaw.edu/bjil/vol40/iss3/1.

Brown, Glenn A. “Consumers’ “Right to Delete” under US State Privacy Laws”. *Privacy World*, on Squire Patton Bogs, March 3, 2021. https://www.privacyworld.blog/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/.

Brozzetti, Filiberto Emanuele. “EU Digital Sovereignty: How Long Will the “Brussels Effect” Last?”. *Rivista Internazionale Di Filosofia del Diritto*, 2 (2024): 343-378. https://iris.luiss.it/handle/11385/246379.

Buchanan, Bill. “Chameleon Hashes”. *Medium*, December 22, 2022. https://medium.com/asecuritysite-when-bob-met-alice/chameleon-hashes-c9e969a91ccb.

Center for Competition Policy. “Portal On Regulatory Sandboxes”. Accessed May 2025. https://competitionpolicy.ac.uk/research-projects/portal-on-regulatory-sandboxes/.

Chang, Henry. “Blockchain: Disrupting Data Protection?”. *Privacy Law & Business International Report*, University of Hong Kong Faculty of Law Research Paper No. 2017/041, (November 2017). https://ssrn.com/abstract=3093166.

Christidis, Konstantinos, and Michael Devetsikiotis. “Blockchains and Smart Contracts for the Internet of Things”. *IEEE Access* 4 (2016): 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339.

Commission Nationale de l'Informatique et des Libertés (CNIL). *Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*. Adopted September 2018. https://www.cnil.fr/sites/cnil/files/atoms/files/blockchain_en.pdf.

Court of Justice of the European Union (CJEU). *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317, judgment of 13 May 2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131.

D’Acquisto, Giuseppe. “Blockchain e GDPR: verso un approccio basato sul rischio”. *Federalismi.it*, n. 2, (2021): 52-65. https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=44784&content=&content_author=.

Datenschutzbehörde (DSB). *Decision DSB-D123.270/0009-DSB/2018*. Adopted December 5, 2018. https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html

De Filippi, Primavera, Morshed Mannan, and Wessel Reijers. "The alegality of blockchain technology". *Policy and Society*, 41(3), (2022): 358-372. https://doi.org/10.1093/polsoc/puac006.

Draghi, Mario. *The Future of European Competitiveness – Part A: A competitiveness strategy for Europe*. European Commission, (Bruxelles, September 2024). https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

Draghi, Mario. *The Future of European Competitiveness – Part B: In-depth analysis and recommendations*. European Commission, (Bruxelles, September 2024). https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

Efthymiou, Venizols, Nikos Hartziargyrou, Mark McGranaghan, Marco-Robert Schulz, Jochen Kreusel, Ricardo Almeida Henriques, Andrei Morch, Dagmar Jarásová, Rad Stanev, Aris Dimeas, Athanase Vafeas, Michele de Nigris, Iva Maria Gianinoni, Rainer Bacher, Mahboubeh Hortamani, and Shafi Khadem. "Regulatory Sandboxes - Policy Report drafted by WG5's Regulatory Sandboxes Task Force". *ETIP SNET*, Publications Office of the European Union, (2023). https://op.europa.eu/en/publication-detail/-/publication/d74556a2-4ba0-11ee-9220-01aa75ed71a1/language-en.

European Commission. *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part A*. December 2023. https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Key+documents.

European Commission. *European Blockchain Sandbox - Best Practices Report, 1st Cohort, Part A, Abstract and Executive Summary*. December 2023. https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Key+documents.

European Commission. *European Blockchain Sandbox - Best Practices Report - 1st Cohort, Part B, Abstract and Executive Summary*. June 2024.

https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Best+practices+report+2023+-+Part+B.

European Commission. *European Blockchain Sandbox - Best Practices Report - 1st Cohort, Part B*. June 2024. https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Best+practices+report+2023+-+Part+B

European Commission. "European Blockchain Sandbox". Accessed March 2025. https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en.

European Commission. "Frequently Asked Questions (FAQ)". European Blockchain Services Infrastructure. Accessed May 2025. https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Frequently+Asked+Questions

European Commission. "Types of EU Law". Accessed February 2025. https://commission.europa.eu/law/law-making-process/types-eu-law_en.

European Data Protection Board. *Guidelines 02/2025 on the Processing of Personal Data through Blockchain Technologies*. Version 1.1, April 8, 2025. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en.

European Data Protection Supervisor. "The History of the General Data Protection Regulation". Accessed February 2025. https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

European Union Council. *Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as Tools for an Innovation-Friendly, Future-Proof and Resilient Regulatory Framework that Masters Disruptive Challenges in the Digital Age*. Adopted December 23, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2020_447_R_0001.

European Union. *Charter of Fundamental Rights of the European Union*. Official Journal of the European Communities, C 364/1, December 18, 2000.

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, L 119, 4 May 2016.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations.* Official Journal of the European Union, L 260, 1 October 2024.
https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

Ethereum.org. "The history of Ethereum". Last modified February 2025.
https://ethereum.org/en/history/#paris

Ethereum.org. "Proof-of-Stake vs Proof-of-Work". Last modified January 2024.
https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/pos-vs-pow/.

Ferracane, Martina F. "The Costs of Data Protectionism". In *Big Data and Global Trade Law*, edited by Mira Burri. Cambridge University Press, 2021.
https://doi.org/10.1017/9781108919234.005.

Finck, Michèle. "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?". In *Panel for the Future of Science and Technology (STOA)*, European Parliamentary Research Service (EPRS), (July 2019).
https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445.

Germani, Patrizio, Michelangelo Amoruso Manzari, Riccardo Magni, Paolo Dibitonto, Fabio Previtali, and Emanuele D'Agostini. "Building Trustworthy AI Systems: AI Inference Verification with Blockchain and Zero-Knowledge Proofs". *6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, (2024): 1-3.
https://doi.org/10.1109/BRAINS63024.2024.10732140.

Giessen, David van de. “Blockchain and the GDPR’s Right to Erasure”. Bachelor's essay, University of Twente, 2019.
https://essay.utwente.nl/78738/.

Haga, Shinya, and Kazumasa Omote. “Blockchain-Based Autnomous Notarization System Using National eID Card”. *EE Access*, vol. 10, (2022): 87477-87489.
https://doi.org/10.1109/ACCESS.2022.3199744.

Humbeeck, Andries van. “The Blockchain-GDPR Paradox”. *Journal of Data Protection & Privacy*, 2(3), (2019): 208-212.
https://doi.org/10.69554/EYOF8218.

Knirsch, Fabian, Andreas Unterweger, and Dominik Engel. “Implementing a Blockchain from Scratch: Why, How, and What We Learned”. *EURASIP Journal on Information Security* 2019, no. 2, (March 2019): 1-14.
https://doi.org/10.1186/s13635-019-0085-3.

Krawczyk, Hugo and Tal Rabin. “Chameleon Hashing and Signatures”. *Theory Of Cryptography*, (October 1997).

Ishiara, Tomoki. “Japan”. In *The Privacy, Data Protection and Cybersecurity Law Review – Fifth Edition*, edited by Alan Charles Raul. Law Business Research, 2018.

Lamport, Leslie, Robert Shostak, and Marshall Pease. “The Byzantine Generals Problem”. *ACM Transactions on Programming Languages and Systems* 4, no. 3 (1982): 382–401. https://lamport.azurewebsites.net/pubs/byz.pdf.

Li, Xin-Yu, Jing Xu, Ling-Yuan Yin, Yuan Lu, Qiang Tang and Zhen-Feng Zhang, “Escaping from Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting”. *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 5 (2023): 3699-3715.
https://doi.org/10.1109/TDSC.2022.3212601.

Lietuvos Bankas. “LBChain”. Accessed May 2025.
https://www.lb.lt/en/lbchain.

Lindahl, Hans. *Fault Lines of Globalization: Legal Order and the Politics of A-Legality*. Oxford University Press, 2013.

von der Leyen, Ursula. *Political Guidelines for the Next European Commission 2019-2024*. Brussels: European Commission, 2019. https://op.europa.eu/en/publication-detail/-/publication/62e534f4-62c1-11ea-b735-01aa75ed71a1.

Lynskey, Orla. "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja González". *Modern Law Review* 78, no. 3 (2015): 522-534. https://www.jstor.org/stable/43829127.

Lyons, Tom, Ludovic Courcelas, and Ken Timsit. "Blockchain and the GDPR". By *The European Union Blockchain Observatory And Forum*, (October 2018). https://blockchain-observatory.ec.europa.eu/document/download/b3a919ed-0045-46f8-89de-f23ca140e037_en?filename=20181016_report_gdpr.pdf&prefLang=fr.

Markellos, Raphael, Sean Ennis, Bryn Enstone, Anastasios Manos, Dimitrios Pazaitis, and Dimitrios Psychoyios. "Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies". *SSRN Electronic Journal*, (March 2024). https://dx.doi.org/10.2139/ssrn.4764911.

Markey-Towler, Brendan. "Anarchy, Blockchain and Utopia: A theory of political-socioeconomic systems organised using Blockchain". *The JBBA* Vol. 1, Issue 1, (March 2018): 13-21. https://doi.org/10.31585/jbba-1-1-(1)2018.

Media2000. "AI Act, Filiberto Brozzetti (Luiss): Qual è l'obiettivo strategico che l'UE si propone?". Last modified March 14, 2024. https://www.media2000.it/ai-act-filiberto-brozzetti-luiss-qual-e-lobiettivo-strategico-che-lue-si-propone/.

Mirchandani, Anisa. "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR". *Fordham Intellectual Property, Media, and Entertainment Law Journal*, Vol. 29, XXIX, no. 4, (2019): 1201-1241. https://ir.lawnet.fordham.edu/iplj/vol29/iss4/5.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System”. October 31, 2008. https://bitcoin.org/bitcoin.pdf.

OECD. *Fostering Cross-Border Data Flows with Trust*. Paris: OECD Publishing, OECD Digital Economy Papers, 2022. https://www.oecd.org/en/publications/fostering-cross-border-data-flows-with-trust_139b32ad-en.html.

OECD. *Going Digital to Advance Data Governance for Growth and Well-being*. Paris: OECD Publishing, 2022. https://www.oecd.org/en/publications/going-digital-to-advance-data-governance-for-growth-and-well-being_e3d783b0-en.html.

O’Regan, Ellen. “Europe’s GDPR privacy law is headed for red tape bonfire within ‘weeks’”. *Politico*, April 3, 2025. https://www.politico.eu/article/eu-gdpr-privacy-law-europe-president-ursula-von-der-leyen/.

Oxford Learner’s Dictionaries, s.v. “erasure”. Accessed February 2025. https://www.oxfordlearnersdictionaries.com/definition/english/erasure

Palmisano Tonino, Vito Nicola Convertini, Lucia Sarcinella, Luigia Gabriele, and Mariangela Bonifazi. “Notarization and Anti-Plagiarism: A New Blockchain Approach”. *Applied Sciences* 12, no. 1: 243, (2022). https://doi.org/10.3390/app12010243.

Pagallo, Ugo, Eleonora Bassi, Marco Crepaldi, Massimo Durante. “Chronicle of a Clash Foretold: Blockchains and the GDPR’s Right to Erasure”. In *Legal Knowledge and Information Systems*, IOS Press, (November 2019). https://www.researchgate.net/publication/337648771_Chronicle_of_a_Clash_Foretold_Blockchains_and_the_GDPR's_Right_to_Erasure.

Popovski, Lewis and George Soussou. “A Brief History of Blockchain”. *Legal Tech News*, May 14, 2018. https://www.pbwt.com/publications/a-brief-history-of-blockchain.

Powles, Julia. “What Did the Media Miss with the Right to Be Forgotten Coverage?”. *The Guardian*, May 21, 2014. https://www.theguardian.com/technology/2014/may/21/what-did-the-media-miss-with-the-right-to-be-forgotten-coverage

Ram, Simona. “How Centralized Is the Bitcoin (BTC) Mining Sector?”. *DailyCoin*, February 7, 2023. https://dailycoin.com/bitcoin-mining-pool-sector-how-centralized-is-it/.

Ranchordás, Sofia. “Experimental Lawmaking in the EU: Regulatory Sandboxes”. *University of Groningen Faculty of Law Research Paper Series*, No. 12, (2021). https://dx.doi.org/10.2139/ssrn.3963810.

Ranchordás, Sofia, and Roberta Meoli. “Regulatory Sandboxes for Sustainable Finance”. *SSRN Electronic Journal*, (December 2024). https://dx.doi.org/10.2139/ssrn.5231506.

Riley, Jenn. *Understanding Metadata*. For National Information Standards Organization (NISO), (Baltimore, MD: NISO Press, 2017). https://www.niso.org/publications/understanding-metadata-2017.

Savelyev, Alexander. “Contract Law 2.0: «Smart» Contracts As The Beginning Of The End Of Classic Contract Law”. *Information & Communications Technology Law*, 26(2), (2016): 116–134. https://doi.org/10.1080/13600834.2017.1301036.

Schneider, Henrique. “Europe’s Innovation Problem: Trying to Regulate the Future”. *GIS Reports*, December 2, 2024. https://www.gisreportsonline.com/r/innovation-regulation/.

Schwartz, Leo. “Two small countries bet on Bitcoin—and it’s paying off big time”. *Fortune Crypto*, November 15, 2024. https://fortune.com/crypto/2024/11/15/el-salvador-bitcoin-holdings-500-million-bhutan-bukele/.

Sestino, Andrea, Adham Kahlawi, and Andrea De Mauro. “Decoding the Data Economy: A Literature Review of Its Impact on Business, Society and Digital Transformation”. *European Journal of Innovation Management* 28, no. 2, (2025): 298-323.

https://doi.org/10.1108/EJIM-01-2023-0078.

Singh, Daljit. “Exploring Blockchain with Zero Knowledge Proof Uses”. *Debut Infotech*, January 6, 2025. https://www.debutinfotech.com/blog/zero-knowledge-proof-uses.

Smith, Andrew. “Roll Up for Digital Whack-a-Mole: Europe Can’t Enforce the Right to Be Forgotten”. *The Conversation*, May 20, 2014. https://theconversation.com/roll-up-for-digital-whack-a-mole-europe-cant-enforce-the-right-to-be-forgotten-26726.

Sobti, Rajeev, and Geetha Ganesan. “Cryptographic Hash Functions: A Review”. *IJCSI International Journal of Computer Science Issues* 9, no. 2 (2012): 461-479. https://www.researchgate.net/publication/267422045_Cryptographic_Hash_Functions_A_Review.

Statista. “Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025”. Accessed February 2025. https://www.statista.com/statistics/871513/worldwide-data-created/#statisticContainer.

Texeira, Lawrence. “The New Black Gold: How Data Became the Most Valuable Asset in Tech”. *Medium*, February 12, 2024. https://medium.com/@lawrenceteixeira/the-new-black-gold-how-data-became-the-most-valuable-asset-in-tech-9e4541262ddf.

Tham, Yuet Ming. “Singapore”. In *The Privacy, Data Protection and Cybersecurity Law Review – Fifth Edition*, edited by Alan Charles Raul. Law Business Research, 2018.

World Bank Group. “Key Data from Regulatory Sandboxes across the Globe”. Last modified November 1, 2020. https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe.

Yaffe-Bellany, David. “At Crypto Summit, Trump Says U.S. Will Be ‘the Bitcoin Superpower’”. *The New York Times*, March 7, 2025. https://www.nytimes.com/2025/03/07/technology/trump-crypto-summit.html.

Zein, Dave, Wiktor Pinkwart, Catarina Silva, Geoffrey Goodell, Harris Niavis, Jonathan Heiss, Jörn Erbguth, Sharmin Chougule, Sophoclis Stephanou, and Stéphanie Attias. “Leveraging Zero-Knowledge Proofs for GDPR Compliance in Blockchain Projects”. *INATBA Position*, (October 2024). https://inatba.org/policy/inatba-publishes-position-paper-on-leveraging-zkps-for-gdpr-compliance/.

Zetzsche, Dirk, Ross P. Buckley, Douglas W. Arner, and Janos Nathan Barberis. “Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation”. *European Banking Institute Working Paper Series*, no. 11, (2017). https://dx.doi.org/10.2139/ssrn.3018534.

Zhang, Peng, Douglas C. Schmidt, Jules White, and Abhishek Dubey. “Consensus mechanisms and information security technologies”. In *Role of Blockchain Technology in IoT Applications*, ed. Shiho Kim, Ganesh Chandra Deka, Peng Zhang. Academic Press, (2019). https://learning.oreilly.com/library/view/role-of-blockchain/9780128171929/S0065245819300245.xhtml#s0050.