UNIVERSITÀ
DEGLI STUDI
FIRENZE

RESEARCH DOCTORATE

XXXV CYCLE

Coordinator Prof. Dr Alessandro Simoni

Building a Techno-legal Framework for Blockchain Technology and Data Protection under EU Law

Curriculum in European and Transnational Legal Studies

Academic Discipline IUS/14

SUPERVISOR	CANDIDATE
Prof. Dr Adelina Adinolfi	Enza Cirone

*A mio **Nonno**,*
fonte di ispirazione e incoraggiamento
a perseguire traguardi sempre più ambiziosi.

*Alla mia **Famiglia**,*
sostegno insostituibile e rifugio sicuro
dalle tempeste della vita.

Table of Contents

Chapter III

Intertwining Blockchain Technology and Data Protection Law: Enemies for Life?138

Chapter IV

Conclusions

Essential Glossary of Terms

Accountability principle: A principle of data protection that requires data controllers to be able to prove their compliance with the law (article 5, para. 2 of the GDPR).

Anonymization: The permanent and irrevocable elimination of personal identifiers, rendering the information incapable of identifying an individual. Anonymized information falls outside the scope of data protection regulations.

Block: The data structure used in Blockchains to group transactions. In addition to transactions, blocks include other elements, such as the previous block's hash and a timestamp.

Consensus Algorithms: They play a crucial role in achieving a unified and unalterable version of the ledger within a Blockchain. They facilitate agreement among network participants regarding the recorded content, even in the presence of potentially faulty or malicious actors. The specific means employed to achieve consensus may vary depending on the requirements of the Blockchain. Some well-known consensus algorithms include Proof-of-Work, Proof-of-Stake, and Proof-of-Authority.

Consent: It refers to an expression of the individual's preferences that is freely given, specific, well-informed, and clearly affirmative. It indicates the person's agreement to process their personal data through a statement or a distinct affirmative action.

Data controller: 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.

Data Protection Principles: The foundational compliance obligations of data protection law, which the controller is responsible for. The principles are lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

Data Subject: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Distributed Ledger: Refers to a database that is shared and synchronized across various locations, organizations, or regions allowing multiple individuals to access it.

Transactions conducted on this ledger are observed by the public. Each node within the network can access the shared records and maintain an identical copy of these records. Any modifications or additions to the ledger are rapidly disseminated to all participants, typically within seconds or minutes.

European Data Protection Board (EDPB): The successor body to the Article 29 Working Party is a body of the European Union with a legal personality which ensures the consistent application of the EU GDPR (article 68 et seq of the GDPR).

Hash: The result of a function that transforms data into a unique, fixed-length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint for any type of data.

Node: A computer running specific software which allows the processing and communication of pieces of information to other nodes; in Blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network.

Permissioned Blockchain: Blockchain that is private and has controlled access via a private network.

Permissionless Blockchain: Blockchain that is open and publicly accessible.

Personal Data: Any information relating to an identified or identifiable natural person ('data subject').

Privacy-enhancing Technology: A set of tools, techniques, or technologies designed to protect and preserve individuals' privacy in the context of data processing and information sharing. These technologies aim to enable secure data handling while minimizing the risk of unauthorized access or disclosing sensitive personal information. Privacy-enhancing technologies are employed to support compliance with privacy regulations, ensure data confidentiality, and grant individuals more control over their personal data in various digital environments.

Private key: It consists of a sequence of random alphanumeric characters associated with a public key. These private keys are exclusively known to the participant. It is possible to liken private keys to passwords used for email addresses; they grant access but cannot be deduced solely by having the email address.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (article 4, para. 1, nr.2 of the GDPR).

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (article 4, para 1, nr. 8 of the GDPR).

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (article 4, para 1, nr. 5).

Public Key: In public key cryptography, commonly employed in various cryptocurrencies, a public key consists of a sequence of random alphanumeric characters associated with a private key. Public keys are accessible to anyone within the system and are employed for data encryption. It is possible to draw a parallel between public keys and email addresses, necessitating a corresponding password (private key) to obtain access**.**

Signature: The process of signing a message or transaction involves encrypting data using a pair of asymmetric keys. Asymmetric cryptography enables the use of one key for encryption and the other key for decryption interchangeably. The private key is used to encrypt the data, while the public key can be used by third parties to decrypt the data and verify that the holder of the corresponding private key indeed sent the message.

Smart contract: Pieces of code stored on the Blockchain that will self-execute once deployed. By leveraging the trust and security of the Blockchain network, they enable users to automate business logic, leading to the improvement or complete transformation of business processes and services.

Tokens: A variety of digital assets that are traceable and exchangeable on a Blockchain. They are frequently used to digitally represent various assets such as commodities, stocks, and even tangible products. Tokens also serve as a means to encourage participants in the upkeep and protection of Blockchain networks.

Transaction: The most granular piece of information that can be shared among a Blockchain network. They are generated by users and include information such as the value of the transfer, the address of the receiver and data payload. Prior to broadcasting a transaction to the network, a user digitally signs its contents using a private cryptographic key. Through the verification of these signatures, network nodes are able to identify the sender of a transaction and guarantee that its content remains unaltered during transmission across the network.

Transactional Data: Information regarding the transfer's value, receiver's address, and data payload.

Validator Node: Designated nodes within a network which are assigned to create blocks and disseminate them across the network. To produce a valid new block, these nodes must adhere strictly to the predefined rules outlined by the consensus algorithm.

Introduction

> *"Why should it be that just when technology is most encouraging of creativity, the law should be most restrictive?"*
>
> Lawrence Lessig[1]

1. Background and Context: Law and Technology – **2.** Blockchain as a regulatory conundrum – **2.1.** Blockchain: A Foundational Technology— **3**. The European Data Protection Framework – **4.** The Interplay between the GDPR and Blockchain **– 5.** Defining the Research Questions and Objectives **– 5.1.** What this thesis is not about – **6.** Research Methodology – **7.** Outline

1. Background and Context: Law and Technology

The rapid pace of innovation and technological advancement in recent decades has resulted in significant transformations in various aspects of society. These advancements have also raised important questions about the adequacy and effectiveness of existing legal frameworks in addressing emerging issues and harmonizing different legal approaches across different jurisdictions.

Legal systems create and enforce standards, regulations, and protocols that govern various technological activities, encompassing ethical considerations, liability, accountability, and safeguarding individual rights. Furthermore, technological innovation frequently serves as a catalyst for legal transformation, compelling the adaptation and evolution of legal frameworks to tackle emerging challenges effectively.[2] Law has indeed perpetually been challenged by the emergence of new

[1] L. Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy*, Bloomsbury Publishing, 2008.

[2] According to De Filippi and Hassan, it is possible to identify four distinct phases representing the evolving relationship between law and technology: digitizing information; automation of the decision-making processes; incorporation of legal rules into code; code-ification of law. See P. De Filippi, S. Hassan, *Blockchain technology as a regulatory technology: From code is law to law is code*, in *First Monday,* volume 21, number 12, 5 December 2016, p. 2.

technologies, and legal systems have been surely affected by technological changes arguably without being undermined.[3]

Against this background, the interplay between technology and law presents complex and multifaceted challenges that require careful examination and understanding. While technology can spur legal change, the law also plays a crucial role in regulating and governing technology. Regulation is indeed often posed as the antithesis of innovation, and nowadays, Blockchain, which is considered one of the most disruptive technologies[4] of all time, is often connected to the concept of freedom: it can "free society from the tyranny of the data overloads".[5]

Distribution and decentralization are core characteristics of the Blockchain,[6] which is a ledger consisting of blocks that hold transaction records or history with no central entity that controls the overall processing of the system.

Each period of technological evolution advocates new paradigms of value, and the history of Blockchain seems not to be exempt from this. It is said to considerably reinvent current socio-economic systems[7] and "create challenges for states and regulators seeking to control, shape, or influence the development of Blockchain technology".[8] Some argue that "if governments struggle to enforce law against autonomous Blockchain-based systems, they could explore relying on Blockchain technology itself to set up a new framework of code-based regulation to regulate people, companies, and machines".[9]

[3] A. Manolopoulos, *Raising Cyberborders: The Interaction Between Law and Technology*, in *International Journal of Law and Technology*, 2003, p. 55; M. Fenwick, W.A. Kaal, E.P.M. Vermeulen, *Regulation tomorrow: what happens when technology is faster than the law?*, in *American University Law Review*, 2017, pp. 561-594.

[4] C.M. Christensen et al, *Disruptive Innovation: An Intellectual History and directions for further research,* in *Journal of Management Studies,* 2018, p. 1043; C.M. Christensen, *Disruptive Class: How disruptive innovation will change the way the world learns,* McGraw-Hill, 2008.

[5] M. Aaron, *CRYPTO 101: Data as the newest financial instrument w/Constellation Network*.

[6] A. Imteaj, M. H. Amini, P.M. Pardalos, *Foundation of Blockchain – Theory and Applications*, Springer, 2021, p. 3.

[7] M. Xu, X. Chen, G. Kou, *A systematic review of Blockchain*, in *Financial Innovation*, 2019, pp. 1-14.

[8] P. De Filippi, A. Wright, *Blockchain and the Law*, Harvard University Press, 2018, p. 5.

[9]M. Iansiti, K. Lakhani, *The truth about Blockchain,* in *Harvard Business Review,* 2017, https://hbr.org/2017/01/the-truth-about-Blockchain, p. 194.

In light of the above and considering the structural framework of this thesis, it seems essential to retrace the concepts that often surround the discussion regarding the possibility of regulating technology, namely Lex Informatica coined by Joel Reidenberg, 'code is law' contended by Lawrence Lessig, and the concept of Lex Cryptographia[10] by Primavera de Filippi and Aaron Wright.

These theories share the idea of a novel form of law that relies on code. In this context, code emerges as one of several regulatory factors that exert normative influence on individual behaviour. It assumes the character of law, albeit as only one of many sources of law without overriding the others.

In this respect, it is also worth covering some of the antithetical public narratives[11] that have so far engaged with Blockchain since the opposite views within the Blockchain literature may show how the freedom/restraint set influences the public discourse on Blockchain and how it characterizes the so-called "Blockchain conundrum".

2. Blockchain as a Regulatory Conundrum

The increasing interest in Blockchain has emphatically drawn attention to the normative context in which this technology operates.

[10] "characterized by a set of rules administrated through self-executing smart contracts and decentralized (and potentially autonomous) organizations.", A. Wright, P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia,* 10 March 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

[11] In particular, the association of Blockchain with financial freedom characterized the claims within the 'hype literature', which tended to the messianic and euphoric. This narrative sees in Blockchain's distribution, security, and truth features the possibility of "absolute privacy and freedom from any government intervention through cryptographically reclaimed privacy or through a dismantling of government interference". Conversely, the 'critical literature' sees Blockchain as the constraint threatening freedom, or better, as a "further set of chains binding the data serfs of the present, both ideologically and materially, to the emergent satanic techno-mills of digital capitalism." See L. Robb, F. Deane, K. Tranter, *The Blockchain conundrum: humans, community regulation and chains,* in *Law, Innovation and Technology,* 2021, pp. 4-8.

As mentioned above, some authors argued that the deployment and adoption of Blockchains "require a shift in the way we perceive the role of law", thus emphasizing the potential effects they could have on contemporary legal systems.

The Blockchain relights the cyber-libertarian flame.[12] Hence, to frame a discussion about Blockchain and law, this thesis first questions whether the technology *can* be subject to legal and administrative oversight and then whether it *should* be.

By accenting Satoshi Nakamoto's proposal,[13] which is creating a solution to the problem of *government control*, proponents of distributed ledger technologies claim that regulation and Blockchain are antithetical.

Some indeed affirm that Blockchain, due to its decentralized structure, is ontologically immune to state interference; others even assert that not being (nor being able to be) regulated is one of the main features of this technology.[14]

In this regard, it may be worth questioning and assessing whether the development of distributed ledger technologies[15] – Blockchain in particular - has given renewed substance to the allegation that there are noteworthy analogies between the regulation adversity of some Blockchain community members[16] and the initial

[12] This theory "refers to a discourse that claims that the Internet and related digital media technology can and should constitute spaces of individual liberty.", see L. Dahlberg, *Cyberlibertarianism,* in *Oxford Research Encyclopedia of Communication*, 2017. This topic will be further investigated in Chapter II, section 2 of this thesis.

[13] Satoshi Nakamoto is the pseudonym behind the white paper of Bitcoin. For further details see Chapter I, para 3.

[14] M. Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713. It can be also resumed by the following remark: "Bitcoin anarchy is a feature, not a bug. Sometimes it's good to have no human governance" published by Elaine Ou in Bloomerg, https://www.bloomberg.com/opinion/articles/2018-03-14/bitcoin-Blockchain-demonstrates-the-value-of-anarchy.

[15]"A distributed ledger is a consensus of replicated, shared and synchronised digital data geographically spread across multiples sites, countries or institutions without any central administrator or centralised data storage", N. Chowdhuri, *Inside Blockchain, Bitcoin, and cryptocurrencies,* CRC Press, 2020, p. 9.

[16] "The Internet did represent something big and new. But the legal system was able to incorporate it, as it has incorporated every technology since at least the printing press. It turns out that while cyberspace is nowhere, the people and companies and systems that deliver Internet services are very much somewhere. There are any number of control points, from the Internet service and hosting providers that manage the flow of bits to the financial services firms that control the flow of money, which regulators can target to control online activity. The Internet is a regulated space, which is not to

interpretation of Internet regulation.[17] Proponents of this analogy use it to claim that the experience of the evolution of Internet regulation demonstrated how the vision of unregulated digital spaces failed since the Internet is not fully decentralized "but, rather, has points of control (the regulatory access points) that can be coerced to comply with law."[18]

Besides the technical aspect, it seems quite difficult to disintermediate governments and private institutions,[19] and the stakes are high enough to expect governments not to let up on the issue of Blockchain regulation.[20]

In the history of technological innovation, law and technology have seen complicated and interconnected phases involving the "incorporation of legal rules into code on the one hand, and the emergence of regulation by code on the other."[21] Governments first tried to exercise their sovereignty over the Internet by regulating code to (indirectly) regulate users. Yet, later, code started being employed in various sectors to regulate behaviours jointly with or in addition to existing laws.

The mentioned situation led to the emergence of new forms of regulation relying on code. The so-called codification of law, "which entails an increasing reliance on code not only to enforce legal rules, but also to draft and elaborate these rules",[22] has started with the introduction of *smart contracts* and is now evolving into something different.

say, of course, that it is regulated the same way everywhere, or that online transactions are regulated identically to their offline analogues. Working through the practicalities of Internet regulation has been a twenty-year global process, with no end in sight. Yet a key point is incontestable: Internet regulation is not an oxymoron.", K. Werbach, *Trust, but verify,* in *Barkeley Technology Law Journal,* 2018, p. 21.

[17] See D.R. Johnson, D.G. Post, *Law and Borders: The rise of Law in Cyberspace,* in *Stanford Law Review*, 1996, p. 1367; J. Goldsmith, T. Wu, *Who controls the Internet? Illusions of a borderless world,* Oxford University Press, 2006.

[18] M. Finck, *Blockchain, Regulation and Governance in Europe,* Cambridge University Press, 2018, p. 38.

[19] K. Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, in *Florida Law Review*, 2017, p. 887.

[20] J. Goldsmith et al (2006), cit.

[21] P. De Filippi, S. Hassan, *Blockchain technology as a regulatory technology: From code is law to law is code,* in *First Monday*, volume 21, number 12, 5 December 2016, p. 2.

[22] *Ibidem.*

More recently, a phenomenon[23] has been put under the spotlight: the diffusion of Non-Fungible Tokens (NFTs),[24] a cryptographic asset on a Blockchain containing unique identifying information and code, which “represent an evolution of the physical ownership of a specific asset”.[25] “NFTs can be used to create verifiable digital ownership, authenticity, traceability and security, easily exploitable in different sectors and activities. These include crypto art, digital collectables, online games, patents or other intellectual property rights, real estate, precious objects, vehicles, licenses and financial documents.”[26]

Although NFTs will not be deepened in this research, they represent a further and emblematic example of what “paradigm shift” means when referring to Blockchain and all its derivates.[27]

This introductory overview highlights a decisive question: should traditional legal systems be adapted to the new reality resulting from Blockchain? Or should an *ad hoc* legal system be created?

2.1. Blockchain: A Foundational Technology

Blockchain has not merely the potential to innovate but also to redefine our economic and social systems. As the adoption of Blockchain technology progresses

[23] Cfr. C. Pinto-Gutiérrez et al, *The NFT Hype: What draws attention to Non-fungible tokens?*, in *Mathematics*, 2022, pp. 1-13.

[24] For an in-depth legal analysis of the underpinning of NFTs, see J. Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, in *Indiana Law Journal*, 2022, Available at: https://www.repository.law.indiana.edu/ilj/vol97/iss4/4; see also, H. Taherdoost, *Non-fungible tokens (NFT): A systematic review,* in *Information,* 2023, pp. 1-12.

[25] C. Di Bernardino, A. Chomczyk Penedo, J. Ellul, A. Ferreira, A. von Goldbeck, R. Herian, A. Siadat, N. L. Siedler, *NFT - Legal Token Classification*, July 22, 2021, EU Blockchain Observatory and Forum NFT Reports, available at SSRN: https://ssrn.com/abstract=3891872, p. 2; P. De Pasquale, *Crypto art e NFT nell'Unione europea: aporie sistemiche e ragioni di una (dis)attesa disciplina,* in *Il diritto dell'Unione europea,* 2022, pp. 1-26.

[26] *Ivi*, 3.

[27] It is worth mentioning that NFTs are currently living a period of crisis, which has led some to claim that they are dead. For an interesting analysis, see R. McDougall, *Are NFTs Dead?*, in *MarketPlace Fairness*, October 2023, https://www.marketplacefairness.org/cryptocurrency/are-nfts-dead/.

gradually and steadily, rather than in a sudden wave, it becomes evident that Blockchain can serve as both a technology subject to regulation and a technical model that can facilitate regulation itself. It possesses the characteristics of being both regulatable and regulatory, signaling its dual role in shaping the legal and regulatory landscape.

These characteristics are, therefore, strictly related to the discussion around the concept of code-based rules and the relationship between code and the law.

From a factual point of view, it might be difficult for the law, in the absence of regulatory intervention, to directly alter the code, stop its execution or reverse its effects if they were contrary to the law.

Concerning the political dimension, this reflects the divergence between those who claim the autonomy of the Blockchain system and who approach it as any other technology, searching within the broader realm of socio-technological solutions that are embedded within comprehensive political and legal contexts.

From a legal perspective, it is a debated question as to what extent some rules (i.e., regarding specific legal protection and possible opting out) can (or should) be mandatory on the international level in transactions deployed across legal and geographical borders.

In the context described, several legal questions have started arising with respect to, *inter alia*, how Blockchain can transform certain areas of law and whether the technology can be subject to legal control. The reason is that, as already mentioned, some even consider that Blockchain might not be "bound by terms of law and jurisdiction"[28] but only by code.

Clearly, when it comes to approaching the regulation of Blockchain, it is essential to consider that this does not simply imply considering either what features of Blockchain might be adaptable to the traditional regulatory systems or whether it

[28] P. Vigna, *Chiefless Company Rakes In More Than $100 Million*, *https://www.wsj.com/articles/chiefless-company-rakes-in-more-than-100-million-1463399393*.

requires an *ad hoc* scheme; it must deal equally with prior concerns for regulatory legitimacy and be untied from its application to cryptocurrency so as to understand the broader implications.

Since Blockchain promises to create an entirely novel socio-economic model and a unique paradigm shift regarding data collection, sharing and processing, analyzing the potential/possibility to regulate Blockchain lays the groundwork for investigating to what extent existing legal frameworks can be applied to the technology and consequently the implications of using this technology for the individual's rights.[29]

3. The European Data Protection Framework

In 2011, the World Economic Forum published a report titled "Personal Data: The Emergence of a New Asset Class,"[30] expressing concerns about the erosion of user confidence and trust due to rapid technological advancements and the commercialization of personal data. The report highlighted the growing apprehension regarding the misuse of personal data and the public's unease concerning the extent of knowledge about individuals.

Since then, various scandals have come to light, revealing unethical practices in collecting personal data that have had detrimental effects on democracy. One notable example is the Cambridge Analytica scandal,[31] which surfaced in early 2018. These

[29] Both the CJEU and the ECtHR tend to treat data protection in their case-law as closely related to the right to privacy. Particularly, the ECHR has no corresponding provision to Article 8 of the Charter, and in the absence of such a provision, the ECtHR has derived the right to data protection from Article 8 of the ECHR on the right to privacy. *See,* Judgements of the ECtHR of 16 February 2000, *Amann v. Switzerland,* no.27798/95, para 65; and 4 May 2000, *Rotaru v. Romania,* no. 28341/95, para. 43. For an in-depth analysis of the differences between the two Courts, *see* J. Kokott, C. Sobotta, *The distinction between Privacy and Data Protection in the Jurisprudence of the CjEU and ECtHR,* in *International Data Privacy Law,* 2013, vol. 3(4), pp. 222-228.

[30] https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

[31] During the 2010s, a British consulting firm named Cambridge Analytica collected personal data from millions of Facebook users without their consent, primarily for use in political advertising. The data acquisition occurred through an application known as "This Is Your Digital Life," created by data scientist Aleksandr Kogan and his company, Global Science Research, in 2013. This app featured a series of questions aimed at constructing psychological profiles of users and gathering personal data

incidents have heightened the urgency to address personal data protection, and in response to these concerns, the EU implemented the General Data Protection Regulation (GDPR)[32] in May of the same year.

The GDPR replaced the previous directive and aimed to establish updated safeguards for personal data and the right to data protection, which is enshrined in Article 8(1) of the Charter of Fundamental Rights[33] and Article 16 of the Treaty on the Functioning of the European Union (TFEU).[34]

from the Facebook friends of its users through Facebook's Open Graph platform. The app managed to harvest data from as many as 87 million Facebook profiles. Cambridge Analytica utilized this data to provide analytical support to the 2016 presidential campaigns of Ted Cruz and Donald Trump. The firm was also widely accused of interfering in the Brexit referendum, although the official investigation determined that the company's involvement was limited to initial inquiries, and no significant breaches occurred. The revelation about the misuse of this data came to light in 2018 when Christopher Wylie, a former Cambridge Analytica employee, disclosed the information in interviews with The Guardian and The New York Times. In response, Facebook issued an apology for its role in the data collection, and CEO Mark Zuckerberg testified before Congress. In July 2019, the Federal Trade Commission announced that Facebook would be fined $5 billion for privacy violations. Additionally, in October 2019, Facebook agreed to pay a £500,000 fine to the UK Information Commissioner's Office for exposing its users' data to a "serious risk of harm." In May 2018, Cambridge Analytica filed for Chapter 7 bankruptcy.

For further information: https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10?r=US&IR=T;
https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[32] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

[33] As rightly maintained by Rossi Dal Pozzo and Zoboli, "Article 8 of the Charter of Fundamental Rights is the culmination of a codification process and *constitutionalization of the right to the protection of personal data* as built up in the case law, and at the same time it constitutes the cornerstone of the new legislative framework. With Article 8 of the Charter, from a dimension of essentially negative character – codified also by Article 7 of the Charter concerning the right to respect for private and family life – the right to the protection of personal data leads to a positive dimension: Article 8 of the Charter establishes the existence of a new autonomous right." See F. Rossi Dal Pozzo, L. Zoboli, *To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within the EU,* in *Eurojus,* 2021, p. 318.

[34] "Everyone has the right to the protection of personal data concerning them.
The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union."

This landmark Regulation not only harmonizes data protection laws across EU Member States but also serves as a global standard[35] and a benchmark in the fields of data protection and EU law.[36] The GDPR represents a significant milestone in returning control over personal data to individuals, emphasizing their rights as data subjects. [37]

The GDPR is a technologically neutral Regulation,[38] as it ensures the protection of personal data without any inclination towards specific technologies used for data processing. It applies to both automated and manual processing as long as the data is organized based on predetermined criteria (such as alphabetical order). The storage method and means of data processing is also irrelevant under the GDPR's scope. Whether stored in an IT system, captured through video surveillance, or documented on paper, the GDPR mandates that personal data adhere to the specified protection requirements.

In shaping this Regulation,[39] the European Union sought to provide robust protection for individuals' personal data. However, the EU data protection framework extends beyond the scope of the GDPR and encompasses a substantial body of case

[35] "The EU has successfully influenced other regional privacy laws by restricting the transfer of personal data from member states to countries without adequate privacy protection", J. Brown, C.T. Marsden, *Regulating Code: good governance and better regulation in the Information Age*, Cambridge: MIT Press, 2018.

[36] As Herian pointed out: "[t]he EU's influence in this regard extends far beyond the boundaries of the Union, which thus implies a far-reaching impact of the GDPR for Blockchain use-cases that do not specifically, intentionally or directly involve personal data of EU citizens.", see R. Herian, *Blockchain, GDPR, and Fantasies of Data Soverignty*, 2019, available at https://oro.open.ac.uk/69445/9/69445.pdf, pp. 45-46.

[37] The GDPR reflects some changes to EU law that have occurred in recent times, such as the enactment of the Treaty and the promotion of the Charter of Fundamental Rights to primary law.

[38] This claim has been proved in Chapter IV, para II.

[39] It is crucial to note that the adoption of the GDPR does not exclude the importance of the previous case law of the CJEU on the interpretation of the repealed Directive nor the Guidelines adopted by the so-called Article 29 Data Protection Working Party (which has become the European Data Protection Board, hereafter EDPB, under articles 68 et seq. of the GDPR). Indeed, during its first plenary meeting the European Data Protection Board endorsed the GDPR-related WP29 Guidelines, see https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

law developed by the European Court of Justice (CJEU).[40] This case law[41] is instrumental in shaping the interpretation and application of data protection principles, emphasizing the overarching objective of upholding the fundamental rights and freedoms of individuals throughout the processing of personal data.

While the right to data protection is not absolute, it grants individuals the autonomy to make informed choices regarding disclosing their personal information. Striking a balance between this right and other fundamental rights is of utmost importance when evaluating the lawfulness of online activities involving the processing of personal data. This balance ensures personal data protection while respecting the broader rights and interests underpinning a democratic society.

In addition to the GDPR and case law, it is crucial to consider other European legal acts[42] that contribute to the comprehensive data protection framework. These acts supplement and complement the GDPR, providing a holistic overview of the legal provisions and mechanisms in place to safeguard personal data.

4. The Interplay between the GDPR and Blockchain

The European Commission's Digital Strategy[43] emphasizes the EU's aspiration to become a global leader in Blockchain technology. However, this objective creates an

[40] For an overview see F. Rossi Dal Pozzo, *La giurisprudenza della Corte di Giustizia sul trattamento dei dati personali*, in *Annali AISDUE I*, 2020, pp. 63-86.

[41] See, *inter* alia, case C-293/12 and C-594/12, *Digital Rights Ireland;* case C-131/12, *Google Spain and Google,* para. 66; case C-40/17, *Fashion ID,* para. 50; case C-362/14, *Schrems,* para. 38; case C-101/01, *Lindqvist;* case C-507/17, *Google*; case C-70/10, *Scarlet Extended*.

[42] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act); Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence and amending certain Union legislative acts, COM(2021)206 final; Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data, COM(2022)68 final.

[43] https://digital-strategy.ec.europa.eu/en/policies/Blockchainstrategy#:~:text=The%20EU%20wants%20to%20be,what's

intriguing conflict between two EU goals: the protection of personal data as outlined in the GDPR and the ambition to excel in Blockchain.

Blockchain technology is designed to achieve decentralization and resilience through replication and function as an append-only ledger. On the contrary, the GDPR aims to facilitate the unrestricted movement of personal data among EU Member States while establishing a framework characterized by specific obligations for data controllers and rights for data subjects. The existence of these rights within the GDPR highlights the inherent conflict between personal data regulations and the immutable nature of Blockchains, which, for instance, could make it challenging to ensure some of these specific rights, such as the right to erasure or rectification.

Prima facie, a structural tension seems to exist between the technical underpinning of the GDPR – the centralized processing of data – and the inherently decentralized nature of the Blockchain technology.

The primary concerns revolve around interpreting the broad definition of personal data according to the GDPR and defining roles and responsibilities in the decentralized environment of the Blockchain. The core idea behind the technology is collective data processing through a peer-to-peer shared protocol, which makes it more difficult to identify a single data controller.

Furthermore, when it comes to applying and complying with the GDPR, it seems easier to operate private Blockchain networks that adhere to the regulations, given that they seem well-suited to fulfil the "privacy-by-design" compliance requirements of the GDPR since monitoring the network is relatively achievable. On the contrary, compliance with the GDPR can be more demanding for public Blockchain networks that operate without permission and, therefore, pose a risk of being incompatible with the objectives and fundamental principles of the Regulation since all data processed in the Blockchain is available to an unlimited number of individuals.

%20in%20it%20for%20you%3F&text=Follow%20the%20latest%20progress%20and%20learn%20more%20about%20getting%20involved.

In general, understanding if there are chances of compatibility for Blockchains and the GDPR relies on the potential interpretations of the Regulation itself and its various technological designs that are being developed.

Notwithstanding this potential incompatibility, both the GDPR and Blockchain share a common purpose, which is crucial for pursuing their objectives and ensuring their coherent application: transparency, data security, and empowering individuals by granting them more control over intermediaries. Furthermore, as already claimed, the GDPR strives to be technologically neutral.[44] As a result, if Blockchain technology were to comply with the complies with the GDPR, it couldof personal data rather than jeopardize it.

In light of the above, this thesis aims to question the interplay and compatibility between Blockchain technology and the GDPR and analyze and assess the possibility of positing Blockchain as a possible solution to protect personal data and return control to data subjects.

5. Defining the Research Questions and Objectives

The primary objective of this research is to thoroughly examine the implications of Blockchain technology on data protection and propose innovative approaches, mechanisms, and best practices to foster a productive dialogue between the technology and the law and to ensure individuals have greater control over their personal information.

The rapid adoption of Blockchain technology has mainly brought promising advancements in the field of digital identity management. This study delves into the legal, technological, and ethical dimensions surrounding Blockchain-based

[44] Recital 15 GDPR. For a distinction between 'technology neutral law' and 'technologically neutral law, see M. Hildebrandt, L. Tielmans, *Data Protection by Design and Technology Neutral Law,* in *Computer Law and Security Review*, 2013, p. 516.

applications, specifically focusing on self-sovereign identity systems. The objective is to provide valuable insights into the necessary adaptations and enhancements required to align these applications with data protection legislation.

The choice to focus on the digital identity management system stems from users/data subjects being at its heart, as they actively participate as agents in the data governance architecture. This use case offers an interesting opportunity to explore whether a decentralized system like Blockchain can be structured to support advanced techniques that implement privacy-enhancing solutions for decentralized data management.

Against the background described above, this PhD thesis, starting from an evaluation of the current data protection regulatory framework, addresses the following research question: Does GDPR provide a conducive framework for Blockchain-based solutions? If affirmative, could the Blockchain be seen as a Privacy Enhancing Technology (PET)?

Answering these questions calls for a techno-legal approach and entails a host of sub-questions:

(i) *Can* Blockchain be subject to legal oversight? If yes, *should* it?[45]

(ii) Should conventional legal systems be modified to accommodate the new paradigm of Blockchain technology, or should a technical legal framework be established to address its unique characteristics?[46]

(iii) What are the key characteristics and technical foundations of Blockchain technology that impact personal data protection, and how can they be addressed effectively?[47]

[46] Questions (i) and (ii) will be addressed in Chapter II.

[47] This topic will be the subject of Chapter III.

(iv) What role can privacy-enhancing protocols play in mitigating privacy concerns within Blockchain ecosystems?

(v) Can Blockchain be considered a tool to achieve GDPR's objectives?[48]

(vi) Can Blockchain-based self-sovereign identity (SSI) enhance data protection rights?[49]

5.1.What This Thesis Is Not About

This thesis lies at the intersection of Information technology law, European Union law, fundamental rights law and technology assessment. Therefore, substantive questions pertinent to the technology will be considered insofar as they are useful to address legal issues.

Although this work examines the Blockchain from a regulatory perspective, this research is not about regulatory models for technology. Nevertheless, analyzing the regulatory challenges is warranted to provide much of the groundwork for examining the data protection implications brought about by this technology.

Likewise, while this thesis assumes that there are ongoing developments in the field of data protection engineering,[50] these results are just occasionally mentioned to investigate whether such techniques can support the practical implementation of data protection principles. Yet, the challenge of proposing how this new approach could improve Blockchain is not taken up.

[48] Questions (iv) and (v) will be addressed in Chapter III and IV.

[49] Chapter IV will be entirely dedicated to the use case of Self-Sovereign Identity.

[50] "Data Protection Engineering can be perceived as part of data protection by Design and by Default. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles. Undeniably it depends on the measure, the context and the application and eventually it contributes to the protection of data subjects' rights and freedoms.", see ENISA, *Data Protection Engeneering – From theory to practice,* January 2022, available at https://www.enisa.europa.eu/publications/data-protection-engineering.

6. Research Methodology

This research combines an information technology perspective and a normative perspective[51] to investigate how the General Data Protection Regulation could be interpreted to meet Blockchain's features. Accordingly, it uses a legal informatic method, focusing on the relationship between law and IT. The legal informatics methodology aims to bridge the gap between IT architecture development and legal expertise, ensuring compliance with legal requirements.

In line with this approach, the thesis will commence by elucidating EU laws and other relevant legal sources pertaining to the personal data domain. This will be accomplished through a legal dogmatic approach,[52] scrutinizing the established legal sources. Subsequently, an analysis will be conducted to evaluate the compatibility of the law and its underlying principles and mechanisms with the Blockchain. The examination will ascertain the extent to which the existing data protection law and Blockchain technology align and identify the legal challenges that need to be addressed.

It is crucial to emphasize that this study will not rely solely on the legal dogmatic approach,[53] as it would not adequately address the goals of this thesis. This is because the research inquiries revolve around a relatively novel technology that has not been extensively explored in EU courts thus far.

The legal analytical method seems the best one to deepen the discussion's terms, as it examines the law from a technical standpoint and allows for critical analysis of potential conflicts between the law and the technology. It further offers certain advantages as it permits the inclusion of various sources, including non-traditional

[51] D. Watkins, M. Burton, *Research methods in law*, Routledge, 2018, p. 29.

[52] A. V. Petrov, A. V. Zyryanov, *Formal-dogmatic approach in legal science in present conditions*, in *Journal of Siberian Federal University - Humanities and Social Sciences*, 2018, pp. 968–973; J. M. Smits, *What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644088, 2015.

[53] The legal dogmatic approach primarily focuses on describing the law as it currently stands, utilizing established legal sources to interpret and clarify its structure.

rules and foreign legal perspectives. This approach creates opportunities to scrutinize the law without necessarily focusing on what is already established or clarified but on how it functions and can be improved. By adopting an analytical perspective, the thesis aims to assess the law without confining itself to a single definitive or optimal solution.

Regarding the research material, the thesis incorporates a wide range of sources to comprehensively address the research questions, confining them within the borders of EU Law. The primary sources include articles from the General Data Protection Regulation (GDPR) and legal cases from the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR) case law. Whilst the CJEU has not yet ruled specifically on Blockchain cases, rulings on other Internet-related questions could be important to understand how interpreting regulatory instruments in force can meet new needs.[54]

In the early days, the Internet raised the same issues that Blockchain now raises. Hence, the normative purpose of this research is to use a comparative method by applying the same approach adopted to fill the regulatory gap created by the Internet.[55]

Given that the thesis deals with the intersection of law and technology, non-legal sources will also be utilized to describe Blockchain technology and its functioning, such as, among others, literature on the operation of the Bitcoin and Ethereum Blockchains. Additionally, non-binding sources of law and opinions from practicing IT lawyers, will be consulted. Besides the academic literature, news articles and other

[54] Richard Posner also observed that: "The messy work product of the judges and legislators requires a good deal of tidying up, of synthesis, analysis, restatement, and critique. These are intellectually demanding tasks, requiring vast knowledge and the ability . . . to organize dispersed, fragmentary, prolix, and rebarbative material.", see Posner R., *In Memoriam: Bernard D, Meltzer (1914–2007)*, University of Chicago Law Review 74, 2007, 409–45, 435, 437.

[55] J. R. Gallagher, *A Framework for Internet Case Study Methodology in Writing Studies*, in *Computers and Composition*, 2019, https://www.sciencedirect.com/science/article/pii/S8755461518300598.

sources, such as blog posts, will be used sparingly to highlight specific issues, trends, perceptions, or noteworthy events.

In addition, this study will entail a *de iure condito* analysis of data protection law, also in light of the documentation produced by the supervisory authorities, i.e., the European Data Protection Supervisor and the European Data Protection Board (henceforth referred to as EDPS and EDPB), as well as the most active and authoritative national Data Protection Supervisory Authorities, such as the CNIL and the AEPD.

Then, the thesis will embark on a *de iure condendo* investigation since – as of now – there are no cases nor legislation which directly target the issues of the data protection implications of Blockchain. Therefore, a critical assessment of the existing scholarly debate on the data protection implications of Blockchain technology will be provided, and models proposed by scholars will be scrutinized, especially focusing on the applicability of the GDPR to Blockchain-based solutions for decentralized digital identity. The results of this extensive literature review will lay the theoretical foundation for this research.

As Webster and Watson recommended, [56] the review started with a keyword search and collecting relevant peer-reviewed literature. Thus, the search has focused on the main terms closely related to the topic of this thesis, namely *Blockchain* and *distributed ledger technology* (the term "Bitcoin" was avoided on purpose, as it only represents one use case of Blockchain technology) and the word *GDPR*, which includes the term *privacy* and *data protection regulation*.

Literature about the research methodology was also collected but is not integral to this main review.[57] The result of this literature review will help to ascertain to what

[56] J. Webster, R. T. Watson, *Analyzing the past to prepare for the future: Writing a literature review,* in *MIS quarterly,* 2002, xiii-xxiii.

[57] C. McCrudden, *Legal Research and the Social Sciences* in *Law Quarterly Review* 122, 2006, pp. 632–650; M. Van Hoecke, *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?*, Oxford Hart Publishing, 2011; R. Cryer, T. Hervey, B. Sokhi-Bulley, A. Bohm (2011).

extent the data protection implications of Blockchain are researched and point out the gap in the current research, as well as identify potential areas for future research.

To that end, along with the research questions listed above, the research process and methodology[58] will be guided by other specific questions,[59] which can be resumed by the following terms that identify the category to which those sub-questions belong: definition,[60] comparison,[61] relationship,[62] testimony,[63] circumstance.[64]

7. Outline

Since the research question revolves around Blockchain, it is imperative first to introduce the technology. Hence, the first chapter of this thesis attempts to outline a simplified yet comprehensive description of all the fundamental concepts underlying the technology.

The second chapter addresses the topic of regulating Blockchain. It does not seek to create a comprehensive European Blockchain technology law or provide an exhaustive regulatory examination of the technology. Instead, it aims to explore potential approaches and regulatory principles for governing this technology. The aim is therefore to provide insights into the regulatory and governance challenges associated with Blockchain technology. By clarifying the key terms and concepts within this discussion, the chapter sets the stage for an in-depth exploration of data protection issues.

[58] For more on the different research methodologies, see R. Cryer, T. Hervey, B. Sokhi-Bulley, A. Bohm, *Research methodologies in EU and International Law*, Hart Publishing, 2011.

[59] D. Watkins, M. Burton (2018), cit, p. 28.

[60] What are the main characteristics of this new technology? What is, if it is already definable, its legal regime? Can data protection law apply to Blockchain-based applications?

[61] *What is this technology like and unlike? Can the approach adopted for internet-based applications be useful to solve data protection issues for Blockchain-based applications?*

[62] *How should this innovation be regulated? Do Blockchain-based applications meet the requirements of the GDPR? In which area this technology is not aligned with the principles of GDPR?*

[63] *What has been written about?*

[64] *How do Blockchain-based digital identity solutions work? Could these applications be regulated by the existing data protection framework?*

The third chapter begins with a concise overview of the circumstances that prompted the development of the GDPR and then delves into the fundamental principles of the GDPR and assesses how it interacts with Blockchain technology. Furthermore, it investigates possible compliance solutions, both from a legal point of view (particularly, on the interpretative level) and a technical point of view, given that margin for mutual adaptation cannot be excluded *a priori.* This last assertion is leveraged by the assumption that the GDPR has a technologically neutral nature and that this is a clear indication of the legislator's willingness to ensure greater longevity of the European Regulation with respect to technological evolution. Additionally, another element to consider is that the Blockchain is still under development and that technological solutions concerning privacy-enhancing techniques[65] can be found to ensure data protection fits with the stage of technology development.

The fourth chapter aims to assess whether Blockchain-based digital identity systems, precisely the Self-sovereign Identity (SSI), could potentially provide a solution to allow users to assume control of their identities. While we acknowledge that SSI is a technological paradigm founded on various principles, making it a technology-agnostic concept that doesn't inherently require Blockchain for implementation, we often use it interchangeably with the term 'Blockchain-based identity management systems.'

Moreover, in our attempt to outline the existing regulatory framework that governs Blockchain-based digital identity systems, we will also encounter the eIDAS Regulation, which is the reference law for digital identities and does not encompass SSI, although it is currently under revision.

[65] In Chapter 4 the thesis will investigate whether Blockchain could be defined a Privacy Enhancing Technology (PET), which "stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system. PET try to manage the privacy threats that software agents face.", see G. V. van Blarkom, J.J. Borking, J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies,* College bescherming persoonsgegevens, 2003, p.3.

The proposal to review the eIDAS Regulation will also be analyzed[66] in order to verify whether the proposed new legal provisions leave room for Blockchain and, if yes, in what terms and what degree of potential effectiveness.

[66] A detailed analysis of all new changes would go beyond the scope of this thesis; hence, we will focus only on those most relevant for the implications to the SSI systems.

Chapter I

Blockchain Technology: Easing into the Nodes

> *"[A]ll truth passes through three stages: First, it is ridiculed.*
> *Second, it is violently opposed.*
> *Third, it is accepted as self-evident."*
>
> Arthur Schopenhauer

1. Introduction – **2.** The Concept of Decentralized Technologies – **2.1.** Decentralized Ledger Technologies in the European Legal Framework - **3.** History and Evolution of Blockchain – **4.** Clearing up the Clouds: a Deep Dive into the Technology – **4.1.** Blockchain's Architecture – **4.2.** The Consensus Protocols: Trust in Algorithms? – **4.3.** Cryptography as a Key Feature – **4.4.** Types of Blockchain – **5.** Blockchain Use Case's Structure: An Overview – **5.1.** Smart Contracts – **6.** Conclusion

1. Introduction

This chapter introduces the notion of distributed ledger technologies (DLTs) and deepens Blockchain technology[67] by providing an overview of its technical components from a functional perspective.

The legal implications of such technical elements will be briefly presented at times, as they will be the subject of the following chapters.

From a technical point of view, the Blockchain is just one of the DLTs. Although this thesis will exclusively focus on Blockchain, some references to DLTs will be made to highlight their differences and commonalities.

[67] M. Swand, P. De Filippi, *Toward a philosophy of Blockchain: A symposium, Introduction*, in A. T. Masoobian (ed.), *Metaphilosophy*, 2017, p. 603; for a critical analysis see M. Atzori, *Blockchain technology and decentralized governance: is the state still necessary?*, 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713; R. Ramadoss, *Blockchain technology: An overview*, in *IEEE Potentials*, 2022, pp. 6–12; Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress,* 2017, pp. 557–564.

A detailed analysis of the features underlying the Blockchain would go beyond the scope of this thesis, which intends to focus on the data protection implications of this technology. However, given that data protection is closely related to the functioning of technologies, it is worth giving a synopsis of specific components of Blockchain, which are essential from a data protection law perspective.

Despite considering those technical concepts from a legal perspective, accurate and detailed informatic language will be maintained.

This chapter is divided into 10 sections and sub-sections. After this introduction, Section 2 establishes an idea of decentralization and how it merged with technological developments. Section 2.1 briefly focuses on the legal definitions of decentralized ledgers. Section 3 elaborates on the history and evolution of Blockchain since the advent of Bitcoin. Section 4 – including its sub-paragraphs - presents Blockchain in its technical components by highlighting the elements that pose the most significant problems from a data protection point of view, and that will be deepened hereinafter. Finally, sections 5 and 5.1. provide an overview of the use case's framework, deferring any details to the following chapters.

2. The Concept of Decentralized Technologies

Decentralization is one of the core characteristics of every Blockchain.[68]

The term refers to the process of transferring or distributing power away from a hierarchical and centralized entity. It can be both a private organization and a public authority.

In 1964 Paul Baran, in his memorandum[69] RM-3420-PR "On distributed communications: I. Introduction to distributed communications networks",

[68] For a detailed and through analysis of this concept, see: M. R. Hoffman, L. D. Ibáñez, E. Simperl, *Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework* in *Frontiers in Blockchain*, 2020, pp. 1-18.

[69] P. Baran, *On distributed communications: I. Introduction to distributed communication networks*, Santa Monica, CA: RAND Corporation, 1964, available at https://www.rand.org/pubs/research_memoranda/RM3420.html.

introduced the concept of information distribution. "He indicated and proposed (by presenting suitable calculations) a decentralized and distributed method of connecting nodes (devices) and sending data (the Blockchain was developed much later, based on that concept). He classified (data-distribution) networks into three types: centralized, distributed and, within that category, decentralized networks".[70]
Over the years, this phenomenon has involved various domains, such as decentralization of administration, economics, politics, and technology.[71]
As effectively described by Benkler, decentralization allows "conditions under which the actions of many agents cohere and are effective although they do not rely on reducing the number of people whose will counts to direct effective action."[72]

According to a report by the United Nations Development Program (UNDP), one of the meanings of decentralization is "…a complex phenomenon involving many geographic entities, societal actors, and social sectors. The geographic entities include the international, national, sub-national, and local. The societal actors include government, the private sector and civil society. The social sectors include all development themes- political, social, cultural and environmental. In designing decentralization policies and programs, it is essential to use a systems approach encompassing these overlapping social sectors and the different requirements which each makes…. Decentralization is a mixture of administrative, fiscal and political functions and relationships. In the design of decentralization systems, all three must be included."[73]

[70] D. Szostek, *Blockchain and the law*, Nomos, 2019, p. 35.

[71] B. Bodó, J.K. Brekke, J.H. Hoepman, *Decentralisation in the Blockchain space* in *Internet Policy Review*, 10(2), 2021, pp. 1-12.

[72] Y. Benkler, *The Wealth of Networks - How Social Production Transforms Markets and Freedom*, Yale University Press, 2006, available at http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf

[73] *Decentralization: A Sampling of Definitions*, Working Paper by UNDP, 1999, available at http://web.undp.org/evaluation/documents/decentralization_working_report.pdf.

Essentially, decentralization embraces multidisciplinary models that can be used for different purposes.[74] Thus, the primary function of decentralization is to shift the central point of control from a centralized system to a decentralized one; consequently, in these structures, any particular entity does not have all the power to alter any aspect of the system. This simple concept has been applied in cyberspace as well.

A decentralized system can run as a peer-to-peer network of independent computers globally and not managed by a central party; therefore, the role of a third party or intermediaries is reduced.

One of the first use of the term Distributed Ledger Technology can be traced back to 2016 in a document entitled "A Report by the UK Government Chief Scientific Adviser".

> The authors stated that distributed ledgers are "a type of database that is spread across multiple sites, countries or institutions, and is typically public. Records are stored one after the other in a continuous ledger, rather than sorted into blocks, but they can only be added when the participants reach a quorum. A distributed ledger requires greater trust in the validators or operator of the ledger".[75]

Blockchain is a technology that functions on a decentralized data governance model. Blockchain-based systems are designed to support technological decentralization to a certain degree. Decentralization in Blockchains refers to the global network of computers operating on a peer-to-peer basis.

[74] Given that it is still difficult to clarify the specific degree of decentralization of Blockchain, some authors propose a method based on two approaches: J. Lee, B. Lee, J. Jung, H. Shim, H. Kim, *DQ: Two approaches to measure the degree of decentralization of Blockchain*, in *ICT Express*, *7*(3), 2021, pp. 278–282.

[75] *Distributed Ledger Technology: beyond block chain - A report by the UK Government Chief Scientific Adviser* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 2016, pp. 17-18.

> Brakeville pointed out: "[t]he decentralized peer-to-peer Blockchain network prevents any single participant or group of participants from controlling the underlying infrastructure or undermining the entire system. Participants in the network are all equal, adhering to the same protocols. They can be individuals, state actors, organizations, or a combination of these types of participants."[76]

Vitalik Buterin, the creator of Ethereum, the second most relevant Blockchain platform thus far, further clarifies the concept of decentralization by dividing Blockchain technology into three areas: architectural, political and logical.

The architectural (de)centralization answers the question: "How many *physical computers* is a system made up of? How many of those computers can it tolerate breaking down at any single time?"; the political (de)centralization answers the question: "How many individuals or organizations ultimately control the computers that the system is made up of?". Ultimately, the logical area answers the question: Do the interface and data structures that the system presents and maintains look more like a monolithic object or an amorphous swarm? One simple rule of thumb is: if you cut the system in half, including providers and users, will both halves continue operating as independent units fully?

> For Buterin, "Blockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state, and the system behaves like a single computer)."[77]

The words of one of the key players in the Blockchain world summarise what has been already anticipated in the previous pages: decentralization is grounded on creating a

[76] S. Brakeville, *Blockchain basics: Introduction to distributed ledgers*, 2018, available at https://developer.ibm.com/tutorials/cl-Blockchain-basics-intro-bluemix-trs/.

[77] V. Buterin, The meaning of decentralization, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

public ledger, including a complete record of past transactions shared amongst all nodes of the network, instead of relying on a centralized ledger.

Decentralization implies a kind of distribution, and Blockchain brings new technologies to consistency in distributed systems and mutual trust, recognition, and interconnection worldwide.

As will also be analyzed in the following pages, decentralization makes the Blockchain-based infrastructure verifiable and transparent, ensuring the integrity of the system and participants from the moment the data are stored across the global network of computers. This feature provides the security of the data to a large extent, furthermore, "[t]he magic of distributed ledger is to make certain activities trustworthy without the need to trust anyone in particular"[78].

We will return to these features of Blockchain that raise the most remarkable data protection problems on which this research has focused the most.

2.1.Decentralized Ledger Technologies in the European Legal Framework

The regulatory aspects of Blockchain will be dealt with more extensively in the following chapter, which is dedicated to the challenges posed by the attempt to regulate this phenomenon. This section only intends to present briefly the first – and, so far, most recent – European law on distributed ledger technologies, leaving its critical assessment to the rest of the dissertation.

Nevertheless, while presenting the technical features of Blockchain, the definitions contained in that Regulation will be evaluated.

[78] K. Werbach (2018), cit., p. 497

On 30 May 2022, Regulation (EU) 2022/858[79] came into force, regulating a pilot regime for market infrastructures based on distributed ledger technology (DLT). The Regulation establishes and regulates a temporary pilot scheme to enable market infrastructures operating with DLT technology to trade and settle crypto-assets transactions covered by financial services legislation. Notably, the Regulation applies from 23 March 2023. It is part of the EU Commission's broader 'Digital finance package',[80] which includes, *inter alia*, two other parts of legislation (the MiCA regulation on the market in crypto assets[81] and the DORA regulation on digital operational resilience for the financial sector[82]), as well as the necessary amendment of directives in force. This Regulation establishes a temporary regime for market infrastructures that operate through DLT to test such technologies and allow the development of crypto assets that fall under the definition of financial instruments while ensuring a high level of investor protection, market integrity, financial stability and transparency.

This scheme will be subject to a 'review' in 2026, following a report on the functioning and risks of the pilot scheme by the Commission, which, based on a cost-benefit analysis, will determine whether the pilot scheme can be extended for a maximum

[79] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance), OJ L 151 of 2.6.2022, p. 1–33.

[80] "Based on broad public consultations and the Digital finance outreach, the European Commission adopted on 24 September 2020 a digital finance package, including a digital finance strategy and legislative proposals on crypto-assets and digital resilience, for a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability. The package supports the EU's ambition for a recovery that embraces the digital transition. Digital financial services can help modernize the European economy across sectors and turn Europe into a global digital player. By making rules more digital-friendly and safe for consumers, the Commission aims to leverage synergies between high innovative start-ups and established firms in the financial sector while addressing associated risks", https://finance.ec.europa.eu/publications/digital-finance-package_en.

[81] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

[82] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

period of three years and/or broadened to other types of financial instruments, amended, made permanent or abolished.[83]

According to the regulation, "(1) distributed ledger technology or 'DLT' means a technology that enables the operation and use of distributed ledgers" and "(2) 'distributed ledger' means an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism."
These definitions' terms (some unclear at this stage) will be cleared hereinafter.

3. History and Evolution of Blockchain

Having introduced what decentralization means, this section targets Blockchain from a technological point of view. The analysis of the various layers of the Blockchain ecosystem will lay the foundation to reflect on the evolution of some specific use cases and applications of the technology and investigate which areas of law might be affected by Blockchain's impact.
We will retrace some of the notions already anticipated in the introduction to detail them more thoroughly or to use them to introduce other essential concepts.

The Blockchain was described for the very first time in a paper distributed online[84] in late 2008 by a person (or a group of people)[85] known by the pseudonym Satoshi Nakamoto who applied to Blockchain many concepts already familiar to

[83] Among the most important innovations, the Regulation introduces the notion of a "DLT financial instrument" understood as financial instruments which are issued, transferred and stored on a distributed ledger and new, dedicated market infrastructures in which such instruments are traded. Moreover, only shares, bonds and fund shares are admitted to trading or may be registered in a DLT market infrastructure within the limits of thresholds identified both in relation to the issuer of the securities and the aggregate market value limits, in order to avoid financial stability risks.

[84] S. Nakamoto, *Bitcoin a Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf.

[85] Nakamoto is the pseudonymous mastermind behind Bitcoin.

cryptographers. Almost all the components originated in academic research from the 1980s to 1990s,[86] and many digital currencies (such as Digicash, for instance) can trace their origins as far back as 1989.[87]

Satoshi Nakamoto described how cryptology and an open distributed ledger could be combined into a digital currency application to create a new monetary unit. Accordingly, rather than being an entirely novel technology, Blockchain is better known as an inventive combination of existing mechanisms. The novelty was represented by the innovative way the system was implemented to create a decentralized form of digital cash, called bitcoin, a "purely peer-to-peer version of electronic cash".[88]

The paper by Satoshi Nakamoto has been defined as "[t]he most important contribution in monetary economics in the twenty-first century."[89] He/they proposed the introduction of an electronic version of money, allowing direct peer-to-peer (P2P) payments to eliminate participation in the payment system of central authorities and intermediaries.

Although Blockchain was created to facilitate cryptocurrency transactions and, at first, the extremely high volatility of bitcoin and the attitudes of many Countries toward its complexity restrained its development somewhat, it has managed to

[86] A. Narayanan, J. Clark, *Bitcoin's Academic Pedigree*, in *Communications of the ACM*, 2017, p. 36.

[87] David Chaum founded Digicash in 1989 to capitalize on his theoretical work in digital currency. In 1982 Chaum earned his doctorate in computer science from the University of California, Berkeley with a dissertation entitled "Computer Systems Established, Maintained and Mutually Trusted by Suspicious Groups" which is a prototype of Blockchain technology. Although Digicash fail to build on early successes, it was a crucial early proponent of public and private key cryptography, the same basic principle that is used by digital currencies today. Known as "Blind Signature" technology, Chaum's invention both enhanced security for DigiCash users and made electronic payments untraceable by outside sources, D. Chaum, *Blind signatures for untraceable payments,* 1998, http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

[88] Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

[89] F. Schar, A. Berentsen, *Bitcoin, Blockchain and cryptoassets*, The MIT Press, 2020, p.3.

distinguish itself from cryptocurrencies, and its edges have attracted increasing attention.[90]

Blockchain's advantages include its distributed ledger, decentralization, information transparency, tamper-proof construction, and openness.

The application of Blockchain technology has extended from digital currency to finance, from health care to supply chain management, market monitoring, smart energy, and copyright protection.[91]

Based on the above, this chapter provides an overview of the characteristics of Blockchain, which, while using complex technology, has a simple yet disruptive function: providing a distributed and accurate ledger of which everyone can maintain a very identic copy.

As anticipated, this thesis intends to present only some of the technical key mechanisms underlying this new paradigm.[92] Specifically, it will be clarified that three features are common to every Blockchain: decentralization, security and scalability.[93] These attributes lead to the other two pillars of this technology:

[90] See: I. Pejic, *Blockchain babel – The Crypto Craze and the Challenge to Business*, Kogan Page, pp. 1-23.

[91] For further details on the application of the Blockchain to various sectors, see the reports of the EU Blockchain Observatory and Forum https://www.euBlockchainforum.eu/knowledge.

[92] A. Narayanan, J. Clark (2017), pp. 36-45.

[93] This is also defined as 'The Blockchain Trilemma', that addresses the challenges developers face in creating a Blockchain that is scalable, decentralized and secure — without compromising on any facet. Blockchains frequently encounter challenges that necessitate trade-offs, limiting their ability to simultaneously achieve all three fundamental aspects. Decentralization means designing a Blockchain system that operates without dependence on a central authority or control point; scalability means ensuring that the Blockchain system can effectively handle a continuously expanding volume of transactions; security means establishing the capability of the Blockchain system to operate reliably, withstand attacks, address bugs, and mitigate unforeseen issues. Blockchains often face difficulties in striking a balance among these aspects, making it challenging to achieve optimal levels of decentralization, scalability, and security simultaneously. Regardless of the shape of the Trilemma, it is agreed that it is difficult for any Blockchain system to effectively achieve decentralization, scalability, and security. Cfr. J. Werth, M. Berenjestanaki, H. Barzegar et al, *A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma,* in *International Conference on Enterprise Information Systems, ICEIS – Proceedings,* 2023, pp. 146-155; S. Reno, M. Haque, *Solving Blockchain trilemma using off-chain storage protocol*, in *IET Information Security,* 2023, pp. 681-702.

transparency and immutability.[94] Instead, the openness of the system and the consensus protocol may differentiate from one Blockchain to another.

Considering Blockchain technology can be seen as both an ideology and a paradigm for efficient practical uses, this chapter will highlight how a Blockchain works by stressing the importance of the *consensus protocol* for making a Blockchain trustworthy. Ultimately, as anticipated, sections 5 and 5.1 of this chapter will overview the most interesting and common use cases already in place.

4. Clearing up the Clouds: A Deep Dive into the Technology

In the years that followed the creation of Bitcoin, many other cryptocurrencies were created, differing from the Bitcoin network in various ways.

Numerous definitions of Blockchain exist; some of them stress different technical features of the respective forms of data management.

> "[D]espite a plethora of definitions, descriptions, and applications of Blockchain and decentralized ledger, the technology and its various incarnations share a core functionality in providing a decentralized consensus. Decentralized consensus is a description of the state of the world—e.g., whether the goods have been delivered or

[94] Blockchain is also considered a deterministic system, as it supports only one version of the truth: "Blockchain is known for carrying out transactions in a transparent and highly secure way. These transactions are approved by Blockchain nodes, who have the exact same copy of the complete Blockchain ledger — or technically called the "state" of the Blockchain — at any given time. The "state" of the Blockchain refers to the data contained in the Blockchain ledger and a new state is achieved every time a new transaction is added to the Blockchain. No node on the Blockchain can have a different state compared to the rest of the network. This is only possible when each node can produce the same result for the same input at any point in time. And as Blockchains are transparent, any node that tries to manipulate the state can easily be noticed and thus, disregarded, keeping the integrity of the system intact.", A. Abbas, *What is Determinism in a Blockchain Network?* — Alacrity Network, 2020, https://medium.com/@adilsvp/what-is-determinism-in-a-Blockchain-network-alacrity-network-5d1f58449779.; see also, Y. Zhao, X. Kang, T. Li, C. K. Chu, H. Wang, *Toward Trustworthy DeFi Oracles: Past, Present, and Future*, in *IEEE Access*, 2022, pp. 60914–60928.

whether a payment has been made—that is universally accepted and acted upon by all agents in the system."[95]

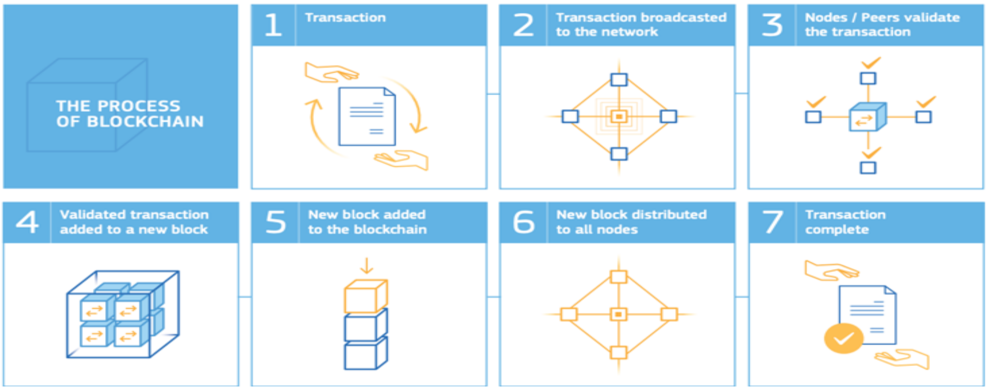

THE PROCESS OF BLOCKCHAIN
1 Transaction
2 Transaction broadcasted to the network
3 Nodes / Peers validate the transaction
4 Validated transaction added to a new block
5 New block added to the blockchain
6 New block distributed to all nodes
7 Transaction complete

Figure 1. *How a Blockchain works*
Source: S. Nascimento et al, *Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*, EUR 29813 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-08977-3, doi:10.2760/901029, p.14.

The term Blockchain[96] refers to a technology that allows creating and managing a decentralized and distributed digital ledger in which 'transactions'[97] are stored, recorded in chronological order, transferred and finally shared among the nodes[98] participating in the network.[99] The latter are hardware devices communicating with others in the so-called peer-to-peer network. As a result, a Blockchain allows the storage and transmission of information transparently and securely without relying on a trusted third party.

[95] L.C. Cong, Z. He, *Blockchain disruption and smart contracts*, in *Nber Working paper series*, 2018, p. 1.
[96] There is no agreement on the terminology.
[97] In its most basic meaning, a transaction is any operation that can change the state of a system. In the case of Bitcoin, a transaction consists of the transfer of an amount from one address to another. As a result of the transaction, the state of the Blockchain is changed (the 'balance' of the two 'accounts' before and after the transaction is in fact different). In blockchains that support smart contracts, transactions, rather than transferring value, are a means of interacting with a smart contract, i.e. 'operations' (recorded on the Blockchain) that aim to change the state of the contract, e.g. through the creation and/or transfer of digital assets (tokens). The important aspect is that whatever the content of a transaction, the ultimate goal is to change the state of the system (resulting in 'write' operations on the Blockchain). In contrast, merely reading the state of a Blockchain is not a transaction (and in fact has no associated cost in terms of 'gas', in the case of Ethereum). Cfr. https://river.com/learn/how-does-a-bitcoin-transaction-work/.
[98] For more details about the distinction between nodes, see section 4.1.
[99] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, *Blockchain,* in *Business and Information Systems Engineering*, 2017, pp. 183-187; B. Singhal, G. Dhameja, P. Sekha Panda, *Beginning Blockchain – a beginner's guide to building Blockchain solutions*, Springer, 2018; V. Dhillon, D. Metcalf, M. Hooper, *Blockchain-enabled application*, Springer, 2017.

The described networks achieve resilience through replication, and, as its etymology reveals, they are structured as a series of encrypted blocks[100] aggregated and networked along a chain. A single block groups together multiple transactions that are then added to the existing chain of blocks through a hash function. This refers to using cryptography to transform data of any size into a unique fixed-sized output.[101] Cryptography[102] is a Blockchain's distinctive architectural element that allows data not to be retroactively altered once recorded in a given block unless all subsequent blocks are altered. This feature will be the focus of section 4.3 of this chapter.

One of the ledger's properties is resilience, as the data is simultaneously stored on many nodes. This means the data is unaltered even if one or several nodes fail. Such data replication entails no central point of failure at the hardware level; however, the following chapters will argue that there is a central point of attack at the governance level.[103]

Furthermore, a Blockchain can qualify as an append-only data structure since blocks are continuously added but never removed. Accordingly, before being added to the chain, each block must be checked, validated, and executed according to the chosen

[100] Each block also contains a "header": '[e]ach block has a block header, a hash pointer to some transaction data and a hash pointer to the previous block in the sequence. The second data structure is a per-block tree of all transactions included in that block. This is a Merkle tree and allows us to have a digest of all the transactions in the block in an efficient way'. See A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Godfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* Princeton University Press, 2016; also see figure 2 below.

[101] See A. Jamshed, M. Bhardwaj, M. Pandey, K. Kant Agrawal, *Securing through pseudorandom number generator and hashing in cryptography,* in *Journal of emerging technologies and innovative research,* 2019, pp. 203-206.

[102] See D. Yaga, P. Mell, N. Roby, K. Scarfone, *Blockchain Technology Overview*, Draft NISTIR US Department of Commerce, National Institute for Standards and Technology, 2018, https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf.

[103] Though the coercive power of the law cannot be readily applied to regulate Blockchain-based systems, existing laws can, nonetheless, indirectly influence the operations of these platforms. This means that even if many Blockchain-based networks operate outside of the reach of the law, the various actors involved in the governance of these networks can be subject to the law. See chapter II, para 4.4.

validation protocol, also known as the "consensus algorithm" or "consensus mechanism".[104]

The non-need for trust is indeed a pivotal premise of Blockchain systems.

4.1. Blockchain's architecture

Before talking at length about how the trust mechanism in the Blockchain works, it is worth spending a few more words on what the nodes are, as they represent a critical component of the Blockchain's infrastructure.

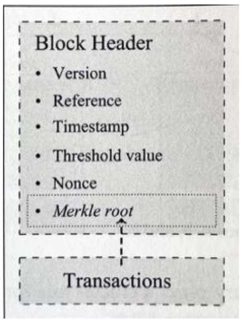


Figure 2. *Structure and components of a block* (F. Schar, A. Berentsen, 2020)[105]

Each node is a computer connected to the network responsible for controlling the integrity of the decentralized registry that constitutes the Blockchain.

Nodes receive information from users' applications – that is, the transactions - and they have the task of validating, checking and aggregating it into a block. Then every new block is added to the chain and retransmitted to the other nodes.

In a nutshell, all nodes on a Blockchain are connected and constantly exchange the latest Blockchain data with each other, so all nodes stay up to date.

[104] The consensus mechanisms make possible for distributed network of peers to store information in a Blockchain without the need to rely on any centralized operator or middleman. See A. Narayanan et al (2016).

[105] F. Schar, A. Berentsen, *Bitcoin, Blockchain, and crypto assets -A comprehensive Introduction*, The MIT Press, 2020, p. 141.

In this regard, it is worth stressing that only some Blockchain participants perform the same functions. A distinction must indeed be drawn between full nodes and light nodes.[106] Full nodes contain a full copy of the transactions that have ever been performed on the Blockchain. Thus, they are essential to ensure the Blockchain's integrity by downloading and verifying the whole chain of blocks.

Nonetheless, considering this operation is costly regarding time and resources, a participant unwilling to engage in this effort can be a 'light node'. Light nodes do not interact directly with the Blockchain but can send transactions using full nodes as intermediaries. This enables them only to keep a partial copy of the whole chain of transactions.

In the network, an essential category of nodes is that of *mining nodes* which have a crucial function: validating the transactions. Accordingly, a mining node must always run a full node to select valid transactions to form a new block. As peers, they determine which blocks will be added to the Blockchain through the consensus protocols that allow network actors to agree on the transaction's validity.

It is worth clarifying from the outset that the mining nodes do not agree on the specific content of each transaction. Instead, they verify that the solution to the complex cryptographic puzzle is the same for many nodes.

[106] "A full node stores all the data in the Blockchain, including block headers and data records. A miner is a full node with great computing power, responsible for constructing consensus proofs (e.g., nonce in the Bitcoin Blockchain). A light node stores only block headers, which include the consensus proof and the cryptographic hashes of a block. Note that the data records are not stored in light nodes. To ensure the integrity of queries over a Blockchain database, the query user could join the Blockchain network as a full node. Then, the user can download and validate the entire database and process queries locally without compromising the query integrity. However, maintaining a full copy of the entire database might be too costly to an ordinary user, as it requires considerable storage, computing, and bandwidth resources. For example, the minimum requirements of running a Bitcoin full node include 200GB of free disk space, an unmetered broadband connection with upload speeds of at least 50KB per second, and a running time of 6 hours a day.", see https://www.researchgate.net/figure/A-Blockchain-Network-node-A-full-node-stores-all-the-data-in-the-Blockchain-including_fig1_333865080.

In light of the above, one might wonder what precisely the nodes reach a consensus on. The answer is that nodes must agree on exactly which transactions were broadcast and the order in which these transactions happened so that the result is a single, global ledger for the system. Hence, at any given point, all the nodes in the peer-to-peer network have a ledger consisting of a sequence of blocks; each block usually[107] contains at least one transaction on which they have reached a consensus.[108] Every block must include some specific content. A block must include the so-called block header consisting of 640 bits of descriptive data that allow the block to be identified and located within the Blockchain.

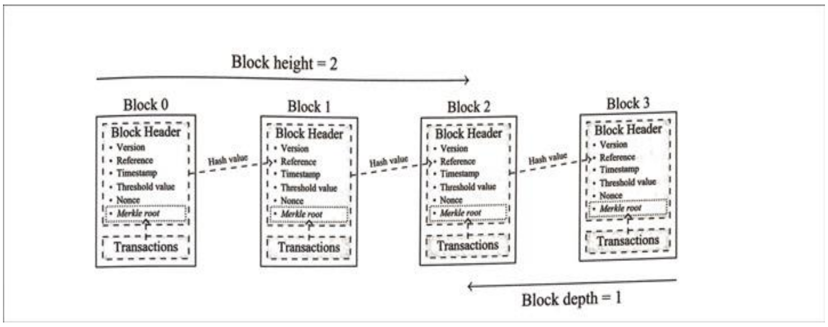


Figure 3. *Example of a Blockchain* (F. Schar, A. Berentsen, 2020).
F. Schar, A. Berentsen, *Bitcoin, Blockchain, and crypto assets -A comprehensive introduction*, The MIT Press, 2020, p. 143.

The definition of 'DLT network node' contained in the Regulation (EU) 2022/858[109] perfectly condenses what a node in the Blockchain is: "(…) a device or process that is part of a network and that holds a complete or partial replica of records of all transactions on a distributed ledger".

[107] Technically, it is true that every block contains at least one transaction, i.e. the one that rewards the miner for adding the block to the Blockchain. Apart from this (which represents a particular type of transaction called "coinbase" because it is the one that generates new cryptocurrency), it is possible to have empty blocks. In this case, the miner will only be rewarded for the added block, not the individual transaction fees. Cfr. https://cointelegraph.com/news/you-don-t-see-that-every-day-bitcoin-empty-block-found.

[108] More accurately, each node has a pool of outstanding transactions that it has heard about but has yet to be included on the Blockchain. For these transactions, a consensus has not yet been reached, and so by definition, each node might have a slightly different version of the outstanding transaction pool. In practice, this occurs because the peer-to-peer network is imperfect, so some nodes may have heard about a transaction other node have not heard about.

[109] See article 2, n.4. of the Regulation (EU) 2022/858.

Having given an idea of what the nodes are and what tasks they perform, it is now possible to dispel doubts about the consensus protocol.

4.2.The Consensus Protocols: Trust in Algorithms?

An age-old problem that permeates not only the computer science domain and Blockchain technology but all of humanity is how a group makes *decisions.*

For what is worth in this chapter, trust and consensus are the crucial concepts of this technology. Trust can be defined as a conscious act of an individual and a foundation for economic operation and social stability. Consensus has been studied for ages in biophysics, ethics, and philosophy, and it can be described as a set of rules significant to consolidating society. The formal study of consensus in computer science started when the airline industry decided to make computers assist in flying and monitoring aircraft systems: this included monitoring altitude, speed, and fuel, as well as processes such as fly-by-wire and autopilot. This was an incredible challenge as being at such a high altitude poses many threats to the normal execution of computer programs. Therefore, dependable computer systems were first pioneered by aircraft manufacturers, who realized that introducing redundancy in their systems would have represented the key to resolving their problems. Instead of using a single computer onboard the aircraft, thus having a single point of failure, they used multiple computers onboard to distribute the points of failure.

At this point of the dissertation, one might ask: *How is the history of aircraft related to Blockchain and the problem of trust in decentralized systems?*

The link can be better understood by trying to answer another question that summarizes another critical challenge in the Blockchain environment: *How are these computers coordinated amongst each other?*

Early literature had focused on enabling the coordination of processes, where these processes could be treated on a CPU or computers in a network, given that they are separated spatially.

One of the most impactful pieces of literature during this time was "Time, Clocks, and the Ordering of Events in a Distributed System",[110] written by the computer scientist and mathematician Leslie Lamport in the late 70s. In this work, Lamport shows that two events occurring at separate physical times can be concurrent so long as they do not affect one another.

Much of the paper logically and physically defines causality – what it means for an event to happen before another. This is important because determining the order of when events occur, such as the measurement of a sensor or detection of error and subsequent error correction – as well as determining which events took place in the first place – is crucial to the correct functioning of a distributed system.

Lamport realized that causality in distributed systems was analogous to special relativity. In both, there are no notions regarding the total ordering of events that may appear to happen at different times to different observers (in the case of relativity) or processes (in the case of distributed systems).

Although this section does not intend to deepen the origin of the consensus mechanisms from a computer science perspective, it is essential to recognize that through the efforts of Lamport and other scientists, the formal study of distributed systems began to take shape. In other words, consensus attempts to create a reliable system from potentially unreliable parts – parts like the computers in aircraft that are vulnerable to bit flips due to radiation or power outages in a data centre. *It provides consistency among the many copies of the ledger.*

> Shou-Cheng Zhang said: "The history of mankind follows the logic of division and unity in turn, and Blockchain technology is taking the Internet era into such a logic.

[110] L. Lamport, *Time, Clocks, and the Ordering of Events in a Distributed System,* in *Massachusetts Computer Associates, Inc*., pp. 588-565, https://lamport.azurewebsites.net/pubs/time-clocks.pdf.

> We are now witnessing a new revolution in this era brought about by Blockchain and decentralized technology."[111]

> For De Filippi and Wright "[c]onsensus mechanisms make it possible for a distributed network of peers to record information to a Blockchain, in an orderly manner, without the need to rely on any centralized operator or middleman".[112]

To this extent, it can be even better understood that the reason why Satoshi Nakamoto produced private money was to provide "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."[113]

Thus, in its original guise, the consensus mechanism was aimed at counteracting situations where the network participants disagree on the actual state of the Blockchain.

Regulation (EU) 2022/858 defines the consensus mechanism in a straightforward and clear way as "the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated."[114]

Against this backdrop, another consideration deserves attention.

Blockchain is often compared to the Internet for being a radical and disruptive innovation. However, there are quite a few differences, even with trust.

Whereas the biggest problem of the Internet is its incapacity to address the issue of trust, Blockchain provides a solution that goes entirely beyond conventional thinking.

Blockchain trust has several essential features. First, it creates a consensus mechanism based on mutual trust without a trusted central party. It thus sets a decentralized,

[111] L. Yuming, *Sovereignty Blockchain 1.0 – Orderly Internet and Community with a Shared Future for Humanity*, Springer, 2021, p. 79.

[112] P. De Filippi, A. Wright, *Blockchain and the Law -The rule of code*, Harvard University Press, 2018, p. 42.

[113] S. Nakamoto (2008), p. 1.

[114] See Regulation (EU) 2022/858, article 2, n.3.

trustworthy system without having to trust anyone, which marks a fundamental step from centralized algorithmic credit toward decentralized credit.

Second, the consensus protocols govern how information can be added to the shared repository and how blocks are added to the chain. They also ensure that the content of each block (i.e., transactions) is consistent across the whole network so that every node has the exact version of the ledger,[115] and no block is altered. Cryptography has an essential role, as already anticipated, but it will be clarified after the following observations.

Third, the system of crypto-economic incentives – namely, the rewards at stake for solving the cryptographic puzzle - favours honest behaviours. Thus, honesty becomes the winning strategy[116] among parties in (public) Blockchain networks.

Notwithstanding, it must be recognized that this "trustless trust narrative" does not mean that human decision-making can be entirely replaced, as "humans are still needed to, for example, maintain Blockchain protocol (…)".[117]

The root issue is what the game theory theorizes as the *problem of cooperation*, meaning that every time two strangers trade, they face a dilemma of cooperating. According to Vili Lehdonvirta, this problem is conventionally solved by parties' incentives to maintain their reputation or through reliance on a trusted third party.[118] With Blockchain, this mechanism is replaced by a technical protocol.

[115] This sentence must be understood dynamically because it is often the case that two miners arrive at the solution almost simultaneously. Given the time required to propagate the information over the network, each of the two nodes will initially add its own block to the chain and send the information to neighbouring nodes, which will use the new chain as a basis to add other blocks. At some point, it will be necessary to decide which, between the two chains, is the 'real' one, and this is where the consensus rule in Bitcoin comes into play: the longer chain wins because it requires more work.

[116] K. Werbach, *Blockchain and the New Architecture of Trust*, MIT Press, 2019, p. 100.

[117] M. Finck (2018), p. 12.

[118] V. Lehdonvirta, *The Blockchain Paradox: why distributed ledger technologies may do a little to transform the economy,* Oxford Internet Institute, 2016, https://www.oii.ox.ac.uk/news-events/news/the-Blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/.

This idea explains why, for some commentators, Blockchain is not seen as a technology but rather as an *ideology,*[119] promoting a world without institutions where people trust cryptography more than their human peers. As we will discuss at length in the following chapter, Cryptopunks share those views.

All things said: how do nodes ultimately reach a consensus on a block?

At regular intervals, every node in the system proposes its outstanding transaction pool to be the next block. Then the nodes act according to the chosen consensus protocol, where each node's input is its proposed block. In this scenario, some nodes may be malicious and put invalid transactions into their blocks, but it is possible to assume that other nodes will be honest. If the consensus protocol succeeds, a valid block will be selected as the output. Some valid outstanding transactions may not be included in the block, but this is not a problem. If some transaction did not make it into a specific block, it could wait and get into the next block.

A digital signature based on asymmetric encryption (public and private keys) is generally applied to verify the authentication of the transactions.[120] This peculiar aspect will be further detailed in the paragraph dedicated to the security-enhancing feature of Blockchain.

Different consensus protocols can be distinguished, proof-of-work and proof-of-stake being the most known.

In proof-of-work (PoW) based Blockchains, such as the one used for the Bitcoin network, the mining nodes compete to add the following block by solving a

[119] T. Schrepel, *Blockchain: from ideology to implementation,* in *Blockchain + Antitrust,* 2021, pp. 2–17; G. S. Brekhov, *Crypto-Anarchism: The Ideology of Blockchain Technologies,* in *RUDN Journal of Political Science, 2022,* pp. 393–407; O. Korhonen, J. Rantala, *Blockchain governance challenges: Beyond libertarianism,* in *AJIL Unbound, 2021,* pp. 408–412; T. Corballis, M. Soar, *Utopia of abstraction: Digital organizations and the promise of sovereignty,* in *Big Data and Society*, 2022.

[120] G.J. Simmons, *Symmetric and asymmetric encryption,* in *Secure Communications and Asymmetric Cryptosystems,* Taylor and Francis, 2019, pp. 241–298; M. Kaushal, *Cryptography: A Brief Review,* in *International Journal for Research in Applied Science and Engineering Technology*, 10(2), 2022, pp. 763–767.

cryptographically complex calculus that requires high computational power and electric power energy. Due to the high energy consumption of mining, many environmental activists have railed against Blockchain[121] and the EU Blockchain Observatory and Forum recently published a report entitled "PoW Energy Consumption in EU".[122]

In the proof-of-stake (PoS) mechanism, the factor determining which node will add to the next block is the node's stake, namely the amount of cryptocurrency invested to participate in the creation of new blocks: thus, if node A has invested ten times the amount invested by B, A will have ten times the probability of B to be selected.

For now,[123] examples of Blockchains using the proof-of-stake protocol include Polkadot, Avalanche, Cardano, Nxt, and Blackcoin.[124] Ethereum, designed initially as a proof-of-work Blockchain, recently transitioned to a proof-of-stake Blockchain called Ethereum 2.0.[125]

4.3.Cryptography as a Key Feature

This section will briefly introduce the cryptographic apparatus of Blockchain, thus preparing the ground for the analysis of Blockchain's implications for data protection law. Many of the concepts covered here will be taken up and explored in greater detail

[121] K. Mohsin, *Cryptocurrency & Its Impact on Environment*, in *International Journal of Cryptocurrency Research*, 2021, pp. 1-4; N. Sapkota, K. Grobys, *Blockchain Consensus Protocols, Energy Consumption and Cryptocurrency Prices,* in *Journal of Energy Markets*, Vol.13, No.4, 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778604; C. Gola, J. Sedlmeir, *Addressing the Sustainability of Distributed Ledger Technology,* Bank of Italy Occasional Paper No. 670, 2022, available at SSRN: https://ssrn.com/abstract=4032837 or http://dx.doi.org/10.2139/ssrn.4032837.

[122] European Blockchain Observatory and Forum (EUBOF), *PoW Energy Consumption in EU*, 1 November 2022, available at https://www.euBlockchainforum.eu/sites/default/files/reports/PoW%20EnergyConsumptionReport.pdf.

[123] Updated to September 2023.

[124] For an updated list, cfr. https://cryptoslate.com/cryptos/proof-of-stake/

[125] From the Ethereum website: "Proof-of-stake (PoS) underlies Ethereum's consensus mechanism. Ethereum switched on its proof-of-stake mechanism in 2022 because it is more secure, less energy-intensive, and better for implementing new scaling solutions compared to the previous proof-of-work architecture."

in the following. Our research has revealed that using alternative data encryption[126] may be one of the solutions to ensure a balance between Blockchain and data protection law.

Although we will focus only on aspects relevant to the subsequent analysis of the implications for data protection law, we will maintain the point of view of computer science. The in-depth analysis of the cryptographic tools will be left to Chapter III, which is dedicated to testing whether the GDPR can hold steady in the Blockchain environment.

We already clarified that the name Blockchain derives from its structure: it is a chain of blocks. Every block contains a heading and a batch of valid transactions that are hashed and encoded into a Merkle Tree. In short, a Merkle Tree is a way of structuring data that allows a large body of information to be verified for accuracy efficiently and quickly. The Merkle Tree is crucial for Blockchain's security since it makes using as little data as possible when processing and verifying transactions feasible. The block is then time-stamped and secured by a hashing process.

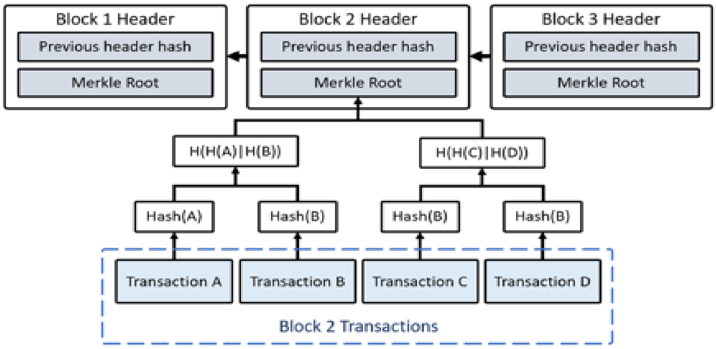


Figure 4. The architecture of the Merkle tree in the Blockchain (Chen et al., 2019).

At the outset, it must be pointed out that cryptography is the foundation of the technology, as it is Blockchain's distinctive architectural element that makes it

[126] A clarification is needed: cryptography defines the method of securing a message using encryption and decryption methods. Encryption is the application of cryptography.

immutable.[127] Two cryptographic tools are essential in Blockchains: the hash function and the public key infrastructure (PKI).

A hash can be defined as a digital fingerprint to serve as an identifier for anything digital. Essentially, it is the combination of characters of fixed length assigned to a dataset of any size. The chain's integrity is guaranteed since every block links together and incorporates the previous block's hash. This means that there will never happen to see different datasets with the same hash and run the hash functions backwards to find the piece of information based on the string of numbers.

A hash is unique and unidirectional; it cannot be reversed. Since data is chronologically ordered, making it difficult to tamper with information without altering the following blocks if a transaction is an error, a new transaction must be used to reverse the mistake, and both transactions would be visible. Also, if someone changes the information in a block, the hash of this block will be different from the previous and, therefore, the mismatch will be evident.

Because every block is linked in a specific sequence, such an action will only be accepted with a majority of consensus.

The characteristics of non-repudiation and non-forgeability guarantee a unique and historical version of the records that can be agreed upon and shared among all participants in a particular network.[128]

Tamper evidence is often considered the Blockchain's value proposition. It is indeed the basic concept of data distribution among all participants in a network, and the impossibility of making changes leads to several problems because of data protection regulation. For instance, it seems impossible to update or delete personal data stored on a Blockchain (whether necessary). This means that, Blockchain's append-only

[127] "One reason that Blockchain-based systems are effective in creating distributed trust is that instead of law, they rely on cryptography and can avoid such problematic legal oversight.", see Werbach (2018), p. 220.

[128] S. Nascimento et al. (2019), cit., p.16.

structure seems to burden compliance with data protection requirements, for instance, concerning the application of the right to be forgotten and the right to rectification. Nonetheless, as it will be observed, those points of tension can be mitigated by acting at both the infrastructure and application levels.

Returning to this section's subject, the other fundamental cryptographic instrument in the Blockchain is the public key infrastructure (PKI), which enables participants to sign transactions digitally while remaining pseudonymous.[129]
This is possible because Blockchains rely on a two-step verification process with asymmetric encryption. Every participant is provided with a pair of keys, mathematically related one to another: the public and private keys (both are a string of letters or numbers representing the user). The public key is an account number; the private key is a password usually randomly generated,[130] known only by its owner and used to create a digital signature through an algorithm.[131]
The mathematical relationship between these keys allows the private key to sign the transaction virtually. It means that once the transaction is digitally signed, a counterpart of a transaction can use the sender's public key to verify that the owner

[129] J. Bacon et al, *Blockchain Demystified*, Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017, p.4, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218.

[130] "The way you create your private key though is super important. You would never choose the number 1 as your private key. That's too dangerous! Anyone, using the same mathematical functions, can infer a bitcoin address from a private key. And if that bitcoin address owns coins, they can easily be stolen. In fact, if you run a script that tries every number (private key), counting from the number 1 to 100,000, you will find (in some seconds) dozens of usable bitcoin addresses! In order to find if an address is usable (an address owning some coins in the bitcoin network), one has to iterate through the entire Blockchain and if a reference to that account is found, Boom! One can steal all the coins from it using that weakly generated number (private key). In fact, the bitcoin address derived from the private key number 1 is usable: 1EHNa6Q4Jz2uvNExL497mE43ikXhwF6kZm.", A. Lymbouras, *Shallow Dive Into Bitcoin's Blockchain Part 2 – Transactions*, https://towardsdatascience.com/a-shallow-dive-into-bitcoins-Blockchain-part-2-transactions-d4ee83067bae.

[131] "The private key is imported into the wallet to guarantee the security and authentication of the cryptocurrencies. If the private key is lost or stolen, it cannot be recovered, which means that the user cannot access the wallet with any other alternative means and that his cryptocurrencies in the wallet are unavailable.", N. Gupta, *Security and Privacy Issues of Blockchain Technology*, in K. Shiko, C.D. Ganesh (eds), *Advanced application of Blockchain Technology*, Springer, 2020, p. 214.

of the pair made it.[132] Thus, other users can prove that the owner of that specific public key performed a transaction, but they cannot trace the public key back to the private one. As a consequence, a party's identity is unknown when digital signatures are used. However, many commentators argued that the physical identity hiding behind the public address might be hypothetically unveiled if matched with additional information, given that identities on a Blockchain are pseudonymous.

In the following chapters, we will significantly investigate the nature of public keys. Yet, before dealing with that question, evaluating whether the pieces of information injected in the Blockchain by users qualify as personal data will be necessary.[133] Furthermore, it will be paramount to preliminarily clarify the difference between anonymization and pseudonymization from the data law perspective.[134]

4.4.Types of Blockchains

It is valuable to consider that Blockchain is not a singular technology with a predefined set of features but a class of technologies.[135]

Therefore, from a technical and functional point of view and based on its internal governance structure – namely, the process of maintaining the software - the Blockchain can be deployed in an infinite variety of configurations.[136]

In light of that, it is crucial for the following analysis of the data protection implications of Blockchain to differentiate between the different types of Blockchains.

[132] The public key is generated from the private key by applying one-way algorithms (e.g. elliptic curve cryptography). This means that it is possible to derive a public key from a private key, but it is not possible to derive the private key from the public key.

[133] Cfr. Chapter III, para 3.2.

[134] Cfr. Chapter III, para 3.1., 3.1.1.

[135] R. Beck, C. Muller-Bloch, J. King, *Governance in the Blockchain Economy: A Framework and Research Agenda*, 2018, https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda.

[136] S. Zeba, P. Suman, K. Tyagi, *Types of Blockchain*, in *Distributed Computing to Blockchain: Architecture, Technology, and Applications*, pp. 55–68.

There is a clear-cut diversity concerning software management, the visibility of transactions on the ledger and the right to write on the ledger (that is, the right to add new data).

Ordinarily, Blockchains are grouped into two categories depending on the openness of the infrastructure (public/private Blockchains) and the ways of validating the transactions (permissionless/permissioned). Among them, some points of intersection may exist. As a result, if a Blockchain is public, it is open to everyone and relies on open-source software; anyone can join the network by simply downloading and running the relevant software.[137]

A Blockchain is permissionless if there are no (formal) restrictions on participating in the network - since no central authority (nor an administration) grants permission to actors wanting to maintain a node.

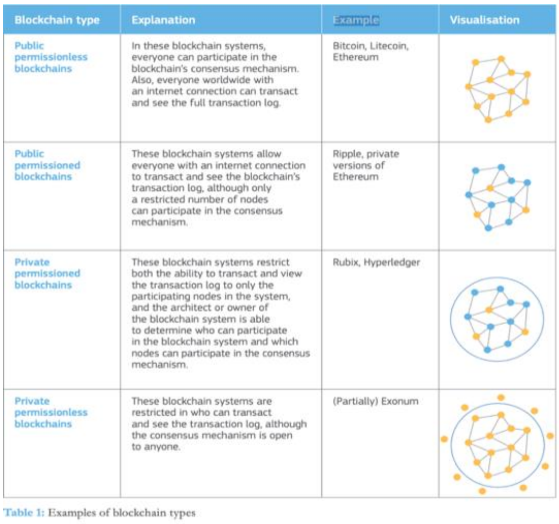
A public Blockchain can be both permissionless and permissioned. An example of public and permissioned Blockchain was represented by Diem, a project of Facebook which never saw the light.[138] As presented by the creators, it would have been a Blockchain open to everyone, but where companies selected by Facebook would have validated transactions.

If prior authorization is necessary to join the network, a Blockchain is private; therefore, it is usually also permissioned, given that someone must grant permission to join the network and validate transactions. This means that a limited number of nodes needs to be set up in the network, and the parties' identity is usually known (at least to the administrator). These types of Blockchains are generally designed for a specific purpose.[139]

[137] Bitcoin and Ethereum represent concrete examples.

[138] https://www.diem.com/en-us/updates/stuart-levey-statement-diem-asset-sale/.

[139] Successful examples of this prototype are Hyperledger by IBM, https://www.hyperledger.org/, and R3 a DLT by Corda created for financial purposes, https://www.corda.net/.



Blockchain type	Explanation	Example	Visualisation
Public permissionless blockchains	In these blockchain systems, everyone can participate in the blockchain's consensus mechanism. Also, everyone worldwide with an internet connection can transact and see the full transaction log.	Bitcoin, Litecoin, Ethereum	
Public permissioned blockchains	These blockchain systems allow everyone with an internet connection to transact and see the blockchain's transaction log, although only a restricted number of nodes can participate in the consensus mechanism.	Ripple, private versions of Ethereum	
Private permissioned blockchains	These blockchain systems restrict both the ability to transact and view the transaction log to only the participating nodes in the system, and the architect or owner of the blockchain system is able to determine who can participate in the blockchain system and which nodes can participate in the consensus mechanism.	Rubix, Hyperledger	
Private permissionless blockchains	These blockchain systems are restricted in who can transact and see the transaction log, although the consensus mechanism is open to anyone.	(Partially) Exonum	

Table 1: Examples of blockchain types

Figure 4. Example of Blockchain types (Nascimento et al., 2019).

The dichotomy between public and private Blockchains is fundamental from a legal standpoint. However, they also present significant technological differences: public Blockchains are revolutionary, but their economic effects may be limited; on the contrary, private Blockchains are technically less innovative but may have relevant economic effects.

At this juncture, it is worth clarifying that while there may be occasional mentions of private Blockchains, [140] the primary emphasis of this study will be on public Blockchains. This choice is driven by a clear rationale: the legal challenges posed by public Blockchains, particularly in the realm of data protection, are indisputable and must be addressed due to their central role in the overall scope of this thesis.
Additionally, although we still need to deepen the relationship between the technology and the data protection law, it is perhaps already evident that applying the requirements of the European regulation could be less challenging in

[140] In the author's own words: "it is private Blockchains that most demand legal attention […] since it's only in them, differently from public Blockchains, that there is room for rational and renewable negotiation of operating rules such as consensus protocols.", J. W. Ibanez Jiménez, *Blockchain: Primeras cuestiones en el ordenamiento español*, Dikinson, 2018, pp. 30-31.

permissioned Blockchain than in permissionless. Therefore, both types of Blockchain will be tackled during the research.

5. Blockchain Use Case's Structure: An Overview

As described above, Blockchain was born with cryptocurrencies but is now being used in many other fields due to its peculiarity of "offer[ing] the potential to simplify and make more secure any process that needs to record and verify the information."[141] Blockchain technology can implement other decentralized services besides currency transactions where trust is built based on intrinsic Blockchain properties.
It has been unequivocal since its launch that Blockchain's full potential was likely to be expressed outside the financial sector.[142]

The capability of Blockchain has been studied in a wide range of fields like smart property, traceability of products along the supply chain, international payments, know your customer (KYC), property, ownership, rights management, identity management, digital identity,[143] electronic voting, verified customer reviews, tokenized incentive economies, derivates markets, sustainability, crowdfunding, trade financing. This is not an exhaustive list of (in some cases, potential) use cases, [144] which is just intended to give an overview of the broad spectrum of likely use cases.

[141] European Commission, *Blockchain in practice – Promoting Blockchain and DLTs in European SMEs*, June 2021, p. 6.

[142] "People are looking at Blockchain technology to disrupt most industries, including automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel. While Blockchain is definitely not the solution for every problem, smart contract automation and disintermediation enable reduced costs, lower risks of errors and fraud and drastically improved speed and experience in many processes.", see European Blockchain Observatory and Forum, p.93.

[143] Cfr. Chapter IV of this thesis.

[144] V. Dieterich, M. Ivanovic, T. Meier, S. Zäpfel, M. Utz, P. Sandner, *Application of Blockchain technology in the manufacturing industry,* Working Paper, Frankfurt School Blockchain Center, 2017; D. Tapscott, A. Tapscott, Blockchain revolution: *How the technology behind bitcoin is changing money, business, and the world,* New York: Penguin, 2016; D. Leonard, H. Treiblmaier, *Can cryptocurrencies help to pave the way to a more sustainable economy? Questioning the economic growth paradigm*, in H. Treiblmaier, R. Beck (Eds.), *Business transformation through Blockchain*—Volume I, Cham, Switzerland: Palgrave Macmillan, 2019; H. Treiblmaier, U. Umlauff, *Blockchain and the future of work: A self-determination theory approach*, in M. Swan,

With the aim to providing some order to the topic, we can argue[145] that three categories of use cases can be identified.

The first one includes the financial system; it covers cryptocurrencies, tokens, Initial Coin Offerings (ICOs), insurance, payment systems and supported financial liabilities.

The second category comprises the industry, trade and market sectors, involving trade and supply chains, manufacturing, energy systems, digital content, health and biopharmaceuticals.

The third category includes the public sector: identity management, certificates and accreditation, land and property transactions (e-notaries), allocation of public benefits and intellectual property rights.

The European Commission is working on several initiatives to unite and enhance Europe's leading role in Blockchain technology. In this respect, the European Blockchain Service Infrastructure (EBSI), the world's first cross-border Blockchain initiative in public administration, represents a significant development.[146] It constitutes a crucial part of the European Blockchain's Strategy for Blockchain designed to meet "gold standards" goals. Data protection is one of them, given that "Blockchain technology should be compatible with, and where possible support, Europe's strong data protection and privacy regulations."[147]

EBSI has focused on a small set of use cases: notarization, diplomas, trusted data sharing and European Digital Identity. We will return to this subject in the following. In particular, this research will extensively focus on Blockchain-based identity management as a use case representing an example of enhanced data governance.

J. Potts, S. Takagi, P. Tasca, F. Witte (Eds.), *Blockchain economics: Implications of distributed ledger technology,* New Jersey, 2019, pp. 105-124.

[145] This taxonomy results from analyzing the use cases currently deployed in the industry and those under consideration by the European Blockchain Service Infrastructure (EBSI).

[146] https://digital-strategy.ec.europa.eu/en/policies/european-Blockchain-services-infrastructure.

[147] https://digital-strategy.ec.europa.eu/en/policies/Blockchain-strategy.

Moreover, analyzing this specific use case will help us demonstrate that Blockchain can be equated to a privacy-enhancing technology for some of its peculiarities.

To conclude this brief overview, a point of clarification is needed: such variegated applications and use cases are possible because the Blockchain's infrastructure can host at the same time a so-called accounting system, which is a method for data storage, and a programmable platform enabling new applications, including smart contracts which will be the focus of the following section.

Blockchain-based applications are the core of the new concept of Web 3.0, also known as Semantic Web[148] or read-write execute. These programs are recognized as decentralized apps (DApps)[149] and are projected to move towards a global internet characterized by the absence of centralized control points where the users can supervise their data. They are basically "smart contracts, or a set of smart contracts, which interact with an off-chain interface to enable applications which users can access, usually through a browser-based interface."[150]

5.1.Smart Contracts

One of the most important applications of Blockchain is smart contracts,[151] of which there is no univocal definition.

[148] A. Patel, S. Jain, *Present and future of semantic web technologies: a research statement,* in *International Journal of Computers and Applications*, 43(5), 2021, pp. 413-422.

[149] Cfr. A. Bogner, M. Chanson, A. Meeuw, *A decentralised sharing app running a smart contract on the Ethereum Blockchain,* in *ACM International Conference Proceeding Series,* 2016, pp. 177–178; S. Nikhil Panday, A. Saini, N. Gupta, *Instigating Decentralized Apps with Smart Contracts,* in *Proceedings - IEEE International Conference on Advances in Computing, Communication and Applied Informatics,* 2022.

[150] J. van der Laan, *Understanding Blockchain,* in M. Aztzt, T. Richter (eds), *Handbook of Blockchain Law: a guide to understanding and resolving the legal challenges of the Blockchain technology,* Kluwer Law International, 2022, p. 29.

[151] Z. Zheng et al, *An overview on smart contracts: Challenges, advances and platforms*, in *Future Generation Computer Systems,* 2020, pp. 475-491.

De Filippi and Wright represent them as "digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without human intervention."[152]

Smart contracts were defined for the first time in 1994 by Nick Szabo, who described them as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[153]

Nonetheless, the real game changer for smart contracts came with the advent of Blockchain. In particular, the achievement of distributed consent led to new discussions on using smart contracts to enforce agreements between individuals without a third party. The peculiarity of smart contracts is that these agreements can be recorded and validated into a Blockchain, which can then automatically execute and enforce the contract. Smart contracts usually work under if-then instructions. This means that the system is self-executing when the previously specified conditions are met by agreement between the parties. For instance, 'if' something happens – if you pay for a car and short-term insurance – 'then' specific transactions or actions will be carried out – the car door unlocks, and the payment is transferred.

It is necessary to clarify that algorithmic contracts are not novel and that what distinguishes smart contracts from past digital contracts is automated execution.

Nevertheless, while automated execution can exist in other systems, none can prevent the contract's execution. Therefore, both automation and enforceability are the main characteristics of smart contracts.

Furthermore, although smart contracts run on a Blockchain, they are not immutable in their effects, which a second transaction could undo with this specific purpose.

> "[W]ith a smart contract, complete execution of the agreement, including any transfer of value, occurs without any such opportunity to interrupt. Accordingly, juridical forums are powerless to stop the execution of smart contracts – there is no room to bring an action for

[152] A. Wright, P. De Filippi (2015).

[153] N. Szabo, *Smart Contracts: Building blocks for digital markets*, 1996, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

breach when breach is impossible. The computers in the Blockchain network ensure performance, rather than any appendage of the state. And, because Blockchains run on a distributed network of independent nodes, with no central control point, a litigant seeking to enjoin performance of a smart contract has no one to sue.

[…] The distinctive aspect of smart contracts is not that they make enforcement easier, it is that they make enforcement unavoidable.

[…] The contract is the scripting code."[154]

Garcia Mexia and Morales Barroso stated, "[t]he smart contract created in this way not only defines the terms and conditions around an agreement, *in the same way as a traditional contract does*, but also controls the fulfilment of those obligations automatically."[155]

Some even argue this is a misnomer [156] as smart contracts are neither 'smart'[157] nor 'contract'.[158] They cannot understand the contractual terms of agreements nor independently verify whether an execution-pertinent event occurred.

Smart contracts would only apply under limited and strictly circumscribed conditions, such as when there is no need for dispute resolution or when reliable data from outside, often referred to as 'Oracles',[159] provides accurate information.

[154] K. Werbach, N. Cornell, *Contracts ex machina,* in *Duke Law Journal*, 2017, pp. 331-332; 348; 349.

[155] Emphasis added. See P. Garcia Mexia, J. Morales Barroso, *Cryptoregulation in a nutshell*, Wolters Kluwer, 2020, p. 57.

[156] C.L. Reyes, *Emerging Technology's Language Wars: Smart Contracts*, in *Wisconsin Law Review*, 2022, pp. 85-113.

[157] T. Schrepel has a different opinion: "Contrary to common wisdom, that definition of "smart" seems about right. The word "smart" comes from the Latin "intelligere," which means "to choose between." Because smart contracts automate the choice according to pre-defined conditions, they are "smart" in the in the term's original meaning.", see *Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach*, Study for the European Commission, p. 16, https://digital-strategy.ec.europa.eu/en/library/smart-contracts-and-digital-single-market-through-lens-law-plus-technology-approach.

[158] See for example X. Xu et al., *Architecture for Blockchain Applications*, Springer Nature Switzerland, 2019, p. 7: "These are often called 'smart contracts', although the programs are typically not very smart and are often not related to legal contracts".

[159] For an analysis of how the reliability of oracles mechanisms can affect the overall reliability of a Blockchain-based system, see Lo S. et al, *Reliability analysis for Blockchain oracles,* in *Computers and Electrical Engineering,* in 2020, p. 83. Cfr. also G. Caldarelli, *Real-world Blockchain applications under the lens of the oracle problem. A systematic literature review*, in *Proceedings of the 2020 IEEE International*

Finally, they are not legal contracts per se, as they do not have underlying legal or contractual provisions,[160] but they are computer codes that can produce legal effects.

Smart contracts are claimed to be unique because they remove the inherent ambiguity of natural language; therefore, they cannot match the enforcement discretion typical of legal contracts. This means that some terms such as 'good faith' or 'best efforts' cannot find a place in the programming language of smart contracts, thus pinpointing that some changes to the current legal framework might be necessary to meet the new requirements of the digital age.

As Werbach affirmed: "Law is not just a set of rules on a page. It is a dynamic enterprise with a complex and varied toolkit. New challenges call for new mechanisms of legal activity."[161]

If this proves to be true, Blockchain and smart contracts will not necessarily entail a radical, disruptive and swift revision of the entire legal ecosystem, yet "[they] will stimulate innovative solutions to make law operate more consistently with governance through software code."[162]

Regarding the current state of play of smart contracts, it is worth specifying that not all Blockchains allow for programming them. More precisely, the Bitcoin Blockchain does not support smart contracts. Conversely, Ethereum was explicitly implemented to be written in a 'Turing complete' language, which can perform any computation. It is, in fact, a "programmable Blockchain", which is a Blockchain that does not limit itself to providing predefined and standardized operations but also allows users to create new operations.

Conference on Technology Management, Operations and Decisions, ICTMOD 2020, 2020, pp. 1–6; S. K. Ezzat, Y. N.M. Saleh, A. A. Abdel-Hamid, *Blockchain Oracles: State-of-the-art and research directions*, in *IEEE Access*, 2022, pp. 1-19.

[160] M. Orcutt, *States that are passing laws to govern "smart contracts" have no idea what they're doing*, 29 March 2018, https://www.technologyreview.com/2018/03/29/144200/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/.

[161] K. Werbach (2019), p. 202.

[162] *Ibidem.*

Substantially, many Blockchain applications - for instance, the above-mentioned decentralized applications - are only possible due to smart contract capability.

6. Conclusion

The previous discussion has illustrated some of the essential technical components of Blockchain technology, which will be retraced in the following chapters focused on the law and governance issues [163] of Blockchains.

Blockchain has emerged as a disruptive way of executing business processes[164] in decentralized systems,[165] and it has become apparent that all the developments referenced thus far have taken place with little or no input from the legal community. The broad interest in this technology suggests the need for new models as it opens a new way of thinking about the interplay between technology and law and poses significant governance challenges.

The European Union is aware of that, as testified by the holistic approach adopted by the Commission, which has repeatedly declared that it intends to position Europe at the forefront of the innovation brought about by distributed systems.

The analysis developed in the following will only consider the European legal framework and the approach of the European legislator, which will be carefully analyzed to understand whether, considering the development of the technology and the legal issues raised, the attitude mentioned above can be considered the most suitable.

[163] A. Zwitter, J. Hazenberg, *Decentralized Network Governance: Blockchain Technology and the Future of Regulation,* in *Frontiers in Blockchain*, 2020, p. 3 ss.

[164] Y. Chen, C. Bellavitis, *Blockchain disruption and decentralized finance: The rise of decentralized business models,* in *Journal of Business Venturing Insights*, 2020, p. 13 ss.

[165] L. Qiao, S. Dang, B. Shihada, M.S. Alouini, R. Nowak., Z. Lv, *Can Blockchain link the future?,* in *Digital Communications and Networks*, 2022, pp. 687-694.

The European legislator has only recently taken a few steps towards regulating the technology in relation to the financial sector.[166] However, despite some cross-references to these laws, our focus remains to evaluate the state of the art to understand how to guarantee the respect of the right to data protection without stifling the technology.

[166] See section 2.1 of this chapter.

Chapter II

Regulating Blockchain: Much Farther to Go?

" [The code] will present the greatest threat to both liberal and libertarian ideals, as well as their greatest promise. We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building. Code is never found; it is only ever made, and only ever made by us."

Lawrence Lessig [167]

1. Introduction – **1.1.** Defining the connotation of the law - **2.** The interplay between technology and law – **2.1.** A stroll around the Principality of Sealand - **3.** Applying the "Code as law" model to Blockchain – **4.** The paradigm of Cryptoregulation: regulating Blockchain – **4.1.** Can Traditional legislative techniques fashion Blockchain? - **4.2.** Blockchain governance and the debate around off-chain vs on-chain rules – **4.3.** Where do we stand in the European Union? – **4.4.** Does Blockchain technology have what it takes to self-regulate? – **4.5.** Unity is strength: the multistakeholder co-regulation approach – **5.** Blockchain the regulator - **6.** What does the future hold for Blockchain?

1. Introduction

The preceding chapter presented Blockchain in its technical features. That premise was crucial to pinpoint why some authors even consider that Blockchain-based[168]

[167] L. Lessig, *Code,* Basic Book, 2006.

[168] See, for instance: D. Zhao, *Application and Development Trend of Blockchain in the Financial Field*, in *Advances in Intelligent Systems and Computing*, Springer, 2021, pp. 558–564; W. Cai, Z. Wang, J.B. Ernst, Z. Hong, C. Feng, V. C. M. Leung, *Decentralized Applications: The Blockchain-Empowered Software System,* in *IEEE Access*, 2018, pp. 53019–53033; P. V. Kakarlapudi, Q. H. Mahmoud, *Design and development of a Blockchain-based system for private data management*, in *Electronics*, 2021, pp. 1-22.

applications might come to disrupt[169] the basis of modern legal systems[170] and build 'new private regulatory frameworks.'[171] In recent times, the word 'disruption' has often been used to describe technology's impact and influence on the law and on almost every field.[172]

Although the technology is still developing,[173] it has gained momentum. Many commentators define it as a tool to redefine socio-economic systems[174]

[169] See K. Tranter, *Disruptive technology disruptive law,* in *Law, Culture and the Humanities*, 2021, Vol. 17(2), pp. 158–170. For an interesting parenthesis about the origin of what he defined 'the disruption frame', see p. 160: *"The idea that technology "disrupts" has its origins in Harvard Business School's Clayton Christensen's 1997 The Innovator's Dilemma. In that book Christensen looks at how firms develop products and how decisions to incrementally innovate and improve existing products for existing clients has led to the decline of specific firms. His insight is that established firms fail to develop radically new products for new customers; while new products tend to be developed outside of established market players. He suggests that by the time the new product is gaining market share it is too late in the cycle for the established firm to respond. Within Christensen's initial context the idea of "disruptive technology" was not tied to the digital; with only one of his case studies on disk-drives manufacturing and innovation over the 1970s–1990s relating to information and communication technologies. Further, Christensen's original use of "technologies" was misleading."*
Likewise, Tranter said, " *(…) the disruption frame offers a less than ideal matrix through which to think law and technology. The focus on a "disruptive technology" tends to result in analysis that has two limitations. The first is a narrowing of the temporal focus. Disruption establishes an anxious present that has no understanding of its past and a cloudy conception of its future. The second is that this presentism tends to result in a reaffirmation of the tools and techniques of modern law to manage disruption. Disruption sets up an urgent law reform agenda of fixing the law so as to catch-up with the feared consequences of technological change."* p. 171.

[170] M. Abramowicz, *Cryptocurrency-Based Law,* in *Arizona Law Review,* 2016, p. 35.

[171] O. Pollicino, G. De Gregorio, *Blockchain and Public Law: An introduction,* in O. Pollicino, G. De Gregorio (eds), *Blockchain and Public Law,* Edward Elgar, 2022, p. 2.

[172] European Investment Bank, *Artificial intelligence, Blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy,* June 2021, https://www.eib.org/attachments/thematic/artificial_intelligence_Blockchain_and_the_future_of_europe_report_en.pdf. Furthermore, some AI experts warned about the risks of AI, which according to them could even lead to extinction, see https://www.bbc.com/news/uk-65746524 (last accessed 10 August 2023).

[173] A. Bardhan, *Recent Developments in Blockchain,* in *Journal of University of Shanghai for Science and Technology*, 2021, pp. 1487–1498; M. Maslin, M. Watt, C. Yong, *Research methodologies to support the development of Blockchain standards*, in *Journal of ICT Standardization*, 2019, pp. 249–268.

[174] "Blockchain has attracted substantial hype in recent years. In one sense, it could join the queue of technological innovations in human history that have altered existing economic, political, and social structures.", M. Zou, *Code: and other laws of Blockchain,* *https://ora.ox.ac.uk/objects/uuid:7af6d923-07fa-4eb6-8340-e05205f7b4ee/download_file?file_format=pdf&safe_filename=Zou_2020_Code_laws_Blockchain.pdf&type_of_work=Journal+article*; see also M. Pisa, M. Juden, *Blockchain and Economic Development: Hype vs Reality,* in *Center for Global Development, CGD Policy* (107), 2017, pp. 1–49.

or as a solution to ‘virtually every human problem in existence’.[175]

A stable and predictable legal regime is crucial for the technology to constitute a good value proposition for businesses and even more so for consumers.

Hence, while use cases continue to take shape, multiple legal questions on the interplay between the law and this new class of technologies have started arising.

Many of those queries precisely concern the possibility of regulating the technology, which was initially designed to be censorship resistant.[176]

At first sight, code and law are divergent: broadly speaking, the rule is general, while the code is specific. Notwithstanding, more and more mutual influences can be noticed.[177] On the one hand, the software has been assuming a normative dimension as it regulates the actions of those who interact with it; on the other, the law has been carrying the feature of code in the form of ‘legal codification’ which has started a new era in the digital evolution.

Against this backdrop, Blockchain could play an important role, considering it has enormous potential as a regulatory technology for two main reasons.

First, Blockchain protocols can be built upon their developers’ normative choice and, therefore, create an ecosystem that may reflect the laws in force or require creating and adopting new rules.

[175] A. Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains,* in P. Hacker, I. Lianos, G. Dimitropoulos, S. Eich (eds), *Regulating Blockchain. Techno-Social and Legal Challenges,* Oxford University Press, 2019.

[176] This characteristic has two implications. First, any party wishing to transact on the network can do so as long as they follow the network protocol rules; second, it prevents any party from altering transactions on the web.

[177] “The digital is disrupting law, but not because cars are becoming self-driving robots rendering some provisions of the existing traffic rules ludicrous. Law as a material practice is a system of information management; and modern law at essence can be characterized as a material practice of information management that uses paper and humans. The digital with its features of speed, rigidity and automation fundamentally challenges – disrupts, even – the features and manifestations of modern law. The disruption frame is problematic for law and technology because it disguises the very real, and given the rigid ossification of code, the very urgent task of determining what values, processes and structures should be built into the emerging architecture of digital law.”, K. Tranter (2021), p.171.

Second, as already discussed,[178] Blockchain allows the deployment of smart contracts[179] designed to be self-enforcing.

The regulatory potential of Blockchain technology and the impact of legal codification will be unfolded in the following.

We must clarify why we need regulations to delineate the research's boundaries. It is impossible to summarize the process and development behind the regulating activity or settle on a single theory. For our purposes, it is sufficient to recall that the law has been established to guarantee non-violent coexistence within the human community, as resumed by the famous Latin maxim *"Ubi homo, ibi societas. Ubi societas, ibi jus. Ergo ubi homo, ibi jus."*[180]

For this research, it is worth recalling that, according to Robert Baldwin and others, the authors of 'Understanding Regulation',[181] there are three types of regulation:

- a specific set of commands: "set of rules to be applied by a body devoted to this purpose";
- an exercise of particular influence on business and social behavior;
- all forms of social or economic impact.

Besides defining what type of regulation is necessary, another crucial aspect is regulatory enforcement, which is the power with which laws bind people or behaviors and which lies with public authorities.

These general observations are the starting point for figuring out which specific questions need to be addressed and, after that, hypothetical practical solutions.

[178] See Chapter I, para 5.1.

[179] A. Stazi, *Smart Contracts: Elements, Pathologies and Remedies*, in J. Loo, N. Remolina Leon (eds), *Law and Change: An Asian Perspective*, SMU, 2022.

[180] A possible translation is: "where there is humanity, there is society. Where there is society, there is the law. Therefore, where there is the law, there is humanity."

[181] R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2013, p. 3.

First and foremost, the discussion about Blockchain and law could be preliminarily framed in two questions: *Can* Blockchain be subject to legal oversight? If yes, *should* it?

Accordingly, this chapter will table the following questions: *to what extent will Blockchain transform certain areas of law? Should traditional legal systems be adapted to the new reality resulting from Blockchain? Or should an* ad hoc *legal system be created? Should the technology be generally regulated, focusing on the code, or should the regulation be directed to specific use cases?*

This set of questions proves that this thesis refuses the idea that Blockchain and regulation are two parallel lines that will never meet[182] or that the relationship between code and law is one-way[183] where the code is an active part, and the law is an inanimate item, as the supporters of the Utopian movement claimed.

In any event, while supposing the substantial differences between the legal order and the technology, these two quite different systems for governing interactions between strangers are likely to interact.[184]

> *"It is imperative that law and regulation do not continue to underestimate the pace of change wrought by Blockchain or the desire of its stakeholders and the ecosystem they constitute."*[185]

Within the described setting, this chapter aims neither to draft a European law of Blockchain technology nor to conduct a thorough investigation of the technology from

[182] J. E. Cohen, *Between Truth and Power - The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019; J. Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, *University of Cincinnati Law Review*, 1997, pp. 177-205; J. E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, in *Stanford Law Review*, 2000, pp. 1373-1438; J. E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, in *Connecticut Law Review*, 1996, p. 981 ss; Q. S. Mulford, *Utopian Thought and Technology,* in *American Journal of Political Science*, 1971, pp. pp. 1921e ss.

[183] J. Schradie, *The Revolution that Wasn't*, Cambridge, MA: Harvard University Press, 2019.

[184] T. Schrepel, *Anarchy, State, and Blockchain Utopia: Rule of Law vs Lex Cryptographia,* in *General Principles and Digitalisation*, Hart Publishing, 2020; A. Mouzakitis, *Modernity and the Idea of Progress, in Frontiers in Sociology*, 2017; A. Rosenberg, *Philosophy of Social Science*, Boulder: Westview Press, 2008, pp. 19.

[185] R. Herian, *Regulating Blockchain – Critical perspectives in law and technology*, Routledge, 2019, p. 6.

a regulatory perspective. Nonetheless, observations about possible approaches and principles for regulating this technology will be discussed.

The ultimate purpose of this analysis is to offer an account of related regulatory and governance challenges. Understanding the terms of the discussion around these aspects will lay the ground to turn to the substantive merits of the debate over data protection issues.

Nevertheless, the announced task of *understanding* what regulating Blockchain means (or should mean) is not the easiest as it occurs within a contest of continuing (and, in some cases, past whilst in others current) conflicts to achieve solid regulation and governance of commercial platforms and related domains.

As observed by relevant authors, policymakers can address Blockchain technology's “alegal” characteristics in two ways: either by expanding existing legal provisions to include new activities that require legal coverage or by narrowing the scope of the law to exclude activities that should not have been encompassed initially. Under the first approach, policymakers may address the "lack of legality in Blockchain" by bringing certain activities necessary to function and maintain a Blockchain-based network under legal regulations. On the other hand, the second approach involves intentionally excluding specific actions from the legal framework by granting legal immunities, allowing these activities to occur without the usual constraints of the legal system. This deliberate exclusion of activities from the traditional legal framework would transform the alegal nature of this technology into an extra-legal one.[186]

[186] P. De Filippi, M. Mannan, W. Reijers, *The alegality of Blockchain technology*, in *Policy and Society*, 2022, pp. 1–15.

1.1.Defining the connotation of the law

Julia Black defined *regulation* as "the intentional use of authority to affect behaviour of a different party according to set standards, involving instruments of information-gathering and behaviour modification." [187]

Fundamentally, this definition evokes that of Lawrence Lessig, whose theory will be presented in the following. According to this author,[188] regulation results from *constraints* that define individual behaviour.

Regulation can promote innovation, as legislative decisions can impact innovation in the internal market.

As the recent 'AI Act' proposal proves, the European legislator is aware of that.[189]

[187] J. Black, *Critical reflections on regulation,* in *Australian Journal of Legal Philosophy*, 2002, p. 1.

[188] "Behavior in the real world — this world, the world in which I am now speaking — is regulated by four sorts of constraints. Law is just one of those four constraints. Law regulates by sanctions-imposed ex post — fail to pay your taxes, and you are likely to go to jail; steal my car, and you are also likely to go to jail. Law is the prominent of regulators. But it is just one of four. Social norms are a second. They also regulate. Social norms — understandings or expectations about how I ought to behave, enforced not through some centralized norm enforcer, but rather through the understandings and expectations of just about everyone within a particular community — direct and constrain my behavior in a far wider array of contexts than any law. Norms say what clothes I will wear — a suit, not a dress; they tell you to sit quietly, and politely, for at least 40 minutes while I speak; they organize how we will interact after this talk is over. Norms guide behavior; in this sense, they function as a second regulatory constraint. The market is a third constraint. It regulates by price. The market limits the amount that I can spend on clothes; or the amount I can make from public speeches; it says I can command less for my writing than Madonna, or less from my singing than Pavarotti. Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates. And finally, there is the constraint of what some might call nature, but which I want to call "architecture." This is the constraint of the world as I find it, even if this world as I find it is a world that others have made. That I cannot see through that wall is a constraint on my ability to know what is happening on the other side of the room. That there is no access-ramp to a library constrains the access of one bound to a wheelchair. These constraints, in the sense I mean here, regulate. To understand a regulation then we must understand the sum of these four constraints operating together. Any one alone cannot represent the effect of the four together.", see L. Lessig, *The Laws of Cyberspace*, 1998, pp.2-3.

[189] "Artificial intelligence is a rapidly developing family of technologies that requires *novel forms of regulatory oversight* and a safe space for experimentation while ensuring *responsible innovation* and integration of appropriate safeguards and risk mitigation measures. To ensure a *legal framework that is innovation-friendly*, future-proof and resilient to disruption, national competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxes to facilitate the development and testing of innovative AI systems under strict regulatory oversight before

Moreover, with the definition of the 'Blockchain Strategy', the European Commission clarified that "[t]he EU wants to be a leader in Blockchain technology, becoming an innovator in Blockchain"[190].

The question remains whether the actions carried out by the EU legislator can be genuinely effective.

We need to review some specific issues before analyzing the strength of the EU's action.

Firstly, the narrative of Blockchain as a technology that is impossible to be regulated will be verified. Similarities and differences with the theories promoted in the past for (non) regulation of Cyberspace will be presented to prove that those challenges are common to Blockchain and evaluate whether some solutions, already adopted for the Internet, can be applied in this new context.

As a matter of fact, not only is Blockchain continuing the regulatory conundrum experienced by the Internet, but it is also further problematizing it by introducing socio-economic concerns in the analysis.

Given the links with past experiences, traditional legal frameworks are always the starting point for any discussion. Although this is undoubtedly justifiable, the regulatory landscape for evolving technologies could benefit from critical approaches beyond the traditional framework and the conventional way of thinking, including those that affirm the predominance of code over the law.

The initial studies on this issue mainly focused on the effects introduced by the Blockchain code on law and the different governance models.[191]

these systems are placed on the market or otherwise put into service.", *Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, COM(2021) 206.

[190] https://digital-strategy.ec.europa.eu/en/policies/Blockchain-strategy.

[191] A leading work about Blockchain and law is undoubtedly that of Primavera De Filippi and Aaron Wright which intended "to provide an understanding of how blockchains work, the potential uses for the technology, the distinctive characteristics of *lex cryptographica*, and the potential avenues for

In particular, the discussion on the intersection and interaction between different governance methods revolves around conventional law (the code of law) and the rule of code (code *as* law).

In the Blockchain context, the expression 'code as law' identifies rules endogenous to Blockchain systems, which take the form of executable software code and technical protocols.

In practical terms, the issue is far more complicated than it appears.

The so-called Asimov's Laws[192] are no longer a fantasy, and the legislator needs to deal with those matters. The problem, however, is not in identifying the reasons behind the regulation (namely public, economic or social interest) but rather in formulating hypotheses on the reach of the technological power. Considering these aspects, it is important to understand whether to regulate the applications of the technology or to limit the use of the technology itself.

As discussed, despite understanding the considerable potential of Blockchain in many domains, the attention of the European legislator seems more focused on some specific use cases. This stance is perfectly reflected by the strategy outlined by the European Commission, which is concerned with implementing pilot case studies and creating a regulatory sandbox[193] involving different stakeholders in defining principles and standards for regulating Blockchain.

regulation", P. De Filippi, A Wright, *Blockchain and the Law – The rule of code,* Harvard University Press, 2019, p. 9.

[192] (1) A robot may not injure a human being or, through inaction, allow a human being to come to harm. (2)A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law. (3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

[193] A regulatory sandbox creates a space where regulated entities and regulators can collaborate and discuss innovations and inventions without fearing enforcement actions. In exchange for sharing information about potentially risky new products and services, the regulated entity receives guidance and advice from the regulator. Moreover, successfully participating in the sandbox can allow the regulated entity to leverage the regulator's assistance brand-newly.

The term "regulatory sandbox" was coined in 2015 by the Financial Conduct Authority in the UK to describe an environment to develop "mutual learning about the impact of current regulation on new financial products and, more generally, to reduce the phase of 'time to market' in financial innovation", As a general observation, by taking as a model the steps followed to delineate the regulation of Artificial Intelligence[194] and confronting some initiatives already in place for Blockchain, four policy techniques for regulating this technology may be identified:

- Option 1: a European legislative tool creating a regulatory scheme (so-called 'command-and-control regulation');
- Option 2: an 'ad hoc' approach resulting in the regulation of selected use cases which prove to be a combination of joint forces among involved stakeholders ('multi-stakeholders regulation');
- Option 3: 'meta-regulation', namely "the state's oversight of self-regulatory arrangements",[195] i.e., a combination of horizontal EU legislative instruments following a risk-based approach + codes of conduct for non-high-risk systems;
- Option 4: instruments of soft law - such as guidelines, codes of conduct, and recommendations - which can help keep a balance in the system at different levels while waiting for Institutions to take a clear position ('self-regulation').

Although these policy options will be individually assessed below, it may be worth anticipating that the first two techniques have already been tested, while the third one is yet to be applicable. While the European legislator is taking a holistic approach to the issue of regulating Blockchain, the definition of 'high-risk' and 'non-high-risk' systems is not straightforward for decentralized networks and requires more investigations from an IT point of view.

The fourth option, instead, seems easily practicable and has already been explored.

see R. Mangano, *Blockchain securities, insolvency law and the sandbox approach,* in *European Business Organization Law Review*, 19(4), 2018, p. 728.

[194] C. Schepisi, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE*, 2022, pp. 330-356.

[195] B. Hutter, *Risk, regulation and management*, in P. Taylor-Gooby, J. Zinn (eds), *Risk in social science*, OUP, Oxford, pp 202–227.

Based on the above, the reflections contained in this chapter unfold as follows. Three critical areas of regulatory interest will be explored. First, it will be clear that Blockchain is not a "non-regulatable technology" (i.e., a technology which cannot be regulated) or, quoting Primavera De Filippi, is not *alegal,* in other words, "situated beyond the boundaries of existing legal orders."[196]

This analysis will eventually lead to arguing that Blockchain, despite its cypherpunk origins, depends on law and reflects it. Thus, Blockchain becomes a regulatory system that facilitates the rise of a more specific regulation.

Before coming to that conclusion, section 2 will investigate the relationship between law and code and focus mainly on the "Cyberlibertarian theory", which has gained new life recently.

> "One of the persistent arguments that are made by proponents of new technologies is that any type of early intervention on the part of regulators will result in a fatal wounding of an infant industry that will never recover. The inference is that society will have lost something precious that can never be replicated, thereby denying society a technical advancement today that presumably may take years to recapture, since the course of technology will be unnecessarily diverted."[197]

Section 3 will give a cursory overview of the 'code as law' paradigm and test whether it is true that "Blockchain technology reinforces the tendency to rely on code (rather than on the law) to regulate individual actions and transactions [and] enables a whole new type of regulation by code, which —combined with smart contracts— also promotes a new way of thinking about the law."[198]

Section 4 will be dedicated to 'Cryptoregulation', intended and used broadly as a synonym for Blockchain regulation; accordingly, the earlier mentioned legislative

[196] P. De Filippi, M. Mannan, W. Reijers (2022), p. 1.

[197] M. Kianieff, *Blockchain technology and the Law – Opportunities and Risks,* Routledge, 2019, p. 186.

[198] P. De Filippi, S. Hassan (2016), cit.

techniques of command-and-control, self-regulation and co-regulation will be presented.

Generally, the debate around technology regulation has often been presented as a trade-off between *top-down* and *self-regulation* and resumed by the following questions: *should the law of technology remain independent (self-regulation)? Or should the states take an active role in the evolution by regulating this process?*

While responding to those queries, historical parallelism to the Internet will be made. The Internet is undoubtedly a prominent and reasonable place to start looking for emerging Blockchain regulation and governance trends.[199] Several workable solutions could be ideally suited to the Blockchain context.

For instance, as shown by the concept of 'privacy by design', the utopian paradigm[200] could be replaced by a more progressive legal regime that could ensure certainty, predictability and fairness over the anarchical interpretation of Blockchain.

[199] "Consequently, CyberLaw, as the legal branch of the Internet and of the "pre-Blockchain" digital environment, constitutes a scientific antecedent of unavoidable reference to CryptoLaw, this understood as the legal system of Blockchain and DLTs. This explains why multiple concepts or solutions from Blockchain or applicable to Blockchain, have been previously made or previously tested in cyber-legal contexts. This is the case with chronological challenges regarding cryptoregulation (new law or recourse to existing law), territorial or jurisdictional problems, the intensity of cryptoregulation, among others; but, above all, it is the case with methodological aspects of cryptoregulation, since it flows directly from so-called *Lex Informatica,* obviously dealt with by Cyberlaw. ", see P. G. Mexia, J. M. Barroso (2020), p.150.

[200] "(…) Blockchain accounts are reductionist on several levels. They are reductionist by focusing on the underlying architecture of Blockchain technology without considering its technological and functional latencies. Those latencies interact with existing social domains and stakeholders and are 'resolved' in the course of these interactions in favour of certain configurations that are not necessarily democratising and emancipatory. Utopian Blockchain narratives are also reductionist in their limited conception of trust issues and the roles played by trusted third parties within social interactions, as well as the wider significance of trust for social and political communities. Finally, a corporate collective action lens suggests that Blockchain decentralisation arguments overestimate the feasibility and virtues of decentralised management over delegated centralised decision-making processes. Whilst the latter suffers from a systemic agency problem, the separation of ownership and control within a company constitutes a compromise answer that seeks to balance the 'democratic' empowerment of a large and diverse group of shareholders against the efficiencies of a division of labour; much like centralised government seeks to articulate, coordinate and represent the preferences of a diverse citizenry and thereby enable autonomous self-governance.", U. Kohl, *Blockchain utopia and its governance shortfalls*, in O. Pollicino, G. De Gregorio, *Blockchain and Public Law*, cit., 2022, pp.39-40.

Regulations and standard-setting can be powerful tools for guiding Blockchain-based applications in the right direction while minimizing the transaction costs that result. Technology undoubtedly has enormous potential in that sense; therefore, steps must be taken to give it a chance to succeed. In this process, the law can and does have a very significant role to play in helping to guide Bl
ockchain to its fullest potential.

Given the interplay between the digital jurisdiction and the ordinary one, the state could choose among various regulatory strategies, sometimes overlapping with each other, which could be performed towards the digital sphere.

In this thesis, emphasis will be put on the European legislator's legislative strategy for creating a common framework for Blockchain.

In evaluating the state of the art of the debate, it will also be considered that the discussion has been fuelled by (sometimes random) observations of academics and practitioners. Some believed in the absolute power of the law on Blockchain, while others contested this power – like Braithwaite and Fisse - who affirmed that "State regulators won't have the power to enforce a regulatory law as if it is something felt from inside and not imposed from the outside".[201]

2. The interplay between technology and law

As they are incentives for innovation in society, all relevant technologies have been confronted at some point with the existing legal and regulatory framework.

New technologies have tested legal systems and society, changed existing social patterns and put pressure on the legal status quo.

[201] B. Fisse, J. Braithwaite, *Corporations, crime and accountability,* Cambridge University Press, 1993.

Both law and technology can shape the individual's behaviors and influence each other through a complex of dependencies and interdependencies.[202]

The advent of the Internet before and new technologies later have made clear that technology is designed to channel human actions towards certain specific behaviors and that, therefore, the individual free space of action is minimal.

As Cockfield pointed out: "[since] our lives become more entwined with technology, many observers assert that technology exerts more influence on our values, norms, interests and culture."[203]

The relationship between technology and regulation has been researched by jurists, sociology scholars and science and technology studies. [204]

The potential of digital tools to allow different engagements with information emerged predominantly in contrast to the linearity of paper-based legal activities.

The idea of the interplay between technology and law has evolved in recent years through an approach that can be defined as either autonomous or substantive, meaning that technology follows its logic and has substantive and independent effects

[202] In 1986 Langdon Winner wrote about the 'politics' of technology, arguing that technological design choices become part of the broader framework for public order, L. Winner, *Whale and the Reactor,* University of Chicago Press, 1986, pp. 19-39.

[203] A.J. Cockfield, *Towards a law and technology theory*, in *Manitoba Law Journal*, 2004, pp. 383-415.
Moreover, scientific method and technology were also increasingly becoming tools to understand and govern society and human nature, "as reflected in the birth of social sciences, the role of 'experts' in government, and the rise of positivism in sociology, philosophy and law in the 18th century, as well as the emergence of pseudo-scientific theories of Social Darwinism in the late 19th century.", U. Kohl (2022), p. 13.

[204] The complex relationship between law, science and technology is discussed in an extensive body of literature. See, for instance, and without claiming to be exhaustive, See e.g. A.J. Cockfield (2004), cit; A.J. Cockfield, J. Pridmore, *A Synthetic Theory of Law and Technology*, in *Minnesota Journal of Law, Science & Technology*, 2007, pp. 475-513; B.J. Koops, *Ten Dimensions of Technology Regulation - Finding Your Bearings in the Research Space of an Emerging Discipline*, in M. Goodwin, B.J. Koops and R. Leenes (eds), *Dimensions of Technology Regulation*, Wolf Legal Publishers, 2010, pp. 309- 324; N. Katyal, *Disruptive Technologies and the Law,* in *Georgetown Law Journal,* 2014; H.L. Vogel, *Disruptive Technologies and Disruptive Thinking,* in *Michigan State Law Review*, 2005; R.H. Brescia, *What We Know and Need to Know about Disruptive Innovation*, in *South Carolina Law Review*, 2016.
For an updated and rich overview of this field of legal inquiry, see R. Brownsword, M. Goodwin, *Law and the Technologies of the Twenty-First Century. Texts and Materials*, Cambridge University Press, 2012.

on social, economic, political, and historical developments. Consequently, society becomes the result of technological developments.

Notwithstanding, some commentators have further affirmed that the human mind was determined by technology to the extent that the purpose of life and human happiness could only be achieved through technology.[205]

The above technology-centric theory cannot be supported as it would deny the fundamental idea that humanity is independent and provided with free will. The point of view adopted in this thesis appears more in line with Vismann's thoughts. This author noted that there is a legacy effect when the material substrate of information changes, resulting in a reluctance to embrace the potential of the new media.[206]

Nevertheless, as long as the materiality of information changes in the digital world, the idea of law also changes. However, this idea is different from what David R. Johnson and David Post argued regarding the uniqueness of cyberspace with its lack of physical geography that required new forms of laws without borders.[207] They indeed affirmed that the emergence of cyberspace fundamentally has undermined the connection between legally significant online phenomena and their physical location, as the expansion of the global computer network has been eroding, among others, the correlation between geographical location and the authority of public powers to regulate global phenomena.

[205] Jacques Ellul defined the technological society as a new 'milieu' between people and nature, meaning that what previously had only been determined by the laws of nature derived than from rules determined by technology. The author compared the characteristics of independence and self-determination of nature with those of technology, J. Ellul, *The technological society*, New York: Knopf, 1964.

[206] C. Vismann, *Files: Law and Media Technology,* Stanford University Press, 2008, p. 163.

[207] D. Johnson, D. Post, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, pp. 1367-1402: "[The Internet] undermin[ed] the feasibility – and legitimacy – of laws based on geographic boundaries."

With its speed, rigidity and automation, the digital world has been transforming what law *is*, not just what is known as cyberspace. [208]

Technology has become no longer a simple target of regulation but also a regulatory actor[209] and a regulatory tool by incorporating laws and instruments for legal compliance into its design.

Accordingly, the assumption that the fact-finding dimension was independent from the normative dimension and, logically and chronologically, occurred before the making of normative judgments has been deconstructed; [210] likewise, the idea that technology was neutral. Regarding this concept, Hildebrandt and Tielemans clarified that an act could be considered neutral when it generates the same normative effect no matter what technology is applied since legislation is not meant to be neutral, as it represents the outcome of a political debate between several stakeholders promoting different views of the general interest. Therefore, the result of the political process substantially entails the imposition of a specific legal normativity with a specific legal effect. Consequently, the legislative process perpetuates a normative bias, a term that the authors do not use in a derogatory way but "as a reminder that law is meant to have a normative impact."[211] According to this vision, in constitutional democracies, the normative bias of legal rules combines the instrumental dimension of legal regulations, which is meant to achieve specific objectives, with their inner protective dimension. This means that law embodies its clear normative bias, implying that "the

[208] J. Goldsmith, *Against Cyberanarchy*, in *University of Chicago Law Review* 65, 1998; J. Goldsmith, T. Wu (2006).

[209] This is what De Filippi and Hassan called the third phase in the evolving relationship between law and technology which involves "the incorporation of legal rules into code on the one hand, and the emergence of regulation by code on the other", see P. De Filippi, S. Hassan (2016), cit.

[210] B. Wynne et al., *Taking European Knowledge Society Seriously*, Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission, Luxembourg: Office for Official Publications of the European Communities, 2007.

[211] M. Hildebrandt, L. Tielemans (2013), cit., p. 511.

neutrality of law in respect of different technologies requires that the law generates the same normative effect irrespective of the technological environment in which these norms apply."[212]

Returning to the analysis of the interplay between law and technology, the original idea that they were two separate entities reciprocally aware of each other's boundaries has been replaced by a new awareness: *they are reciprocally interrelated and complement each other.* What emerged from the debate around Internet regulation was that the "artificial division of virtual and real-space activity" [213] was a mistake.

However, this has yet to be translated into entirely new principles, as predicted by Judge Easterbrook, who argued that there was and should not have been a dedicated law for cyberspace. By comparing cyberlaw to an ill-conceived 'law of the horse', Easterbrook affirmed that discrete areas of legal study should have been limited to "subjects that could illuminate the entire law" and argued that areas of law that claimed to be distinct without such broad application were "doomed to be shallow and to miss unifying principles". [214]

The parallelism with horses meant that the law as then known (namely contract law, tort law) was good enough for cyberspace, as it was when horses began to be used as a means of transportation.[215]

The idea of the 'law of the horse' has been disputed by many authors, most notably by Lessig, who countered that "there is an important general point that comes from thinking in particular about how law and cyberspace connect".[216] This argument

[212] *Ibidem.*

[213] K. Werbach (2017), cit.

[214] Judge Frank Easterbrook pronounced these words when addressing an inaugural 'Law of Cyberspace' conference at Chicago Law School. See M. Guihot, *Coherence in Technology Law,* in *Law and Technology* 11(2), 2019, pp. 6-7.

[215] It is interesting to report the words of Lessig who was in the audience: "As is often the case when my then colleague spoke, the intervention produced an awkward silence, then some polite applause, and then quick passage to the next speaker. ", see L. Lessig, *The law of the Horse: what cyberlaw might teach,* in *Harvard Law Review*, p. 1999.

[216] L. Lessig (1999), cit.

provided a first insight into the more complex interaction between technologies and regulation that have evolved since then. It may be that Judge Easterbrook unwittingly offered the ground for establishing consistency in technology law. In order to extend Easterbrook's concept of the law of the horse to technology law, it is crucial to interpret his thesis as suggesting that a comprehensive understanding of technology law can only be achieved by contextualizing it within broader principles of regulation and law.

Over time, it has been proved that Internet regulation has developed based on existing general principles. These principles still govern the technology field today. Hence, *why should it be different for Blockchain technology?*
The answer is that the technological ground of Blockchain requires a dedicated approach. There is indeed a fundamental difference between the Internet and the Blockchain. The Internet is primarily an information technology, which has challenged the legal system by increasing the speed at which the law must be applied, as stated by Judge Richard Posner.[217] Conversely, the Blockchain has one feature that intrinsically identifies it: it is designed as a global and transnational technology built upon two key elements: encryption and immutability.

What has been stated in general terms in this section will be further explained in the following pages, which will outline the approach adopted toward regulating the Internet. The "historical" parenthesis of cyberspace and Internet regulation has reason to be retraced here. The standard error[218] that occurred with the Internet has been recently proposed again with the Blockchain, which has also aroused the reminiscence of Utopian thought. Thus, worthwhile observations can be gained from this comparison.
Borrowing Stilinovic and Hutchinson's words:

[217] See R. Posner, *Antitrust in the New Economy,* in *Antitrust Law Journal* 68, 2001, pp. 925, 939.

[218] The reference is especially to the idea that the Internet was characterized by 'alegality', i.e. it could not be subject to the power of the law.

> “We argue here that to consider the future is to understand the Internet's past, as it is in the past that ambiguity develops: the inception of the Internet history brought wide-sweeping predictions of a future we are now experiencing.“ [219]

2.1.A stroll around the Principality of Sealand

Historically, technology and law have long been engaged in constructing utopias, sometimes in complementary ways.

Technological developments have been seen as the conveyor of utopian futures, but the law has been neither abandoned nor drastically cut back.

As it is today for Blockchain, when the Internet first emerged, it instilled notions of anarchy and lawlessness.

In 1996, by proclaiming ‘The Declaration of the Independence of Cyberspace’, John Perry Barlow and the other representatives of the movement, [220] which included not just traditional sceptics of state power but also innovation-focused developers and legal experts, professed the inapplicability of conventional laws to cyberspace, claiming that regulation settled in state sovereignty could not function in that space:

> “[…] cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature, and it grows through our collective actions […] on behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. […]”.[221]

[219] M. Stilinovic, J. Hutchinson, *The Internet regulation turn? Policy, Internet and technology*, in *Policy and Internet*, 2022, p. 7.

[220] D. Post, D. Johnson (1996).

[221] J.P. Barlow, *A Declaration of the Independence of Cyberspace*, 8 February 1996.

The predominant narrative of the so-called Cypherpunks[222] was that Internet users would create systems that self-regulate and that they would themselves define the rules that apply to them.[223] Moreover, they insisted that states could not exercise territorial competence as cyberspace was not tightly grounded in territorial space.

"[L]egal concepts of property, expression, identity, movement, and context [would] not apply".[224]

Cypherpunk culture also gave origin to the philosophy of Cyberlibertarianism, which claimed that the Internet and related digital media technology could and should constitute spaces of individual liberty, meaning a place where individuals were self-governed and able to express themselves as they chose.[225]

Timothy May, one of the founding members of the 'Cyhpherpunk' movement, sustained in his 'Crypto Anarchist Manifesto' that the Internet and advances in public-private cryptography would soon enable people to interact more anonymously by relying on "tamper-proof boxes which implement cryptographic protocols" [226] and, therefore, altering "the nature of government regulation, the ability to tax and control economic interactions, [and] the ability to keep information secret".[227]

[222] "The cypherpunks were a group of privacy activists who in the 1990s helped establish the use of unregulated digital cryptography within the United States. […] The cypherpunks helped shape our Internet. Beltramini comments they were, "perhaps the single most effective grassroots organization in history dedicated to protecting freedom in cyberspace". However, Dahlberg argues that cyber-libertarian visions of the future, such as those held by the cypherpunks, had mostly dissipated by 2000, he comments that by then the Internet was, "seen as part and parcel of "everyday life" – simply an extension of existing social systems, rather than being a revolutionary medium transcending offline political and economic constraints", see C. Jarvis, *Cypherpunk ideology: objectives, profiles, and influences (1992–1998)*, in *Internet HistorIes,* 2022, VoL. 6, no. 3, pp. 315-316.

[223] H. Rheingold, *The Virtual Community,* MIT Press, 1994; K. Kelly, *Out of Control,* Basic Books 1994.

[224] J. P. Barlow (1996).

[225] "This cyber-libertarian rhetoric was at its strongest in the mid-1990s when it seemed like the Internet could be a space governed by its own rules, free of government control and other impediments associated with offline communication." L. Dahlberg, *Cyber-Libertarianism 2.0: A discourse theory/critical political economy examination,* in *Cultural Politics an International Journal,* 6(3), 2010, p. 333.

[226] T. May, The Crypto Anarchist Manifesto, 1992, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.

[227] *Ibidem.*

Essentially, the defenders of the utopian models neglected any normative legitimacy for states concerning the Internet, as they rejected the law as a legitimate normative tool.[228]

> “Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation’s border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible”. [229]

The ideas of Cyberlibertarianism climaxed with the foundation of the Principality of Sealand, an island built by the British Military forces in North Sea international waters during the Second World War. In 2000 a group of people moved there and launched HavenCo, a data-hosting services company, whose manifesto echoing the famous cyberlibertarian proclamation[230] stated:

> "Free comunication [sic] can never be a crime, and by itself can never hurt anyone. Criminal acts should be pursued at the point where the act takes place, not on the common carriers that enable all individuals to do business freely, such as telephone and Internet infrastructure providers […]”. [231]

[228] In 1992, David Clark of the IETF explained the philosophy of engineers in the following words: “We reject kings, presidents and voting. We believe in rough consensus and running code.” David D. Clark, *A Cloudy Crystal Ball*, Visions of the Future, plenary presentation, 24th meeting of the Internet Engineering Task Force, Cambridge, MA, 13–17 July 1992, http:/ietf20.isoc.org/videos/future_ietf_92.pdf.

[229] E. Hughes, *A Cypherpunk’s Manifesto*, 1993, https://www.activism.net/cypherpunk/manifesto.html.

[230] “Some cyber-activists went so far as to claim an abandoned British naval platform in international waters as the independent territory of Sealand, believing they could operate Internet servers completely outside of legal restrictions.” – see K. Werbach (2018), p. 520.

[231] *Why HavenCo*?, Oct. 18, 2000, http://web.archive.org/web/20001018230840/ www.havenco.com/products andservices/why.html. See also Frequently Asked Questions, HAVENCO (Aug. 16, 2000), http://web.archive.org/web/20000816001345/www.havenco.com/about-havenco/faq. html.

That sort of political experiment failed soon and, as Grimmelmann[232] affirmed, that happened not just for one reason:

> "HavenCo's failure—and make no mistake about it, HavenCo did fail—shows how hard it is to get out from under government's thumb. HavenCo built it, but no one came. For a host of reasons, ranging from its physical vulnerability to the fact that The Man doesn't care where you store your data if he can get his hands on you, Sealand was never able to offer the kind of immunity from law that digital rebels sought. And, paradoxically, by seeking to avoid government, HavenCo made itself exquisitely vulnerable to one government in particular: Sealand's. It found that out the hard way in 2003 when Sealand "nationalized" the company."[233]

In addition to explaining some of the reasons for the failure of this political and social experiment, Grimmelman perfectly condenses the purpose of the movement in a few words: 'immunity from the law'.

At that time, and today, that ideology appears upstream since government and law are generally tools for advancing people's shared values. Cyberlibertarians fundamentally attacked the self-government vision of the rule of law, which found its origins in Rosseau's school of thought: the general will that binds the people derives from and reflects their wishes so that there is no room for an interest contrary to theirs; [234] therefore, laws are legitimate if and only if they derive from the consent of the governed.

This idea explained why Joel Reidenberg, the 'Lex Informatica' father, sustained that states were engaged in a "struggle to establish the rule of law" against Internet threats.[235]

[232] See also this article from the author: J. Grimmelmann, *Welcome to Sealand. Now Bugger Off*, 1 July 2000, https://www.wired.com/2000/07/haven-2/.

[233] J. Grimmelmann, *Death of a data haven: cypherpunks, WikiLeaks, and the world's smallest nation*, 28 March 2012, https://arstechnica.com/tech-policy/2012/03/sealand-and-havenco/.

[234] J. J. Rosseau, *On the Social Contract, or Principles of Political Right* (original title Du contrat social: ou principes du droit politique), p. 1762.

[235] J. R. Reidenberg, *Technology and Internet Jurisdiction,* University of Pennsylvania Law Review, 2005.

Even so, although some supporters of the movement intended to build a new reality without law, neither Clark[236] nor Barlow argued for unregulated cyberspace despite disregarding the role of traditional norms.

On the contrary, since they were rightly aware that this would hinder progress in science and the economy, they imagined self-regulation by engineers as the natural alternative to applying national and traditional laws, namely a sort of law based on cryptographic codes. It is worth specifying that those regulations did not address cyberspace *per se*; instead, they targeted various and specific 'access points' over the Internet.

Considering the above, the Internet's regulatory tradition must be addressed, mainly because Blockchain protocols piggyback on existing Internet technologies. Hence, differentiation among the various network layers needs to be done.

Before exploring how Blockchain can regulate, the following section is dedicated to the reconstruction of the narrative around cyberspace that might help predict whether the growth and development of Blockchain will follow a similar path.

As Werbach articulated: "[t]he cyber libertarians of the 1990s were wrong that the Internet could escape the clutches of territorial regimes, but they were right that governments and courts should take the Internet's potential seriously."[237]

[236] Charles Clark stated: "The answer to the machine is the machine", C. Clark, *The answer to the machine is the machine* in *The future of copyright in a digital environment: Proceeding of the Royal Academy Colloquium,* The Hague Kluwer Law International, 1996, at p. 139.

[237] K. Werbach (2019), p. 226.

3. Applying the "Code as law" model to Blockchain

While the utopian movement was born and growing, Joel Reidenberg coined the concept of *Lex Informatica* by deriving it from the idea of *lex Mercatoria*.[238]

> "Regardless of the terminology used, the core characteristic of [Lex Informatica] is that it relies on code in order to define the rules that people need to abide by."[239]

The peculiarity of Lex Mercatoria is that it combines and merges elements from national and non-national laws. A similar pattern can be observed with Blockchain technology.

Lex Mercatoria has been legitimated without recognition from the state thanks to the community of merchants that played at that time a role that developers now hold.

The same holds as regards the function of coding in the Blockchain context, which has no territorial boundaries and the universal reach of Lex Mercatoria.

However, what represents a significant difference is that, unlike Lex Mercatoria, which a group of homogenous people developed, Blockchain is subject to the influence of people with different backgrounds and roles.

For what concerns *Lex Informatica,* in a pioneering article in the late 1990s, Reidenberg affirmed:

> "For network environments and the Information Society […] law and government regulation are not the only source of rulemaking. Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in

[238] Namely, the rules and principles defined in the Middle Ages to govern trade, which still influence international commercial law today. See R. Amelin, S. Channov, E. Lipatov, *Lex Informatica: Information Technology as a Legal Tool*, in *Communications in Computer and Information Science*, Springer Science and Business Media Deutschland GmbH, 2022, pp. 177–189; B. Deffains, P. Fenoglio, *Economics and legal order of cyberspace*, in *Revue Economique*, *52*(7), 2001, pp. 331–347.

[239] P. De Filippi, S. Hassan (2016), cit. p.2.

> system configurations. […] that […] form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage." [240]

> "Lex Informatica may restrain law's ability to deal with a problem. Lex Informatica may also substitute for law when technological rules are better able to resolve policy issues."[241]

No longer after, the concept of *Lex Informatica* was popularized by Lawrence Lessig, one of the most prominent cyberlaw scholars, who contended that within cyberspace *'code is law'*.[242]
This concept is essential as "[d]iscussion of code-based regulation within the Blockchain context struggles to dodge the influence of Lawrence Lessig (…)".[243]
Moreover, the system offered by Lessig is of pivotal importance in providing a comprehensive framework for Blockchain technology and distributed ledgers in general.

Lessig's theory has been interpreted and appropriated for meanings other than the original. By the concept of 'code is law', he did not assert that code is the *only* applicable normative limit in contrast to government regulation, [244] nor did he propose that code and law were epistemologically identical; instead, he sought to demonstrate the capacity for regulation that the code shared with the law. [245]

[240] J. R. Reidenberg, *Lex informatica: The formulation of information policy rules through technology,* Texas Law Review, volume 76, number 3, 1998, p.555. With the term *lex informatica* the author indicated that policy choices can be expressed through code.
[241] *Ivi*, p. 583.
[242] L. Lessig (1998).
[243] R. Herian (2019), p. 68.
[244] For an insightful analysis of this concept, see L. Lessig (2006), p. 5: "This book is about the change from a cyberspace of anarchy to a cyberspace of control."
[245] "Lawrence Lessig, a long time ago, reassured that the digital would not be a law- less space. Rather the code will be law. There is a sleight-of-hand going on within Lessig's now familiar slogan. Code as law is not what lawyers writing about disruptive technologies see as law. His law must be juxtaposed with the early anarchical ideology of the Net as anything goes that he was attempting to distinguish. Lessig's code as law concerned order, structure and predictability, rather than modern law's commands of sovereigns and centralized, hierarchical decision-makers. His claim was that in the digital, code can

For Lessig, "[code] is one of the multiple regulatory factors exerting a normative influence on individual behavior," which reveals to be law, but only one of the different sources of law that does not overrule the others.

Along with the concept of 'code is law', the 'pathetic dot theory', theorized more than twenty years ago by Lessig, deserves to be analyzed. It is a framework of four modalities of regulating (the law, the social norms, the market, and the architecture) that become 'constraints' on human actions when acting together.

Law limits individual actions through rules and regulations; *social norms* exert influence on cultural behaviours; the *market* acts on individuals as it encourages or discourages specific behaviours through the mechanism of supply and demand, and finally, the (social) *architecture* "features of the world, whether made, or found"[246] consists of biology, geography, technology and others that constrain people's actions.

Against this backdrop, regulation becomes the "sum of these four constraints. Changes in anyone will affect the regulation of the whole. Some constraints will support others; some may undermine others… A complete view therefore must consider these four modalities together".[247]

This means that the interaction of these forces gains importance for regulating cyberspace as it does for the physical world.

In Lessig's vision, the interplay of such elements causes both a direct and indirect effect and contributes to shaping individuals' actions in ways they do not always understand.

> "One is the effect of each modality on the individual being regulated i.e. how does law, for example, directly constrain an individual? How does architecture directly constrain an individual? The other is the effect of a given modality of regulation upon

be seen as doing some of the structural functions that modern law did in earlier eras.", K. Tranter (2021), p. 168.

[246] L. Lessig, *The New Chicago School*, in *The Journal of Legal Studies*, 1998, pp. 661–691.

[247] L. Lessig, *Code: And Other Laws of Cyberspace 2.0,* 2006, http://codev2.cc/.

> a second modality of regulation, an effect that, in turn, changes the effect of the second modality of individuals".[248]

Furthermore, it is worth bringing up the other two elements of Lessig's theory relevant to this research.

First, the intersection between law and architecture can lead to opposite effects: when architecture promotes a value conflicting with the law, the legal system may accept or reject it. Second, the ascertainment that the more the architecture is decentralized, the more difficult regulation will be.[249]

To sum up, Lessig argued that in the realm of cyberspace, where technology and data dominate, computer code serves as a form of regulation akin to the functions of traditional law. This implies that those who control the computer code possess significant law-making powers, similar to what was once exclusive to the state in the pre-digital era.

Consequently, this situation presents two possible outcomes. The controllers of code can either supplant the law-making authority of the state or collaborate with it to achieve public policy objectives in the digital environment. The relationship between the state, the traditional lawmaker, and the controllers of code, as the new lawmakers, becomes intricate, encompassing potential cooperation, competition, and tension. A notable example highlighting these dynamics is the emergence of cryptocurrencies like Bitcoin, which aim to provide an alternative to the state-controlled financial system.[250]

[248] L. Lessig (1999), p. 511.

[249] *Ivi,* p. 534.

[250] In contrast, it is interesting to highlight that during the COVID-19 pandemic, an alliance between Google and Apple was formed to work alongside governmental efforts in developing a decentralized system for contact tracing apps. This exemplifies how the state and code controllers can collaborate in specific contexts. See https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/#:~:text=In%20this%20spirit%20of%20collaboration,security%20central%20to%20the%20design.

Although the framework presented by Lessig has been used to describe the regulation of behaviour on the Internet, where the architecture is computer code,[251] that structure can now be adapted to suppose and prove – at least for advanced applications – its applicability to Blockchain.

The soothed idea of code as law and self-sufficiency of technology has found new strength with the advent of Blockchain, mainly thanks to the critical work of De Filippi and Wright. In their recent book *'Blockchain and the Law – The rule of code'*, they draw on Lessig's theory on regulatory modalities to argue that the state can regulate Blockchain through the law, social norms, market, and code.

For these authors, in Blockchain, "*[t]echnical rules* could increasingly assume the same role and functionality as *legal rules*"[252] and "[i]n some cases, transposing laws into code reduces the uncertainty around the interpretation or application of these rules. (…) Unlike laws written in natural language, code-based rules leave less room for interpretation and can therefore be implemented more consistently and predictably."[253] They affirmed that Blockchain sits between the transportation and application layers and enables protocols and services that are capable of "implementing their own system of rules – *lex cryptographica* – enforced by the underlying protocol and smart contracts."[254]

Moreover, an essential aspect of their research is the analysis of the implication of *lex cryptographica* on the existing legal structure:

[251] *Ivi*, pp. 124-125.

[252] P. De Filippi, A. Wright (2018), p. 194.

[253] *Ibidem*, p. 195.

[254] *Ibidem*, p. 50. The authors also maintained at page 55: "In effect, with *lex cryptographica*, national laws get pushed to the edges. Individuals decide whether to interact with these autonomous systems, frustrating legal regimes focussed on implementing rules on central parties that currently control or help facilitate online activity. If Blockchain-based autonomous systems become increasingly used to provide online services, governments will need to adopt new techniques and approaches to shape or regulate those services. Traditional legal doctrines, especially those focussed on regulating middlemen, will not easily translate to these new decentralized and autonomous systems, and the broader adoption of Blockchain technologies may ultimately require the development of alternative mechanisms of regulation that better account for the distinctive characteristics of *lex cryptographica*."

> "Existing bureaucratic systems, operated by people and institutions abiding by the rule of law, would be replaced by technocratic systems, operated by technical structures and code-based rules that ultimately constrain human behaviour and discretionary choice. Algorithms would define the possible actions that individuals may or may not take, to the detriment of potentially valuable alternatives.
>
> The focal point of power in many of these systems, however, would no longer be centralized institutions and hierarchical structures but rather informal systems of (often invisible) rules dictated by programmers deploying code. As a result, the growing reliance on algorithms to shape our interactions with one another and with third-party operators would increasingly subject us to the 'rule of code' as opposed to the 'rule of law' – eventually placing us in an algocracy."[255]

Additionally, they added that "one of the key consequences of Blockchain could be a rapid expansion of what Lawrence Lessig referred to as "architecture" — the code, hardware, and structures that constrain how we behave — or at a minimum a redefinition of how laws and regulations are designed, implemented, and enforced".[256]

The idea of legal structures implemented and delivered through cryptographic and smart-contracting computer codes is also known by the expression 'Cryptolaw' that has been accused of being no more than Cyberlaw.[257] The reason for this criticism is that, as of then, the debate around Cyberlaw focused on who could regulate the Internet and how. Today, the issue is Blockchain, but the questions are the same.

Notwithstanding, Cryptolaw presents an essential difference from Cyberlaw. The term 'cyberlaw' is nowadays synonymous with "the area of Internet regulation" [258] since "the vast majority of cyberlaw analysis focuses on the application of existing

[255] Ibidem, p. 55.

[256] P. De Filippi, A. Wright (2018), cit.

[257] V. Schonberger, *The Shape of Governance: Analyzing the World of Internet Regulation,* in *Virginia Journal of International law*, 2003, p. 605.

[258] *Ivi,* p. 606.

legal norms—intellectual property, trademark, antitrust, content regulation and the like—to cyberspace issues." [259]

Conversely, Cryptolaw is influenced by the immutability of transactions within the Blockchain and, at the same time, generates trust in the system. Of course, this peculiarity was absent in the discussion around Cyberlaw and the Internet, which for its characteristic of an information system governed by intermediaries, is opposed to Blockchain, which is decentralized and disintermediated. In this regard, smart contracts represent a paradigmatic expression of Cryptolaw since they allow any person to contract with unknown persons or machines.

The development of modern Blockchain codes through the 'datafication'[260] of society made it clear that the code could be used for various applications beyond the financial field. As anticipated, given that contractual clauses and agreements are incorporated into the code, Blockchain takes on the connotation of a 'regulatory technology', a technology setting rules that orient and modify the behaviours of individuals. From that conclusion, some authors observed that Blockchain also affects the creation of the law stemming from the contract; in other words, "law is progressively turning into code".[261] This process is conditioning the modalities of negotiation and stipulation of the contract and the entire system of guarantees established by the contract law framework. The effects of the agreement are unalterably written in the code; therefore, the parties can decide whether to include the traditional contractual safeguards in terms of the contract.

[259] *Ibidem.*

[260] A. Martin, G. Sharma, S. Peter de Souza, L. Taylor, B. van Eerd, S. M. McDonald, H. Dijstelbloem, *Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions*, in *Geopolitics*, 2022; S. Newell, M. Marabelli, *Strategic Opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term social effects of 'datafication'*, in *Journal of Strategic Information Systems*, 2015, p. 3.

[261] P. De Filippi, S. Hassan (2016).

Essentially, *lex cryptographia* and cryptolaw assume that distributed ledgers will empower regulation through code to the detriment of other forms of regulation.

The history of Internet regulation confirms that companies did not settle in Sealand but in well-structured jurisdictions. Similarly, blockchains are not isolated from the real world and their development and diffusion will mostly depend on the credit given by politics and, above all, by law.

The law could serve as an element of wide recognition and, at the same time, support code development. If code is "slow to evolve, the law can assist by removing bottlenecks to innovation."[262]

Undoubtedly, regulatory uncertainty could stifle innovation, while a coherent and straightforward legislative framework can prevent it.

From the above, the question that preliminarily arises is: *Is the law capable of reaffirming its legitimacy over Blockchain and the values that it promotes, or does it merely represent a constraint?*

Is it true that "[d]ecentralized Blockchain-based applications may well liberate us from the tyranny of centralized intermediaries and trusted authorities, but this liberation could come at the price of a much larger threat – that of falling under the yoke of the tyranny of code"?[263]

Given the ontological differences with the Internet, a second question to investigate is: *can Blockchain, which reduces the need for intermediaries, lead to completely eradicating them?*

[262] I. Brown, C. Marsden (2013), p. 31.

[263] A. Wright, P. De Filippi (2018), p. 210.

4. The paradigm of Cryptoregulation: regulating Blockchain

In this paragraph, we will examine Cryptoregulation[264] –the regulation of Blockchain technology - and its ecosystem.

Regulating Blockchain is a complex task, and above all, regulation should not be seen as a final event but instead as an open-ended process.

Co-regulation, which this research considers the most practical solution, explicitly acknowledges that no actor has all the answers and that regulatory principles must be evaluated and revised when necessary.[265]

4.1.Can Traditional legislative techniques fashion Blockchain?

Along with the ongoing technical development of Blockchain, another issue is represented by its characteristic of disintermediation, which leads to asking whether this technology can be regulated through traditional techniques.

> "(…) Blockchain makes up a serious threat to intermediaries, who in turn are relevant because they guarantee social trust. And also, of course, to intermediaries operating on the Internet."[266]

> "At this point, we could well think that, more than a threat, Blockchain and in general DLTs will cause the inevitable end of trust based on human means, and *en passant*, of any intermediaries. That is to say, Blockchain will imply the end of governmental mechanisms of public faith such as notary publics or public registries."[267]

Previous sections dispelled doubts about the ineptitude of regulatory attempts that, for some authors, would have needed to be more effective in contrast to the

[264] As anticipated in the Introduction, this term is used in here with an extensive meaning.

[265] M. Callon, P. Lasoumes, Y. Bathe, *Acting in an Uncertain World: Essay on Technical Democracy* (Inside Technology), MIT Press, 2011.

[266] P. Garcia Mexia, J. Morales Barroso (2020), p. 86.

[267] *Ivi*, p. 88.

irreversibility of the cryptographic code. Blockchain and distributed ledgers are not extra-legal fashions immune to regulation[268], and, in general terms, technology cannot avoid regulation.

On the contrary, the law can influence code, market, and social norms to regulate technology. Substantially, although Blockchain-based applications can be conceived to overlook the law, they still depend on the intermediaries supporting the underlying technology, which can be subject to regulation.

In this given scenario, governments have various options to consider. One approach involves exerting pressure on intermediaries responsible for developing, deploying, or maintaining the technology. For example, governments may require software developers and hardware manufacturers of mining devices to incorporate specific features into their technology. This ensures that governments can intervene, if necessary, to regulate autonomous Blockchain-based systems. In cases of harm, governments could demand that miners censor certain transactions or even revert the Blockchain to a previous state to rectify damages or address harm. Governments could also establish laws targeting commercial operators who interact with decentralized Blockchain-based applications, indirectly regulating the use of these technologies.

Alternatively, or in addition to the mentioned approach, governments could intervene to regulate the incentivization schemes underlying a Blockchain and influence social norms. They could introduce a set of economic incentives aimed at shaping the activities of autonomous Blockchain-based systems. Additionally, governments could attempt to shape the moral or ethical standards of the user and mining community by supporting a specific blockchain-based network, thereby influencing social norms.

[268] "At the same time, a complete lack of regulation could also prove problematic. Given the lack of well-defined regulatory framework for Blockchain-based applications, parties seeking to deploy the technology could find themselves in a legal gray area, incapable of knowing whether what they are doing today is lawful and whether it will continue to be so further down the line. The lack of proper regulatory framework for Blockchain technology could dissuade entrepreneurs, start-ups, and incumbents from deploying these new technologies for fear of stepping too early into untested waters." P. De Filippi, A. Wright (2018), p. 209.

Since a Blockchain operates through distributed consensus, all parties involved in supporting the network possess the ability to intervene, through coordinated action, to enforce the application of specific legal or community norms.[269]

Anyway, beyond the options chosen, what is important to take into account is that regulatory activity never consists of an action *per se*, yet it results from the combination of various forces that can lead to different results.

Blockchain regulation needs to address or independently respond to various of requirements and situations both online and offline, which could be unlikely surrounded by a unique definition.[270]

> As rightly affirmed by Herian, "[t]his does not mean the Blockchain regulatory process, in whatever form it eventually takes, can or should be considered neutral, however. (…) As a general backdrop to questions of Blockchain regulation therefore, (…) regulation can be understood here more generally as 'the intentional activity of attempting to control, order or influence the behaviour of others', which necessarily carries political and ethical principles and burdens that ought to be shared by the community as whole, whether on- or offline."[271]

It is unclear whether decentralized ledgers and blockchains should be treated under existing legal frameworks which focus on a central regulatory point. Moreover, in decentralized systems governed by peers, who could act as a control point?

There is no doubt that, in the relationship between Blockchain and regulation, the various network layers have to be recognized.[272]

> "Classic regulatory conundrums turn on the extent to which regulatees are compliant or can be made to be compliant in the future. Where they are not, and this is already evident amid the excitement of new technologies such as Blockchain, regulators try to

[269] P. De Filippi, A. Wright (2018), pp. 208-209.

[270] Ibidem, p. 51.

[271] R. Herian (2019), p. 53.

[272] See Chapter I.

> 'minimise resistance ex ante or have a strategy for dealing with it ex post' (Brownsword and Goodwin, 2012, p. 62). *Regulators traditionally draw on different combinations of law* (case law, legislation, judicial review, etc.), *regulation* (existing forms of regulation or substantive and general regulatory principles), *and governance* (non-legal but not necessarily less formal modes of command and control), in order to achieve ex ante and ex post regulatory outcomes. Insofar as those are distinguishable options that can mixed and matched as the regulatory setting requires, the three give structure to new regulatory regimes or alternatively mobilise existing structures capable of absorbing certain regulatory targets: behaviours, forms of conduct and the material effects of technology."[273]

Taking Internet regulation as an example, it seems unlikely to uproot existing regulatory models but instead derives the main principles from them.

Therefore, mainstream theories and practices from the regulatory tradition can gain relevance as a valuable measure for defining a regulatory framework for Blockchain.[274] At the same time, it cannot be taken for granted that existing laws will quickly adapt to the claims brought about by new technologies.[275]

The main difficulty – and the essential aim of regulation in this field – is to develop a regulatory framework that sufficiently seizes the transition from the existing regulating system built on bilateral relationships to an increasingly distributed financial world. Likewise, another challenging task is maintaining a unified and consistent approach while contending to formulate a coherent regulatory response, given the speed of technological advancement.

[273] R. Herian (2019), p. 35.

[274] A. Y. P. Yang, *When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?,* in *Stanford Journal of Blockchain Law & Policy,* 2023, available at https://stanford-jblp.pubpub.org/pub/jurisdiction-rules-Blockchain/release/1.

[275] R. Brownsword, *Law, Technology and Society: Reimagining the Regulatory Environment*, Oxford: Routledge, 2019; K. Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of law and Code as Law,* in *Modern Law Review*, 2019, p. 207. Moreover, Brownsword argued that "[e]ach time a new technology appears, or an established technology assumes a fresh significance or moves forward in some way, we should not, so to speak, have to reinvent the regulatory wheel, we do need to refine our regulatory intelligence to bring it into alignment with the characteristics of each particular technology", see R. Brownsword, *Rights, Regulation, and the Technological revolution,* Oxford University Press, 2008, p. 559-564.

Returning to the options analyzed above, legislators may have several tools at their disposal to shape the technology.[276]

For instance, they can impose specific rules, which can directly or indirectly change the underlying functioning of the technology, and they can frame social norms relating to technology through education, the so-called 'command-and-control' technique.

Public authorities could impose obligations on physical persons who act as nodes in the network, but this decision might face obvious difficulties in identifying and controlling nodes. Indeed, even if public authorities decided, for instance, to make smart contracts illegal by depriving them of the guarantees of enforcement before a court, users could continue to use the technology, given that Blockchain software is open source.

However, when there is uncertainty about how to apply existing legal frameworks to new technological applications, various options for interpretation are available.

For instance, when a regulator adheres to the so-called 'wait-and-see approach',[277] and is not ready to issue a position, it can provide informal guidance through guidelines, reports, and working papers. The benefits of this form of communication are to provide stakeholders with some references without jeopardizing future reconsideration of their stance.

As the introduction touches on, another interesting option is to create a regulatory sandbox, [278] a facility where innovators can test their products or business models without being subject to several legal requirements.

[276] M. Finck, *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy,* in *European Law Review*, 2018; L. A. J. Senden, *Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?,* in *Electronic Journal of Comparative Law*, 2005.

[277] S. S. Tyagi, S. Bhathia, *Blockchain for business: how it works and creates values,* Wilei, 2021, p. 265 ss.

[278] Cfr. note 193.

This approach allows regulators to study some of the possible development of the technology from a privileged perspective while having the chance to correct some distortions and guarantee legal certainty to the industry.

4.2.Blockchain governance and the debate around off-chain vs on-chain rules

In assessing what the best approach to Blockchain regulation is, one should also consider the interdependencies between state governance (also known as 'conventional law') and Blockchain governance, which can be regarded as the integration of norms and culture, the laws and the code, the people and the institutions that facilitate coordination and together determine a given organization.[279]

In the Blockchain environment, various stakeholders contribute to the definition of its governance. On the one hand, the core developers suggest the choices or protocol changes from which network participants will select. On the other hand, network participants (miners and validators) must choose between the possible solutions offered by the core developers. Finally, users ultimately contribute to the value of the overall Blockchain network.[280]

To define Blockchain governance two dimensions should be considered: off-chain governance (*of* the infrastructure) and on-chain governance (*by* the infrastructure).[281]
Usually, *on-chain governance* refers to infrastructure-specific rules, precisely the voting procedures used to agree on specific terms and conditions. These rules can be described as a combination of architectural and market rules.
Smart contracts are part of the on-chain world as the Blockchain can automatically enforce them. This expression has also been tightly linked to *Decentralised Autonomous*

[279] A. Fischer, M.C. Valiente, *Blockchain governance,* in *Internet Policy Review*, 2021, pp. 1-10.

[280] M. Zook, J. Blankenship, *New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance,* in *Geoforum*, 2018, p. 251; P. de Filippi, G. McMullen, *Governance of Blockchain Systems: Governance of and by Distributed Infrastructure*, in *Blockchain Research Institute and COALA Research Report*, 2018, https://hal.archives-ouvertes.fr/hal-02046787/document.

[281] W. Reijers, I. Wuisman, M. Mannan, P. De Filippi, C. Wray, V. Rae-Looi, A.C. Vélez, L. Orgad, *Now the code runs itself: On-chain and off-chain governance of Blockchain technologies*, Springer, 2018, pp. 1-22.

Organisations (DAOs), whose bylaws are written in code and enforced by the Blockchain.[282] As such, on-chain governance focuses on enforcing formal and codified rules rather than elaborating on these rules.

'*Off-chain* governance' refers instead to the social and institutional mechanisms allowing these rules to be defined and elaborated, as well as the procedures put in place to apply, enforce, or possibly change these rules, which include endogenous social norms (i.e., rules established by a specific Blockchain community) and exogenous procedures established by law.

While on-chain rules are usually clear and formalised, off-chain rules are generally informal.

Without dwelling too much on the DAOs, which, given their complexity, would require a separate discussion, it is here worth noting that all DAO projects are ultimately a mixture of off-chain and on-chain elements, echoing the idea that, even within Blockchain networks, governance consists of more than coded procedures.

Having clarified the distinction between on-chain and off-chain governance, it is important to consider that, although many similarities between the Blockchain and the Internet networks have been emphasized in this chapter, one should consider that blockchain is currently facing a very different set of challenges than Internet faced twenty years ago.

The regulatory challenge posed by the Internet in the 1990s has been resolved through the regulation of intermediary operators—who could design and modify the technological infrastructure of their online platforms.

[282] S. Hassan, P. De Filippi, *Decentralized autonomous organization*, in *Internet Policy Review*, *10*(2), 2021, pp. 1–10; Y.Y. Hsieh, J.P. Vergne, P. Anderson, K. Lakhani, M. Reitzig, *Bitcoin and the rise of decentralized autonomous organizations*, in *Journal of Organization Design*, *7*(1), 2018; S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, F.Y. Wang, *Decentralized Autonomous Organizations: Concept, Model, and Applications*, in *IEEE Transactions on Computational Social Systems*, *6*(5), 2019, pp. 870–878; K. Saurabh, N. Rani, P. Upadhyay, *Towards Blockchain led decentralized autonomous organization (DAO) business model innovations*, in *Benchmarking,* 2022; M. Singh, S. Kim, *Blockchain technology for decentralized autonomous organizations*, in *Advances in Computers,* 2019, pp. 115–140.

The regulatory issues posed by the public and permissionless blockchains cannot easily be undertaken by using the approach adopted for the Internet, as the decentralised nature of Blockchain networks has challenged the ability of governments and other regulatory authorities to impose their sovereignty over these networks.

In Blockchain networks, no regulatory authority can control or change the *on-chain governance* rules established within the technological infrastructure of the network. Therefore, if a regulatory authority cannot unilaterally modify the code of a Blockchain-based network, it is necessary to focus on the *off-chain governance* rules to influence the design choices of a particular blockchain community.

Though the coercive power of the law cannot be readily applied to regulate Blockchain-based systems, existing laws can, nonetheless, indirectly influence the operations of these platforms. This means that even if many Blockchain-based networks operate outside of the reach of the law, the various actors involved in the governance of these networks can be subject to the law.

Moreover, despite the need for a trusted authority regulating public and permissionless networks, public authorities can still have the power to adopt regulatory and policy acts to impose specific rules and, consequently, influence the entire governance network.

4.3. Where do we stand in the European Union?

2022 represents a landmark for regulatory developments, particularly in the crypto field. Many States, like Singapore,[283] Switzerland, [284] the UK,[285] the United States[286] - especially the state of Delaware[287] - have proved very proactive in that year.

[283] The Singaporean parliament has passed legislation expanding the Monetary Authority of Singapore's (MAS) regulatory powers over the crypto industry. The law – which was passed on April 5th – requires crypto companies that only do business abroad to obtain a license and imposes harsher penalties for failing to maintain platform security. Furthermore, it empowers the market regulator to issue prohibition orders against individuals who are unfit to work in the financial and crypto industries, https://cryptoslate.com/singapore-tightens-laws-for-crypto-companies-in-a-cautious-bid-to-embrace-the-industry/.

[284] "Switzerland's government has indicated that it will continue to work towards a regulatory environment that is friendly to cryptocurrencies. In 2016, the town of Zug, a prominent global cryptocurrency hub, introduced Bitcoin as a way of paying city fees while in January 2018, Swiss Economics Minister Johann Schneider-Ammann stated that he was aiming to make Switzerland "the crypto-nation". Similarly, the Swiss Secretary for International Finance, Jörg Gasser, has emphasized the need to promote cryptocurrencies while upholding existing financial standards.

Building on those objectives, in late 2020, Switzerland's Department of Finance began a consultation on new blanket cryptocurrency regulations that would enable it to take advantage of Blockchain technology without stifling innovation. In 2021, the Swiss Federal Council voted in favor of a proposal to further adapt existing financial regulations to cryptocurrencies in order to address their illegal use."

[285] "While there are no cryptocurrency-specific laws in the U.K., the country considers cryptocurrency as property (not legal tender), and crypto exchanges must register with the U.K. Financial Conduct Authority (FCA). Crypto derivatives trading is banned in the U.K. as well. There are cryptocurrency-specific reporting requirements relating to know your client (KYC) standards, as well as anti-money laundering (AML) and Combating the Financing of Terrorism (CFT). Although investors still pay capital gains tax on crypto trading profits, more broadly, taxability depends on the crypto activities undertaken and who engages in the transaction. As of 30 August 2022, crypto exchange and custodian wallet providers are required to comply with the reporting obligations implemented by the Office of Financial Sanctions Implementation (OFSI). Crypto firms are now required to notify OFSI as soon as possible if they know or have reasonable suspicion a person is subject to sanctions or has committed a financial sanctions offense. In October 2022, the lower house of the British Parliament recognized crypto assets as regulated financial instruments. The draft bill extends current laws regarding payments-focused instruments to stablecoins.", https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122.

[286] "While it is difficult to find a consistent legal approach at the state level, the US continues to progress in developing federal cryptocurrency legislation. The Financial Crimes Enforcement Network (FinCEN) does not consider cryptocurrencies to be legal tender but considers cryptocurrency exchanges to be money transmitters on the basis that cryptocurrency tokens are "other value that substitutes for currency." The Internal Revenue Service (IRS) does not consider cryptocurrency to be legal tender but defines it as "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value" and has issued tax guidance accordingly."https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/.

[287] See, for instance, M. Byhoff, B. Ford, *This State is Becoming America's Crypto Capital*, Bloomberg, 2022.

This is important to fuel the discussion as, although regulation can assume different forms, one must recognize the importance of regulatory guidance from legislative Institutions for a twofold reason. First, they provide certainty to stakeholders operating in the Blockchain domain by allowing them to design compliant Blockchain use cases. Second, because of the first reason, greater regulatory transparency dispels doubts and promotes investment growth in technology.

However, few prevailing approaches emerge among the diverse array of regulatory initiatives, statements, and policymaking efforts.[288]

> "The so-called 'wait and see' or the somewhat more proactive 'wait and monitor' approaches to regulation adopted by the likes of the European Commission are symptomatic not of a reasonable approach to Blockchain, but, I argue, of an unwillingness by governments to muster the energy, let alone the resources, to challenge private self-interest."[289]

This approach might be appropriate considering the state of the art of the technology.

> "Given that Blockchain technology is still largely immature, there is a danger that regulating the technology too early could preclude the emergence of new and unexpected applications that have not yet been fully explored or discovered. Permission-based regulation could prevent public and private parties from freely experimenting with this new technology, ultimately chilling innovation."[290]

So far, a fragmented regulatory landscape has been in constant and fluid evolution.

In the beginning, the academic legal discussions placed disproportionate emphasis on virtual currency and made little mention of the technology behind the currency.

[288] In particular, cryptocurrencies raise some new regulatory and legal issues.

[289] P. De Filippi, A. Wright (2018), p. 209.

[290] *Ivi*, p. 41.

Nonetheless, some authors soon acknowledged the technology's real potential, considering that "more promising perspectives of virtual currencies may lie in the technology they use, i.e. the distributed ledger technologies."[291]

Within European Union, the Parliament was the first to analyze whether the technology or the applications were to be regulated.[292] It was soon clear that the Institution intended to 'wait and see': "[i]t's probably too early to intervene at this stage, because we as legislators don't yet see sufficiently clearly to know what the main issues are going to be — so in order not to stifle innovation, we don't want it to be now."[293] The initial idea was to adapt existing regulations to new technology rather than create new ones.

As mentioned in the previous section, which analyzed the applicability of the 'code as law' approach to regulation, two sub-analyses are preliminary to the investigation. First, it needs to be understood whether the code or the applications must be regulated. Second, there are different types of Blockchain networks – permissionless and permissioned –[294] requiring different approaches and challenges.

Considering these issues, the European legislator first started exploring use cases to test their impact; then, it left space for businesses to experiment.

In Europe, the acceptance and recognition of Blockchain technology has experienced a slow pace, prompting the adoption of a cautious approach that proved fruitful several years ago when uncertainty surrounding the technology prevailed. However,

[291] G. Peters, E. Panayi, A. Chapelle, *Trends in crypto-currencies and Blockchain technologies: A monetary theory and regulation perspective*, in *Journal of Financial Perspectives*, 2015, p. 37.

[292] *European Parliament resolution of 3 October 2018 on distributed ledger technologies and Blockchains: building trust with disintermediation,* P8_TA(2018)0373; *European Parliament resolution of 13 December 2018 on Blockchain: a forward-looking trade policy,* P8_TA(2018)0528).

[293] MEP Jakob von Weizsäcker pronounced these words during an event on the state of the blockchain conversation in the EU. See, N. Acheson, *Regulating Ethereum? EU Parliament Weighs Blockchain's Big Issues,* https://www.coindesk.com/tech/2017/05/12/regulating-ethereum-eu-parliament-weighs-Blockchains-big-issues/., 15 May 2017.

[294] See Chapter I, para 4.4.

this approach has inadvertently resulted in a significant disparity in the legal framework compared to non-European Economic Area (EEA) states.

The freedom left to businesses to experiment with use cases for not stifling the potential of the technology created uncertainties about the legality of those applications, primarily because some of those proved to be able to have a significant impact on state monopoly.

In other words, the precautionary approach of the European legislator was right some years ago when the most considerable risk was caging technological innovation in tight rules. On the contrary, as the following analysis will show, the state of the art shows a profound 'law lag', as "existing legal provisions are inadequate to deal with a social, cultural or commercial context created by rapid advances in information and communication technology".[295]

At the policy level, the European Commission supports Blockchain. All of the different legislative initiatives work in a highly complex and constantly changing transnational context, which requires interoperability. The most considerable part of the blockchain's strategy is undoubtedly represented by the building of its infrastructure, which aims to protect consumers and provide certainty for businesses via the European Blockchain Services Infrastructure's (EBSI)[296] network.

[295] J. Pitt, A. Diaconescu, *The Algorithmic Governance of Common-Pool Resources,* in J. H. Clippinger, D. Bollier (eds), *From Bitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society*, Off the Commons Books, 2014.

[296] "The European Blockchain Services Infrastructure (EBSI) aims to accelerate the creation and delivery of cross-border Blockchain-based services for public administrations and their ecosystems to verify information and make services trustworthy. Created in 2018 by the European Blockchain Partnership (EBP) as a follow-up of a joint declaration at the ministerial level, it is a partnership between the 27 EU Member States and Norway, Lichtenstein, and Ukraine as observers, deploys a network of distributed Blockchain nodes across Europe, supports applications focused on selected use cases, and is the first EU-wide Blockchain infrastructure driven by the public sector. EBSI focuses on developing use cases starting from four broad Use Case families, which all take advantage of the core features of Blockchain technology (immutability, tamper-evidence, decentralisation).
These are:
– Verifiable credentials use cases – verification: Using the internally recognised W3C's Verifiable Credentials standard to ensure interoperability, a self-sovereign information ecosystem is created

Moreover, the Commission funds many research programs,[297] directed to the development of technology and sustainable, interoperable standards.

In the described context, the interaction with the private sector, Academia, and the community of stakeholders is of pivotal importance. The most important actors from

where holders of credentials (claims) can control when and how their credentials are verified using EBSI's ledger to check the accreditation of the issuing entity. Verifiable Credentials make information hard to falsify but easy to verify;

– Track and trace use cases – traceability: Ensuring the integrity and tracing the evolution of data or documents; monitoring of products in the supply chain through their digital passport;

– Trusted data exchange use cases – accountability: Enhancing the implementation of EU policy and compliance procedures between administrations, e.g., for asylum demand management or exchange of VAT numbers for import products, by providing means for secure data sharing among customs and tax authorities (and others);

– IP management use cases – intellectual property: Facilitating right holders' checking and management of intellectual property. Under these four use case families, domain-specific, cross-border use cases were identified and developed by EBSI.

The most advanced Use Cases fall under the Verifiable Credentials family:

– Verifiable Credentials: o Student mobility;

– Education Credentials: A holder (student) can request an educational credential (e.g., diploma) from an accredited issuer (e.g., university) and present it to a verifier (e.g., employer) using their digital wallet. The verifier can instantaneously check the issuing university's accreditation on the ledger. This reduces the time and cost of verification while preserving personal data and preventing forgery.

Worker mobility – European Social Security: Enables the exchange of the PDA-1 document of posted workers, which ensures the transfer of their social security entitlements across borders, and prevents social security fraud. Other Use Case families are also at various stages of development. An overview of some of EBSI's other use cases can be found below:

– Track & trace: o SME Financing: To facilitate new funding sources or funding provisions from different sources, particularly for innovative SMEs. o Product and Document Traceability: This can be used in different areas, like the use of document charactering a product or specific steps in the supply of the product, which can be used for circular economy purposes or to facilitate the management of programmes/projects through the timestamping of documents and checking facilities.

– Trusted Data exchange: o Asylum Process Management: Facilitation of the management of cross-border and cross-authority processes in dealing with asylum applicants.

– IP Management: o EUIPO Anti-Counterfeiting: Helps rights holders to manage their intellectual property along the entire value chain (from manufacturing to distribution). Furthermore, the future evolution of EBSI requires new and improved solutions. In this respect, the European Commission launched Pre-Commercial Procurement (PCP). The PCP aims to go significantly further than what is offered by existing solutions by developing new services for EBSI. The tendering for the PCP started to end 2020, to lead to the deployment of solutions within the next three years." JRC Technical report, *European Landscape on the Use of Blockchain Technology by the Public Sector*, 2022, p. 12-13.

EBSI webpage: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home.

[297] For more details, see: https://digital-strategy.ec.europa.eu/en/policies/blockchain-funding.

those fields are gathered in the International Association of Trusted Blockchain Applications (INATBA)[298] and the European Blockchain Observatory and Forum[299].

From a regulatory standpoint, although to date there are various policy initiatives ongoing in the EU landscape,[300] the European legislator needs to be more open about which aspects of technology to regulate and how to regulate them.

The first relevant initiative is the *Markets in Crypto Assets* (MiCA) Regulation,[301] adopted on 31 May 2023, which is part of the European Commission's Digital Finance Strategy.[302]

The MiCAr aims to build a European regulatory framework for digital assets by 2025.[303] This regulation defines the regulatory treatment of crypto assets not covered

[298] https://inatba.org/.

[299] The EU Blockchain Observatory and Forum is a European Parliament Pilot Project with the financial support of the European Union, https://www.euBlockchainforum.eu/about.

[300] Although not directly relevant to this thesis, we cannot fail to mention the Digital Service Act (Regulation (EU) 2022/2065) and the Digital Market Acts (Regulation (EU) 2022/1925). The DMA focuses mainly on the promotion of a fair and competitive digital market, while the DSA addresses EU concerns about the growing influence of online platforms in political discussions, disinformation campaigns, the spread of fake news in the run-up to elections and the social impact of hate speech. For an interesting analysis of the interplay between the DMA and online users protection, see G. Contaldi, *Il DMA (Digital Markets Act) può contribuire alla protezione dei dati degli utenti online?*, in *Diritti umani e diritto internazionale*, Il Mulino, 2023, pp. 77 – 93; G. Contaldi, *Il regolamento 2022/1925 e la tutela della privacy online*, in *QUADERNO AISDUE, SERIE SPECIALE Atti del Convegno "Ambiente, digitale, economia: l'Unione europea verso il 2030" Bari 3-4 novembre 2022,* Serie speciale, Editoriale scientifica, pp. 119 – 140.

[301] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

[302] "The digital finance strategy sets out general lines on how Europe can support the digital transformation of finance in the coming years while regulating its risks. The strategy sets out four main priorities: removing fragmentation in the Digital Single Market, adapting the EU regulatory framework to facilitate digital innovation, promoting data-driven finance and addressing the challenges and risks with digital transformation, including enhancing the digital operational resilience of the financial system.", https://finance.ec.europa.eu/publications/digital-finance-package_en.

[303] ECB, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures,* Occasional Paper nr. 223/2019, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf?a31360223fb32f0e50a82ce649a8b7fc.

by existing financial services legislation.[304] The crypto assets included in the scope of MiCA are e-money tokens, asset-referenced tokens (stable coins) and utility tokens.
During the definition of its negotiating position, the European Parliament dedicated many discussions[305] to the issue of the environmental impact of mining activities.[306]
The debate was bitter and intense, as some had advanced the idea of banning proof of work as a valid consensus mechanism in Europe. This would have meant the automatic ban of various blockchains, such as Bitcoin, and therefore that proposal met with a heavy backlash from crypto advocates worldwide and eventually not approved.

Another vital part of the Blockchain Strategy is the *eIDAS Regulation*,[307] whose revision was proposed on 3 June 2021. It seeks to create a paradigm shift in the European digital identification of citizens and companies.
To access services, citizens must prove their identity and share electronic documents from their European Digital Identity wallets.
This proposal represents an essential step towards creating a Self-Sovereign Identity framework which gives complete control to the user over their personal information.

[304] See F. M. J. Teichmann, S.R. Boticiu, B.S. Sergi, *The EU MiCA Directive – chances and risks from a compliance perspective*, in *Journal of Money Laundering Control*, 2023; T. van der Linden, T. Shirazi, *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, in *Financial Innovation*, 2023.

[305] https://www.coindesk.com/policy/2022/03/14/proposal-limiting-proof-of-work-is-rejected-in-eu-parliament-committee-vote-sources/.

[306] For more detailed literature on this aspect, see note 120 of this thesis. In addition, one should consider that Blockchain is among the tools that can significantly improve the transparency, accountability and traceability of greenhouse gas emissions; thus it helps companies provide more accurate, reliable, standardised, and readily available data on carbon emissions, see https://digital-strategy.ec.europa.eu/en/policies/Blockchain-climate-action.

[307] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

The proposal for a *Data Act*[308] has to be added to the list of interesting initiatives adopted in the Blockchain field. It was published on 23 February 2022, aiming to ensure fairness in the digital ecosystem, stimulate a competitive market for data and create new opportunities for technological innovation. Smart contracts undoubtedly perform this task, which smooth data sharing while offering adequate technical data protection. Chapter VIII, more concretely, article 30 of the proposal, addresses smart contracts by laying down essential requirements and standards for deploying them under EU rules. The idea is that defining harmonized requirements will promote interoperability[309] and facilitate the use of smart contracts by providing users with guarantees about the respect of legal requirements.

Furthermore, the Commission launched a regulatory sandbox[310] in order to bring together regulators, firms, and tech experts to evaluate innovative solutions, trying to identify their opportunities and risks and create cooperation between the EU and national lawmakers with companies. The goal is to remove legal uncertainties for projects included in the sandbox, such as EBSI use cases and other Blockchain applications.

[308] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.

[309] The European Interoperability Framework (EIF) is the guiding document for creating interoperable solutions and public services. It gives recommendations on four levels of interoperability: legal, organisational, semantic and technical. In November 2022, the European Commission developed the Interoperable Europe Act, which aims to ensure a consistent EU approach to interoperability, establish an EU-wide interoperability governance structure, and set up an ecosystem of interoperable solutions for public administrations. Chapter 3 of the Act defines measures to support innovative solutions. INATBA and EBSI play an essential role in ensuring interoperability.

[310] "Starting in 2023, the sandbox will annually accept cohorts of 20 blockchain use cases. They will be matched with relevant national and EU regulators for a safe and constructive dialogue on the most relevant regulatory issues. Use cases will be selected on the basis of the maturity of the business case, legal/regulatory relevance and their contribution to the EU's wider policy priorities. Every year, the most innovative regulator participating in the sandbox will be awarded a prize. The sandbox is facilitated by a consortium under the lead of Bird & Bird with its consulting arm OXYGY and blockchain experts of WBNoDE. The selection and award process will be overseen by a panel of independent academic experts from European universities.", https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project.

Conclusively, as the last point of this overview, we already mentioned the proposal for a "Pilot regime for market infrastructures" wishing to settle transactions of financial instruments in crypto-asset form.

In the list of interesting initiatives adopted at the European level, the much-awaited Guidelines on Blockchain of the European Data Protection Board (EDPB) need to be included. By the end of 2022, they were expected as part of the III Pillar "A fundamental rights approach to new technologies" within the EDPB Work Program 2021-2022.[311] After more than a year of silence, discussion on the subject seems to have recently been resumed within the EDPB. [312]

Although the action of the EDPB is limited to the right to data protection, it is worth mentioning the work of this Body and the Guidelines as a powerful tool to outline a techno-legal framework for Blockchain. Being a soft-law instrument, the Guidelines only leave users with guidance, but, at the same time, they are not as stringent as a legislative act that, as discussed, at this stage, might risk limiting the development of technology.

This section was essentially devoted to the state of the art of the European legal framework for Blockchain. What has emerged from this overview is that the target of Academia has been shifting toward the technology supporting cryptocurrencies. The European legislator, instead, upheld by the work of many Financial Institutions,[313] is still focused on the financial implications of Blockchain.

[311] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf.

[312] According to the Agenda of the plenary meeting of 14 November 2022, the technical group was supposed to discuss the guidelines,
https://edpb.europa.eu/system/files/202211/20221114_plen1.2agenda_public.pdfo

[313] The reference is to the entry of major traditional players into offering Digital Asset Custody services, such as State Street, NASDAQ, and BNY Mellon.",
https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

The previous sections have addressed the question of whether principles and practices from the past should be considered or if new regulatory techniques should be developed to confront the innovation introduced by Blockchain. The answer was that old techniques could only be applied to this new reality by adapting them; at the same time, practices from the past could represent an essential sample for future regulations.

One of the main problems of the framework designed by the European legislator is that, besides trying to eradicate some elements of this technology, it aims to regulate a new technology with old technology and mindset.

Taking the MiCA Regulation as an example, there are parts where there is excellent regulation imposed on cryptocurrencies to safeguard potential investors and consumers about the risks of investing in them and protect consumer rights in case of Crypto-Assets Service Providers (or "CASPs") insolvency or loss of funds. Likewise, some parts of this Regulation run counter to the nature of Blockchain technology and its feature of an open and permissionless network that compels innovators to ask for permission before deploying their products. Therefore, the European Securities and Markets Authority and the European Banking Authority can stop a token or coin from launching if they deem it a 'threat' to financial stability.

It may be that banks, Institutions and politicians see Blockchain as a threat to their position.[314] Nonetheless, its potential – that resides in the power of decentralization - should not be stifled by trying to centralize it.

It is too early to evaluate whether the mentioned proposals will yield positive effects.

[314] The European Central Bank clarified: "Since Bitcoin appears to be neither suitable as a payment system nor as a form of investment, it should be treated as neither in regulatory terms and thus should be legitimised. Similarly, the financial industry should be wary of the long-term damage of promoting Bitcoin investments - despite the short-term profits they could make (even without their skin in the game). The negative impact on customer relations and the reputational damage to the entire industry could be enormous once Bitcoin investors have made further losses." U. Bindseil, J. Schaaf, *Bitcoin land's stand*, The ECB Blog, 30 November 2022, https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog221130~5301eecd19.en.html.

In general terms, what is emerging is a lack of legal certainty[315] and a fragmented framework which is even more evident in the relation with the GDPR and the protection of data rights, as its governance provisions do not always comply with EU principles.

Consequently, the uncertainty of some technical elements is reflected in the interpretation and application of the legal framework.

Another element to consider is that the described framework will only apply in a few years. Given the speed at which technology is evolving, will it still be valid then?

So far, it is not possible to contemplate a reasoned answer as there is no certainty concerning either the technology or the legal framework.

If the European legislator's approach cannot be regarded as a masterly example of balancing legal certainty and technological innovation, some interesting observations can be formulated for Malta.

What has been developed by the State of Malta leads to the question: *is it necessary to develop ad hoc regulations and should an ad hoc legislator be created?*

Besides the opportunity of creating an *ad hoc* legislator, the state of Malta represents the prime example[316] where regulators emphasize technological aspects of DLT and cryptocurrencies, encouraging the use and adoption of solutions in order to safeguard end users and investors and providing technology assurances.

[315] "The lack of a clear and forcefully implemented regulatory framework is increasing uncertainty and probably prevents institutional actors from entering the market and providing the crypto ecosystem with additional liquidity, which would eventually reduce volatility." Kiel Institute for the World Economy-EU, 2018, p. 17.

[316] "Malta has been called 'the Blockchain island' as it has been one of the first countries in the world to have a comprehensive regulatory regime for crypto assets since 2018. The country has made significant progress in the past 2 years as it became the first to install a Blockchain-based IP Register and transfer 60 000 records using the Blockchain network. In addition, the Malta Gaming Authority has recently announced a digital asset-focused sandbox, while the Malta Digital Innovation Authority launched a Technology Assurance Sandbox.", https://www.euBlockchainforum.eu/news/eu-Blockchain-ecosystem-latest-developments.

In a nutshell, the first policy action carried out by Malta was to create a new regulator, the Malta Digital Innovation Authority (MDIA),[317] for *innovative technology arrangements* (ITAs), defined to be *"the intrinsic elements including software, codes, computer protocols and other architectures which are used in the context of DLT, smart contracts and related applications...as may be further defined in the Innovative Technology Arrangements and Services Act*."

Interestingly, the Authority was not set up to regulate cryptocurrencies or digital assets but to address technology arrangements constituting Blockchain, other DLTs or smart contracts. The reason behind this decision was that the Government of Malta recognised that once deployed, Blockchain can cause a breach of the law – above all, data protection law and anti-money laundering.

Consequently, the Innovative Technology Arrangements and Services Act (ITASA)[318] was adopted. It introduced the initial licences for which one could apply voluntarily since the technology deployment had even been assimilated into the freedom of expression. The Act offers certification to developers of an innovative technology arrangement, which should provide a level of trust in the market.

Basing this system on the developer's voluntary choice is appropriate as it addresses two issues. The first is that the overall concept – a developer going to a State Authority asking for a quality check - is something new. Second, the natural consequence is more guarantees for buyers of the software and, therefore, for consumers.

Given Blockchain's nature, which limits the ability for software and/or data errors to be rectified, the framework established by the government of Malta provides for a

[317] Malta Digital Innovation Authority Act (MDIAA), Chap. 591, Laws of Malta, set up in 2018, having as its explicit purpose "to promote consistent principles for the development of visions, skills, and other qualities relating to technology innovation, including distributed or decentralised technology, and to exercise regulatory functions regarding innovative technology, arrangements and related services and to make provision concerning matters ancillary thereto or connected therewith."

[318] https://legislation.mt/eli/cap/592/eng/pdf.

technology assurance regulatory environment which is voluntary for sectors or applications deemed to be low-risk.[319]

Since Malta is a Member State of the European Union, one could ask whether these initiatives might lead the European legislator to apply some of these provisions and create a more harmonised legal framework for Blockchain.
The EU legislative proposals presented in the previous pages are based on Article 114 TFEU, which confers on the European institutions the competence to lay down appropriate provisions for the approximation of laws of the Member States that have as their objective the establishment and functioning of the internal market.
The aim is to remove obstacles to the internal market for financial services and improve its functioning by ensuring that the applicable rules are fully harmonised.
In other words, the European legislator could exercise much more substantial and broader power by dispelling the legal uncertainties that, despite various open and ongoing initiatives, have the effect of holding back Blockchain development in Europe.

This paragraph was intended to present current European legislative initiatives to show the lights and shadows of the traditional regulation approach. However, besides regulatory guidance, two other policy options may play an essential role: *self-regulation* and *multi-stakeholder co-regulation.*

[319] I. H.Y. Chiu, *Regulating the Crypto Economy: Business Transformations and Financialisation*, Hart Publishing, 2021.

4.4.Does Blockchain technology have what it takes to self-regulate?

It is beyond question that one of the most notable highlights associated with Blockchain is its capacity to diminish the need for central authorities through self-regulatory capacity, meaning that it operates according to coding rules.

Before investigating the efficiency of self-regulation within the Blockchain context, a general definition of self-regulation is deemed necessary.

As Price and Verhulst argue, "there is no single definition of self-regulation that is entirely satisfactory, nor should there be"; furthermore, self-regulation "rarely exists without some relationship between the industry and the state".[320]

Interestingly, Julia Black referred to self-regulation as 'decentred regulation', which is no longer "tied exclusively or even predominantly to the state".[321]

In the EU context, self-regulation is "the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at the European level (particularly codes of practice or sectoral agreements)".[322]

The first initiatives for self-regulation and co-regulation initially focused on three areas: technical standardisation, professional rules and social dialogue.[323]

[320] M. Price, S. Verhulst, *In search of the self: charting the course of self-regulation on the Internet in a global environment,* in C. T. Marsden, *Regulating the Global Information Society*, Routledge, 2000, p. 58.

[321] J. Black (2002), p. 27.

[322] European Commission, Interinstitutional Agreement on Better Law-Making [2003] OJ C 321/ 01, para 22; this document is no longer in force as it was replaced by the Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making, OJ L 123, 12.5.2016, p. 1–14, which does not contain any reference to self-regulation.

[323] While technical standardisation and professional rules will be explored in the following, for what concerns social dialogue, it is worth recalling that "European self-regulation and co-regulation have also become established between social partners. At the inter-sectoral level, the foundations for this were laid by the social dialogue encouraged by European Commission President Jacques Delors (the so-called Val Duchesse meetings), which resulted in a series of joint declarations by the European social partners. Subsequently, the Maastricht Treaty formally recognised the contractual role of the social partners at their express request. Among other things, this provided a special procedure for consulting the social partners – at the sectoral or inter-sectoral level – before embarking on Community legislation on social matters. Such consultation could result in contractual agreements between them instead of

Regarding regulating technology, standards are essential to success in creating a pathway to mass adoption. Blockchain makes no exemption.

In the standards community, the European Commission actively engages and works with relevant bodies worldwide.

In drawing common standards, which are covered mainly by self-regulation by the parties involved, the European legislator took on the role of defining the essential requirements for guarantying harmonization of the European values (namely, health, safety, consumer protection, environment) while delegating the technical specifications to the standardisation bodies that had signed a contract with the Commission. European standards are settled by European committees that consider different interests (e.g., producers, sellers, consumers, public authorities, and research institutions).

The technology standards landscape is complex, covering many supra-national, national and industrial organisations.

Some of the more important organisations include the European Standardization Organizations (ESO), supra-national and industry organizations like ISO,[324] Open Standards bodies like IEEE[325] and the International Association of Trusted Blockchain Applications (INATBA)[326] which contributes to the standards discussion on a European and global level.

regulation. At their request, such agreements between social partners can be ratified by the Council, acting on a proposal by the Commission, and thus take on the force of law." Cfr. European Economic and Social Committee, *European Self- and Co-Regulation*, p.13.

[324] ISO (International Organization for Standardization) is a worldwide federation of national standards bodies; it is a nongovernmental organization that comprises standards bodies from more than 160 countries, with one standards body representing each member country. ISO members are national standards organizations that collaborate in the development and promotion of international standards for technology, scientific testing processes, working conditions, societal issues and more.

[325] "IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.", see https://www.ieee.org/about/vision-mission.html.

[326] INATBA is the International Association of Trusted Blockchain Applications. The project was originally initialized by the European Commission. Since then, more than 100 companies – from start-ups to corporates – have joined the association. The association is not related to any political party or

The European Committee for Standardisation (CEN), the European Committee for electrotechnical standardisation (CENELEC),[327] and the European Telecommunications Standards Institute (ETSI)[328] need to be enumerated as the European Union has officially recognized them as the three official European Standard Organizations[329] and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level. The standards developed by those organizations can cover many aspects, sometimes not directly linked to the technology itself.

Concerning Blockchain, standards are directed towards ensuring common principles on interoperability, security, governance, smart contracts and identity.

group. The administrating board of directors is solely set by people who are working in company. INATBA aims to be a global movement and to attract members from all over the world.

[327] The Commission organised a policy workshop on Blockchain standardisation on 12 and 13 of September 2017 and participated in and followed up the standardisation activities related to Blockchain and Distributed Ledger Technologies carried out by the different Standard Developing Organisations, such as ISO, ITU-T, ETSI or CEN-CENELEC, to engage in and contribute to the development of the future standards. CEN and CENELEC have established a Focus Group on Blockchain and Distributed Ledger Technologies. The first objective of the Focus Group has been to identify specific European standardisation needs (for example, in the context of EU regulations such as GDPR and eIDAS), to map these standardisation needs with the current work items in ISO/TC 307 and to encourage further European participation in ISO/TC 307. On 20 September 2018, the Focus Group developed a White Paper entitled 'Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies'[327] and presented it for consideration to ISO/TC 307.
Interestingly, the Working Group highlighted some issues that should be the subject of particular attention in the definition phase of the technical rules. Particularly, the white paper highlighted that the new standards must guarantee the protection and integrity of personal data, interoperability, and cross-border information sharing and harmonize with the European regulation on digital identity (eIDAS). Based on the recommendations presented in the mentioned white paper, a new Joint Technical Committee JTC19 on Blockchain and Distributed Ledger Technologies was launched in order to identify and adopt international standards already available or under development and pay attention towards specific European legislative and policy requirements supporting the development of the EU Digital Single Market.

[328] ETSI is an independent, not-for-profit, standardization organization in the field of information and communications which supports the development and testing of global technical standards for ICT-enabled systems, applications and services, https://www.etsi.org/.

[329] See Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, L. 316/12.

Regarding the issue of *interoperability,* the aim is to ensure that different Blockchain protocols can exchange data and communicate consistently with each other; for *security,* the purpose is to ensure a trusted communication of nodes, networks and services; *governance*[330] to establish the best practice and standards in managing Blockchain projects and safe and secure use of *smart contracts;* ultimately, common standards on *identity* are directed to promote a common identity framework and/or interoperable identities among different Blockchain platforms.

Consequently, in the Blockchain environment, self-regulation by the mentioned committees is directed at creating a common set of standards and values for those elements.

Regarding self-regulation, codes of conduct, usually supported by the social partners of the sectors involved (e.g., liberal professions), should be included. In this respect, in the last two decades, a broad range of professional activities has been the subject of this form of self-regulation, which undoubtedly facilitates the implementation of the principle of mutual recognition.

In the Blockchain context the creation of codes of conduct as well as guidelines for participants within a given ecosystem may facilitate seamless operations and ensure transparency and security for the system in question. They, in turn, provide trust for users who operate in the spirit of not being subject to malicious elements in the system or beyond.

As it has been for cloud computing, codes of conduct and certification mechanisms may represent an essential means to achieve legal certainty, especially around GDPR compliance, and ensure a higher cohesion with the objectives of the Regulation.

[330] With the aim of "provid[ing] guiding principles and a framework for the governance of DLT systems [and] guidance on the fulfilment of governance, including risk and regulatory contexts, that supports the effective, efficient, and acceptable use of DLT systems", ISO adopted the 'Guidelines for governance', available at https://www.iso.org/standard/76480.html?browse=tc.

Article 40 of GDPR envisages the creation of codes of conduct by associations and other bodies that represent categories of data controllers or processors. Article 42 of GDPR also encourages data protection certification mechanisms to be settled in the form of special seals and marks to demonstrate compliance with the Regulation.

Although establishing those codes of conduct and certification mechanisms will not remove the need for a case-by-case assessment, they would still represent valuable proof of commitment and essential steps towards ensuring that Blockchains are compliant by design according to the principles of data protection by design and by default.

Furthermore, by applying these codes of conduct and certification mechanisms, data controllers could demonstrate compliance with the principle of accountability,[331] which requires that organisations put in place appropriate technical and organizational measures and be able to demonstrate what they have done and its effectiveness when requested.

This cursory overview of self-regulation tools leads the way to present an analysis of the pros and cons of self-regulation as a feasible regulatory technique in the Blockchain context.

In the first chapter of this thesis, it was submitted that Blockchain technology guarantees secure information distributed among network users and is continually synchronized to ensure immutability and redundancy. Likewise, it offers transparency by making all blocks visible to participants.

Three of the main features of Blockchain need to be highlighted as they render the idea of self-regulation by Blockchain concrete.

First, the possibility of creating contractual relationships through smart contracts.

The absence of intermediary services facilitates transactions by solving the issue of mistrust between parties since the execution of the contract is based on algorithms.

[331] Article 24 of the GDPR.

Moreover, by allowing the transfer of shares, realities, or even documents, smart contracts make applications of Blockchain possible beyond the financial sphere.

Second, Blockchain allows a free flow of information through decentralization. A peculiarity of Blockchain is that it breaks down the information asymmetry, which is typical of centralized systems. Therefore, it allows participants within a network to control their personal data.

Third, it establishes an accountability framework whereby its transparency criterion helps mitigate malicious behaviour and incentivize good behaviour. All participants can keep track of transactions without relying on a third-party intermediary or a centralized record-keeping. Accordingly, such characteristics could enforce Blockchain's regulatory capacity.

The option of self-regulation is extremely interesting but, simultaneously, very complex and, to understand its potential, other considerations need to be drawn.

From the previous sections, it emerged that since Blockchain can be independent of third parties, it could support itself independently. To do so, a code acting as law must restrain activity, contractual obligations self-imposed through a service provider's terms of service, privacy policy, and other consumer-directed documents.[332]

Likewise, the previous sections, devoted to the debate concerning Cyberspace, helped define the similarities between the Internet and Blockchain, notably, as species of self-regulation, the prevailing approaches to Blockchain regulation match paradigms of Internet regulation.

> "Given the competing societal interests in controlling content on the Internet, meaningful and effective self-regulation is more effective than the exclusive exercise of government authority. Self-regulation has a greater capacity to adapt rapidly to quickening technical progress and to the transnational development of the new communications medium. In addition to flexibility, self-regulation presents the benefits

[332] R. Bollen, *The Legal Status of online currencies: are bitcoins the Future?,* in *Journal of Banking and Finance Law and Practice,* 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247.

> of greater efficiency, increased incentives for compliance, and reduced cost. A carefully structured programme of self-regulation, often developed in co-operation with government, is in harmony with the new technology, mirroring the Internet itself as a global, essentially private and decentralised network of communication."[333]

Therefore, applying self-regulation to Blockchain is deemed legitimate, given the precedent set by the Internet.

Similarly, the European Commission has advocated self-regulation in the context of the Digital Single Market. Regarding data porting, self-regulatory measures are encouraged "in the form of Union codes of conduct which might include model contractual terms and conditions."[334] Accordingly, high expectations are placed on self-regulation and standardization as valuable means of regulation.

Besides the beneficial similarity with the Internet, a key aspect to consider is Blockchain's decentralized and distributed nature, which renders self-regulation the most realistic regulatory option to conform to different contexts beyond formal regulatory boundaries and jurisdictions.

In the Blockchain landscape, self-regulation is accompanied by a risk-celebration narrative as perfectly condensed by Rachel Botsman:

> "[e]very innovator wants to be first over the line, and it's no different with the quest for the ultimate Blockchain technology. Inevitably, there will be glitches along the way because that's how innovation comes into being and grows resilient, just as a body develops its immune system by being exposed to bugs and viruses. The Blockchain's enormous potential means developers and investors are taking a classic 'fail fast, fail forward' approach."[335]

[333] Ivi, p. 75.

[334] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 *on a framework for the free flow of non-personal data in the European Union*, *OJ L 303 p.59-68,* recital 30.

[335] R. Botsman, *Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart*, 2017, London: Portfolio Penguin.

Price and Verhulst[336] argue that self-regulation is crucial in the technology domain, while Reyes[337] believes that self-regulation cannot solve market failures.

It might indeed induce fragmentation, particularly in the case that "an essentialist approach to self-regulation would require that all the elements of regulation – formation of norms, adjudication, enforcement and others – be self-generated". [338]

Notably, from the perspective of EU Law, self-regulation might strengthen fragmentation in the technology domain and, therefore, make it impossible to create uniform regulatory standards; the lack of regulatory standards caused by self-regulation might lead to determining *ad hoc* rules based on a case-by-case analysis.

While this research submits that a case-by-case analysis is deemed necessary for evaluating Blockchain compliance with data protection law,[339] the same cannot be stated for the regulatory aspect of the technology. Such a theory would undermine the principle of legal certainty, which requires regulatory guidance. For what matters here, the notion of legal certainty has been recognised as a general principle of EU law.[340] It is without any doubt one of the cornerstones of a democratic society that abides by the rule of law as it protects legal and natural persons from arbitrary action by the State and helps guide individuals away from breaking the law.

Legal certainty mandates that the law must be clear and precise and that its legal implications are foreseeable.[341] In other words, it requires regulatory guidance from the regulator or the judicial power.

[336] M. Price, S. Verhulst, *In search of the self: Charting the course of self-regulation on the Internet* in C. T. Marsden (edited), *A global environment. Regulating the Global Information Society*, London: Routledge, 2000, pp. 57–78.

[337] "History intimates that the self-regulatory approach is unlikely to sufficiently resolve the market failures that will ultimately allow illicit and fraudulent uses of decentralized technologies to occur.", C. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: an Initial Proposal* in *Villanova Law Review*, Vol. 61, No. 1, p. 194.

[338] *Ivi*, p. 58.

[339] See *infra* Chapter III.

[340] See e.g., I. Lifante-Vidal, *Is Legal Certainty a Formal Value?*, in *Jurisprudence, 2020,* p. 456.

[341] See e.g., Case C-72/10, *Criminal proceedings against Costa*, para 74; Case C-201/08, *Plantanol GmbH & Co KG v Hauptzollamt Darmstadt*, para 46. Please note that the Court decided in Case C-110/03, *Belgium v Commission*, that "a degree of uncertainty regarding the meaning and the scope of a rule of law" was

This is extremely important since the boundaries between the worlds of legality and illegality regarding Blockchain technology and all its applications still need to be delineated.

Furthermore, self-regulation would also undermine the principle of harmonization of EU law, which is mainly required to guarantee the internal market's functioning.[342] Pursuing harmonized interpretation of legal terms within a legal system is not unique to EU law. However, what sets the EU legal order apart from national legal orders is that divergent interpretations are less likely to occur within a single legal order (where the national supreme court may correct lower courts), but rather between different legal orders of Member States. In such cases, the discrepancy goes beyond theoretical aspirations for legal unity. It can result in divergent treatment of individuals subject to the relevant rules, depending on the Member State in which they are located. This would overall frustrate the efficient functioning of the internal market.[343]

It has also been recognized that, when it comes to self-regulation, a key challenge is understanding how regulation must be deployed to be perceived as legitimate.[344]

"inherent in that rule", and that the Court's control could be "confined to the question whether the legal measure at issue displays such ambiguity as to make it difficult for that Member State to resolve with sufficient certainty any doubts as to the scope or meaning of the contested regulation". See for a detailed analysis, J. van Meerbeeck, *The Principle of Legal Certainty in the Case Law of the European Court of Justice: From Certainty to Trust*, in *European Law Review*, 2016, p. 282.

[342] The ECJ defined the internal market as an "economically integrated entity with a single market, based on common rules between its members", case C-351/08, *Grimme*, para 27, in the context of the refusal of Switzerland to accede to the EEA.

[343] In the Hauer case on the internal market and fundamental rights, the Court held that the "introduction of special criteria for assessment stemming from the legislation or constitutional law of a particular Member State would, by damaging the substantive unity and efficacy of Community law, lead inevitably to the destruction of the unity of the Common Market and the jeopardizing of the cohesion of the Community", see case 44/79, *Hauer*, para 14; see also case C-399/11, *Melloni*, para 60; case C-206/13, *Siragusa*, para 32.

[344] Interestingly, Brownsword and Goodwin defined legitimacy as "one of the oldest concepts in political theory". Furthermore, they add that "[i]t concerns questions of justification of the exercise of power by those over whom that power is exercised. Political legitimacy can be classified into two dimensions. The first concerns the source of authority, or how the government has come to be in power. For example, we no longer accept as legitimate a government that has come to power by deposing a democratically elected government in a military coup. Similarly, we do not accept a government as legitimate where it is imposed by a foreign occupying power. Rather, we generally hold that the source of authority for a government is the will of the people, its self-determination, however that might be

At this stage of technology's development, information asymmetry still represents an essential obstacle for the parties involved in the regulation, given that expertise in the domain is scarce, and individual actors do not have the required knowledge to build a comprehensive and efficient regulation.

In light of the above, we can infer that pure forms of self-regulation are undesirable as they may jeopardize some rights and interests of people not involved in the regulation process. Conversely, the European Commission should encourage and facilitate forms of self-regulation concerning not essential aspects of the legislative acts. This is the approach conceived and adopted by the European legislator regarding AI Regulation. Although any parallelism must consider the technical differences and technological advancement of AI and Blockchain, it can nonetheless be viewed as a valid sample of lawmaking technique which, it is worth emphasizing, as well as Blockchain could have (with already tangible evidence) considerable effects in many fields of knowledge.

4.5.Unity is strength: is co-regulation the key?

The previous sections have tried to shed light on the advantages and disadvantages of top-down legislation (also known as command-and-control) and self-regulation.

To highlight the cons of these regulatory techniques, it is worth recalling that command-and-control does not solve the dilemma of not stifling innovation. At the same time, self-regulation must have public oversight to adequately meet the needs and protect citizens' rights and interests.

expressed or measured. Where the source of power is illegitimate, the exercise of power of what the (illegitimate) government then does once in power is also deemed illegitimate, even were it to be generally perceived as acting for the social good.", see R. Brownsword, M. Goodwin (2012), p. 173.

This thesis has repeatedly argued that there is no best regulatory technique; instead, there are different regulatory designs for different institutional settings and problems.

The current section is intended to present another approach to regulation: the multi-stakeholder/co-regulation method,[345] which, in our opinion, could represent the right balance between the risk of stifling innovation, on the one hand, and not leaving innovation without guidance, on the other.

This approach unites the flexibility of the self-regulatory system with the public policy objectives of command-and-control legislation.

Blockchain technology has multifaceted dimensions that would benefit from an interdisciplinary approach from developers, lawyers, policymakers and scholars.

Blockchain essentially advocates for a legal framework that offers *"sufficient flexibility to accommodate innovation"*.[346] Therefore, it implies that the technology would benefit from conversations from many different disciplines and previous experiences.

Unlike self-regulation, the multistakeholder method is shaped to protect public policy objectives. Public authorities are involved in the regulatory process; thus, the action of private actors[347] is counterbalanced by public oversight.

Another aspect to consider is that the involvement of many actors can help manage information asymmetry, which often represents an issue in the context of rapid

[345] See, M. Gurstein, *The Multistakeholder Model, Neo-liberalism and Global (Internet) Governance,* in *Gurstein's Community Informatics,* 26 March 2014. It is important to note that this method was also endorsed by Don Tapscott and Alex Tapscott: "We believe effective regulation and, by extension, effective governance come from a multistakeholder approach where transparency and public participation are valued more highly and weigh more heavily in decision making. For the first time in human history, nonstate, multistakeholder networks are forming to solve global problems", see D. Tapscott, A. Tapscott (2016), p. 298.

[346] Declaration of Amsterdam, *Cooperation in the Field of Connected and Automated Driving*, 14 April 2016, point II.a.

[347] The key is to find a balance so that private actors do not exercise too much power at the expense of the protection of individual rights. See L. Belli, P. A. Francisco, N. Zingales, *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police*, in L. Belli, N. Zingales (eds), *Platform Regulations: How Platforms Are Regulated and How They Regulate Us,* FGV Direito Rio, 2017, p. 41.

technological development. Some actors involved can be at the forefront of the developing process and have helpful information to direct the innovation processes. Furthermore, this regulating method guarantees the flexibility necessary to experiment in fast-changing contexts as it draws on different areas of expertise and experience, from the government to business, as well as broader public discourse.

The multistakeholder approach has already been adopted regarding the Internet[348] and it may be also used to regulate Blockchain giving the interesting similarities between them. Whereas the Internet democratized information, the Blockchain democratizes value and cuts to the core of traditional industries like banking. Therefore, the Internet governance model may represent a good template as long as the protection of users is ensured (i.e. cutting the middleman does not entail not protecting consumers and citizens).[349]

As it was for the Internet, also Blockchain needs adaptive legal frameworks grounded on a principle-based approach "that provides for cooperation among Member States, as well as self-regulation, should ensure that the framework is flexible enough to take into account the evolving needs of users, service providers and national authorities in the Union. In order to avoid the risk of overlaps with existing mechanisms, thereby avoiding higher burdens both for Member States and businesses, detailed technical rules should not be established."[350]

All the above considered, co-regulation requires constant revision and evaluation of regulatory principles to adapt them to new needs.

[348] The E-Commerce Directive has been portrayed as a co-regulatory legal framework as it entrusts the private sector with the enforcement of norms on the Internet, see B. Frydman, L. Hennebel, G. Lewkowicz, *Public strategies for Internet Co-Regulation in the United States, Europe and China*, in E. Brosseau, M. Marzouki, C. Méadel, *Governance, Regulations and Powers on the Internet, Cambridge, Cambridge University Press*, 2008, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1282826; see also B. Frydman, L. Hennebel, G. Lewkowicz, *Co-regulation and the rule of law,* in E. Brosseau, M. Marzouki, C. Méadel, *Governance, Regulation and Powers on the Internet,* Cambridge University Press, 2012, pp. 133-150.

[349] D. Tapscott, A. Tapscott (2016), p. 299.

[350] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union *OJ L 303, 28.11.2018, p. 59–68,* recital 10.

In the previous sections, the 'code-based regulation' method has been presented as a valid form of (co-)regulation that should not overlook the importance of public oversight but pinpoints the relevance of technical rules. But, *what does co-regulation mean in the European legal framework?*

According to the European Commission's position, it is a "mechanism whereby a [EU] legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognized in the field (such as economic operators, the social partners, non-governmental organizations, or associations)".[351]

The collaborative process entails a complex interaction between different actors involved in the definition, execution and implementation of the regulation.[352]

The first step is the definition of legislative standards by the European Union and then their implementation by the private sector.[353]

Considering the EU legal framework, the mentioned regulatory principles must be the result of a process involving a tech power shared among multiple stakeholders who

[351] European Commission, Interinstitutional Agreement on Better Law-Making [2003] OJ C 321/01, para 18.

[352] R. Brescia, *Regulating the Sharing Economy: New and Old Insights into an Oversight Regime for the Peer-to-Peer Economy,* in *Nebraska Law Review 87*, 2016, p. 134.

[353] An interesting example is the approach adopted to address and counter online hate speech.
One of the first steps was the adoption by the European Commission of the Communication 'A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime', which prompted a Council decision to extend the current list of 'EU crimes' in Article 83(1) TFEU to hate crimes and hate speech. Such decision would enable the European Commission, in a second step, to propose secondary legislation allowing the EU to criminalize other forms of hate speech and hate crime in addition to racist or xenophobic motives. The European Commission's policy "toolbox" also includes dedicated exchanges and tools in support of national authorities in the context of the High-Level Group on combating hate speech and hate crime, which has been in function since 2016. Importantly, to prevent and counter the spread of illegal hate speech online, in May 2016, the Commission agreed with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online". In 2018, Instagram, Snapchat and Dailymotion took part in the Code of Conduct, Jeuxvideo.com in January 2019, TikTok in 2020 and LinkedIn in 2021. In May and June 2022, Rakuten Viber and Twitch announced their participation in the Code of Conduct. Implementing the Code of Conduct is evaluated through a regular monitoring exercise in collaboration with a network of organisations in different EU countries. Using a commonly agreed methodology, these organisations test how IT companies implement the Code's commitments. See, B. G. Bello, *Tackling online hate speech from a European perspective: Potentials and challenges of inter-legality*, in *Oñati Socio-Legal Series*, 13(4), 2023, pp. 1376–1411.

need to experiment to guarantee diverse and flexible rules that must be constantly evaluated and, in case, adapted to new needs.[354]

Co-regulation is characterized by two distinctive elements: creating a collaborative environment and a technology-enabled mechanism.

The creation of a regulatory sandbox is a step toward co-regulating Blockchain. This is precisely the path taken by the European Union that, as previously anticipated, recently launched a call for tenders "to contract a consortium to (1) facilitate and operate a pan-European regulatory sandbox for Distributed Ledger Technologies (DLT) in particular Blockchain, and (2) provide comprehensive legal advice on the operation of the core services of the European Blockchain Services Infrastructure (EBSI) and its use cases as approved by the European Blockchain Partnership (EBP).[355]

The aim of the regulatory sandbox is "to foster a dialogue and cooperation between national and EU-level regulators and lawmakers with companies and thus remove legal and legal uncertainties for use cases based on decentralized solutions on Blockchain and potentially in combination with other technologies, such as Artificial Intelligence or Internet of Things."[356]

The most significant merit of implementing sandboxes is that they can create a space that allows innovative ideas to be piloted and new technologies to be tested in virtual or semi-virtual environments.

With regulatory sandboxes, regulators could learn from private sectors through dialogues and understand the real problems. Firms would find it easier and less expensive to comply with reduced requirements, and the process could be quicker and more straightforward than normal processes. This method is, however, not

[354] Although these principles were identified many years ago by Scott and Trubek concerning new governance, they are still relevant today, see J. Scott, D. Trubek, *Mind the Gap: Law and New Approaches to Governance in the European Union*, in *European Law Journal*, 2002, pp. 4–6.

[355]https://www.euBlockchainforum.eu/news/regulatory-sandbox-Blockchain-and-legal-advice-ebsi-production-phase.

[356] Ibidem.

exempt from side effects: sandboxes represent a closer regulator–industry collaboration. They can thus subject regulators to a more significant regulatory capture[357] and further undermine supervisory effectiveness. In the Blockchain context, this could create difficulties for regulators in making proper rules for the industry as interest groups in the sandboxes may take advantage of such rule-making power to protect certain interest groups or the industry as a whole.

Consequently, private distortion of public objectives could occur.

Additionally, it should be considered that there is neither a dependable definition nor a commonly accepted regulatory sandbox model and this could represent a relevant difficulty in setting up an industry sandbox.

Besides these relevant drawbacks, regulatory sandboxes (and co-regulation in general) have the incredible potential to allow for early intervention when technology is in its first phases of development.

The method of co-regulation is productive for all the parties involved. It presents crucial differences compared to the framework created through self-regulation and top-down. The first one leaves little room for discussion as the public power does not have a role in the process, while the command-and-control method requires more advanced state-of-the-art technology.

Eventually, this method contributes to better defining Blockchain governance – different from state governance - and requires constant and recurrent interaction with many stakeholders involved in developing, operating or maintaining a Blockchain system.

[357] It is unavoidable since it depends on constant interaction between industry and regulators, see L. G. Baxter, *Understanding Regulatory Capture: An Academic Perspective from the United States,* in *Making good financial regulation: towards a policy response to regulatory capture,* (Stefano Cagliari ed., 2012), p. 31, 34.

5. Blockchain the regulator

Section 3 of this chapter documented that code's regulatory potential has long emerged through the work of Joel Reidenberg, Lawrence Lessig and, more recently, Primavera De Filippi and Aaron Wright.

This paragraph aims to contemplate the potential of code to serve as a regulatory source. Increasingly, the law is being transformed into code, where code assumes the role traditionally fulfilled by legal frameworks.[358]

This leads us to ask: *What benefits could come from using Blockchain to transpose some laws into autonomous code-based rules?*

Preliminarily, the literature in this domain can help scrutinize the extent to which code can change the law and further prove that developments in distributed ledgers are renovating the law-making process and legal enforcement by creating new means of information enforcing legal requirements.

Academic literature identified ten features of code that contribute to changing the law.[359]

Some of these traits relate to the nature of the language in which law and technology are written: the law is written in natural language, which is ambiguous, the code relies on mathematical models, so it is usually non-discretional; other characteristics could hypothetically affect the code's ability to safeguard democratic values.

It is, for instance, emphasized that law and code act at different times: law enforcement is *ex-post* while technical code is *ex-ante*.

[358] It has been put forward that distributed ledgers are "the strongest challenge ever posed to the monopoly of the state over the promulgation, formation, keeping and verification of institutions and the public record.", see B. Markey-Tower, *Anarchy, Blockchain and Utopia: A Theory of Political-Socioeconomic Systems Organised using Blockchain*, in *The Journal of British Blockchain Association*, 2018, pp. 1-14.

[359] M. Finck (2018), pp. 80-84.

Also, the code can undermine the rule of law, which in democratic societies requires adherence to the principles of transparency, accountability and legitimacy.

Could such essential characteristics be tracked if a law is enforced through code? Doubts are mainly related to the transparency issues of the algorithms.[360]

In addition, the transition from legal code to technical code also requires adaptation concerning procedural safeguards and substantive principles.

If information technologies boost human rights as they are available to everybody, they could become a means of interference, putting human rights at risk.[361] Finally, the issue of jurisdiction merits a reflection. Blockchain, like the Internet,[362] transcends legal and political boundaries. Therefore, whereas governments can influence the code, they can regulate beyond the territorial perimeter of their state.[363]

[360] F. Pasquale, *The Blackbox Society*, Cambridge, MA: Harvard University Press, 2015; W. J. von Eschenbach, *Transparency and the Black Box Problem: Why We Do Not Trust AI,* in *Philosophy and Technology*, *34*(4), 2021 pp. 1607–1622; B. Brevini, F. Pasquale, *Revisiting the Black Box Society by rethinking the political economy of big data* in *Big Data and Society*, SAGE Publications Ltd, 2020; C. Zednik, *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*, in *Philosophy and Technology*, *34*(2), 2021, pp. 265–288; E. R. Petrick, *Building the Black Box: Cyberneticians and Complex Systems* in *Science Technology and Human Values*, *45*(4), 2020, pp. 575–595; A.Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, 2020, pp. 1-16.

[361] See also G. Sartor, *Human Rights and Information Technologies*, in R. Brownsword, E. Scotford, K. Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press, 2017, p. 424 e ss.

[362] "In cyberspace, [the borders] must be understood more flexibly as referring both:
- to the scope of application of regulatory frameworks of sovereign jurisdiction
- and to technological boundaries defined in particular (but not limited to) communication interface control (for example logs and protocols).

In cyberspace, each entity aims to ensure its Digital Sovereignty since it may be at risk in its relationships with other stakeholders. In this context, some characteristics of Digital Sovereignty may be exposed to extraterritoriality. These dimensions involve public interests, understood as all mandatory requirements and core values within a given jurisdiction. Therefore, extraterritorial jurisdiction may (exceptionally) be used to obtain the compliance of external behaviours to domestic public interests and thereby to Digital Sovereignty, with respect for fundamental rights and values.", see CEN/CENELEC, *Workshop Agreement, Digital Sovereignty - European perspectives, general approach, and implications on standardisation*, June 2023, CWA 17995:2023 (E), p. 12.

[363] "Through the copyright regime developed by You- Tube, the platform has become a proxy for the global application of US copyright law. Similarly, until recently Facebook users throughout the world (with the exception of Canada and the United States) were protected by the European Union's data protection regime, given that Facebook processed such data from its European headquarters in Dublin. The non-territoriality of code also means that, in a data-driven economy, economic actors can more

In the EU context, the GDPR serves as a prime example of this phenomenon. While the right to data protection is governed differently across jurisdictions worldwide, processing personal data can trigger the extraterritorial application of jurisdiction's requirements to ensure higher protection. This means that the regulations may extend to data controllers established outside the jurisdiction. This extraterritorial application can be viewed as an embodiment of the entity's Digital Sovereignty,[364] which refers to the country implementing the regulation. The objective is to safeguard data protection rights within its domestic market and protect the digital integrity of its citizens. In the realm of data, the aspect of sovereignty at stake can be described as "personal data sovereignty." This encompasses concepts such as personal data ownership, the right to a secure connection, and, more broadly, adherence to European values and principles in this domain.

Furthermore, within the relevant European framework, this concept of 'bordless jurisdction' is confirmed by what was recently stated by the Council in its conclusions on EU digital diplomacy, which aim to set out priority actions for strengthening the EU's role and leadership in global digital governance. In particular, the Council defined its objectives to address multilateral issues as an integral part of Digital Partnerships and other relevant Dialogues with countries worldwide "to build consensus around EU positions and promote key principles underpinning the EU's own regulatory framework."[365]

easily settle where they want. This explains the stark jurisdictional competition that is emerging in relation to Blockchain-based ventures. It also explains why Lithuania recently created a scheme that seems inspired by the Estonian E-residency programme. It allows for the creation of 'virtual limited liability companies' that can be created remotely and registered and managed through Blockchain technology. When business models centre on data and code, and teams are spread across jurisdictions, firms might simply incorporate where they receive the best deal.", M. Finck (2018), p. 83.

[364] It is the "ability to analyze, decide or act according to a set of values, principles, interests, and goals while managing digital dependencies and risks on digital capabilities.", see CEN/CENELEC, *Workshop Agreement*, cit., p. 8.

[365] *Council conclusions on EU Digital Diplomacy*, 26 June 2023, 11088/23, https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf

This position assumes extreme relevance in the discussion around these topics as it supports our idea to delineate a regulatory solution defined by the Union that is hypothetically applicable beyond its geographical borders.

Moreover, what makes Blockchain different from other technology and allows it to assess its potential as a regulatory technology is the possibility of implementing smart (legal) contracts. [366] As already defined, smart contracts can be used both to incorporate legal provisions into the code and enforce them. This means a smart contract can be part of a binding legal contract or have no connection.

As presented in this chapter, some issues need to be solved to exploit the potential of Blockchain as a regulatory technology.

First, code is not law, and Blockchain cannot replace the legislative process, resulting from a democratic system not followed by the software developers.

Second, it must be guaranteed that specific legal safeguards apply to smart contracts, although not incorporated in the wording of contracts.

Another aspect to consider is that smart contracts are intended to live and operate in the physical world; this entails that to be as effective as traditional legal contracts, the 'on-chain' and the 'off-chain' world must cooperate and be interoperable. Consequently, the work of *oracles*[367] is essential to obtain a sort of 'external validation' and allow these contracts to be effective in the 'real world'. To do so, it might be necessary for smart contracts to comply with specific requirements demanded by a legal framework to enforce a contract under the applicable law.

In a nutshell, the true potential of Blockchain as a new means of transferring data and value can only unfold appropriately if such transfers are recognized by law.

[366] For more interesting reflections, see the report of the Law Commission of the Great Britain entitled *'Smart legal contract – Advice to government'*.

[367] See chapter I, para 5.1. of this thesis.

For instance, it would not be meaningful to transfer the ownership of tokens incorporated in the smart contracts if one could not claim ownership of the corresponding asset in real life.

This observation makes it clear why the results of the first implementations of the use cases developed by the European Blockchain Service Infrastructure are so eagerly awaited. They all have a real-world impact and present a nexus between the on-chain and off-chain worlds; therefore, they must reflect the applicable law.

Through Blockchain, it is possible to 'cryptoregulate', that is, to make laws so that the code performs its technological function and simultaneously incorporates legal norms that governing bodies can implement.

To be effective and take on this role as regulator, Blockchain's regulatory potential should be first recognized by the law, which should then lay down some core criteria to enforce Blockchain's position into the legal framework. These criteria should at least include the respect of the principle of independence, transparency, and fundamental rights.[368]

To have a thorough overview of Blockchain's potential as a regulator, which here has only been hinted at, attention must be paid to developing *decentralized autonomous organizations* (DAOs)[369] that raise essential questions regarding legal responsibility and the 'regulability' of Blockchain in general.

Although the issue of 'regulating Blockchain' has not been solved yet, the prospect of automated legal governance opens novel scenarios, making it evident that it is getting more and more difficult for the law to keep up with technology and that the

[368] Drawing a parallel with product safety certification through certification bodies, it is relevant to note that the proposed AI Regulation (article 39) allows for the possibility of locating these bodies in third countries, subject to a recognition process. These observations carry significance within the framework of the EU cooperative model and align with the principles outlined in the Union's digital diplomacy.

[369] Chapter II, para 4.2.

role of actors (institutional and non-institutional) is increasingly complex and necessary.

6. What does the future hold for Blockchain?

After singling out some of the issues that have emerged with Blockchain and the Law, this chapter retraced the most interesting and popular narratives surrounding this topic.

Starting from the idea of Blockchain as *'alegal'*, reiterating the statements and elements of Cyberibertarianism, at the outset, three policy and regulatory options have been presented: command-and-control regulation, self-regulation, and multi-stakeholder regulation.

Each option may positively impact, effectively tackle some problems, and achieve policy and regulatory objectives. However, these options could not be thorough and perfect, as they all come with certain costs and negative impacts.

The multistakeholder approach is the preferred option. By using sandboxes, it can be possible to create a space that allows new ideas to be piloted and new technologies to be tested in virtual and semi-virtual environments, as might be the case of the EBSI network.

The previous analysis has shown that building a techno-legal framework could counteract uncertainties in the relationship between Blockchain and the law.

This regulatory approach guarantees a substantial interaction between law and this emerging class of technology, which is of pivotal importance.

In particular, technical standards play a crucial role in regulating the application and adoption of technologies across both established and nascent industries.

In practice, the scope of every regulation on this subject needs to include techno-legal requirements that can facilitate its adoption. To achieve this aim, those requirements should incorporate appropriate standards -whose nature should be defined by all the stakeholders - and address the social and economic aspects of the regulation, as well as guarantee the respect of fundamental rights.[370]

In other words, as the essential part of that regulatory framework, standards initiatives and the implementation of specific use cases need to be cognizant of the various factors that impinge upon that analysis.

In this respect, it is essential to consider that fundamental rights may represent a constraint to adopting Blockchain while being seen as the subject of protection through this means. In other words, the strict correlation between technological developments and the protection of fundamental rights has to be clearly understood, as expressly referred to by the recent Proposal of the AI Act.[371]

A general discussion of the area of fundamental rights protection would go beyond the scope of this thesis. Notwithstanding, the following chapters will assess this position by delimiting the analysis to the sphere of the right of data protection to evaluate to what extent Blockchain can be considered a means to guarantee better protection of fundamental rights.

The proposed approach of encouraging regulatory sandboxes and unleashing the potential of Blockchain as a regulatory tool opens many research questions.

Some of them are common to the primary purpose of this thesis, which is to investigate Blockchain from a data protection perspective and has been anticipated in this chapter and will be debated in the following.

[370] See B. Cappiello, *Where is justice taking place? Blockchain technology as a tool to fill a gap*, in *Rivista di diritto internazionale privato e processuale 3/2019*, pp. 652-680; W. Crumpler, *The Human Rights Risks and Opportunities in Blockchain*, Center for Strategic and International Studies, 2021, pp. 1-90; C. Rueckert, *Cryptocurrencies and fundamental rights*, in *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, pp. 1-12; F. G' sell, F. Martin-Bariteau, *The impact of Blockchains for Human Rights, Democracy and the Rule of Law, Council of Europe*, 2022.

[371] See note 189.

Though extremely interesting, other research areas will not be investigated as they are beyond this thesis's scope and might be explored in future research. For instance, it ought to be defined which technological solutions can comply with existing regulatory requirements or provide equivalent types of safeguards to promote existing policy objectives; furthermore, as the use of sandboxes has been encouraged, another question which would merit further investigation concerns the legal and socio-economic limitations of using those tools in the context of Blockchain governance, as well as well as the private international law implications of the use of smart contracts.[372]

Eventually, each question posed in this chapter and its respective answer should probably consider that "[t]here are no spaces of perfect freedom from all constraints",[373] and, therefore, "all we can do is choose between different types of constraints."[374]

It will be up to the legislator and all those involved to assess whether the path that has been taken, which has only been described to a small extent in this chapter, should be pursued or whether a change would be necessary.

[372] ISDA, Clifford Chance, R3, *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology*, October 2020, https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/Private-International-Law-Aspects-of-Smart-Contracts-Utilizing-Distributed-Ledger-Technology-New-York-Law.pdf.

[373] Y. Benckler, *The wealth of networks: how social production transforms markets and freedom*, Yale University Press, 2006.

[374] P. De Filippi, A. Wright (2018), p. 210.

Chapter III

Intertwining Blockchain Technology and Data Protection Law: Enemies for Life?

"Friends don't spy; true friendship is about privacy, too."

Stephen King

1. Introduction – **2.** Data protection as one of the gold standards for Blockchain – **2.1.** Basic terminology - **3.** Legal requirements for Blockchain-based data processing - **3. 1.** Does the GDPR apply to data stored on a Blockchain? – **3.1.1.** The potential for risk identification and the concept of pseudonymity – **3.2.** Personal data on the Blockchain – **3.2.1.** Public keys as personal data – **3.2.2.** Transactional data – **3.3.** The material scope of application of the GDPR - **3.4.** The extensive territorial scope of application of the GDPR– **4.** Data protection concerns with Blockchain: different ontologies – **4.1.** Roles and responsibilities for GDPR compliance in the Blockchain context – **4.1.1.** Interim results and the implications for data protection - **4.2.** Applying the principles of lawfulness, fairness and transparency – **4.2.1.** Consent Management – **4.2.2.** Legitimate Interest **–** **4.3.** How could data subject rights be upheld in the Blockchain context? – **4.3.1.** The right to access – **4.3.2.** The right to rectification – **4.3.3.** Right to erasure through the prism of Blockchain – **4.3.4.** Right to restriction of processing – **4.3.5.** Data controllers' communication duties – **4.3.6.** The right to data portability – **4.3.7.** The right to object – **4.3.8.** Article 22 GDPR and solely automated data processing – **4.4.** Is a Data Protection Impact Assessment (DPIA) necessary? – **4.5.** Could 'redactable Blockchain' solve the challenges in ensuring data subjects' rights? – **5.** Applying questions of jurisdiction in a borderless ideology – **6**. Addressing the Human Rights Impacts of Blockchain technologies - **7.** Blockchain: A Privacy-Enhancing Technology (PET)? **– 8.** Conclusion

1. Introduction

New technological tools have enabled greater data access, and ethical issues have arisen.[375] Among these technological advancements, Blockchain technology has emerged as a disruptive solution for executing business processes in decentralized environments. Scholars and experts have recognized numerous use cases for

[375] J. Andrew, M. Baker, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, *168*(3), 2021, pp. 565–578.

Blockchain beyond its application in cryptocurrencies. Various industries and business sectors have shown growing interest in utilizing distributed ledgers for their operations.

As defined in the previous chapters, Blockchain is an immutable, decentralized and publicly available database geographically spread across multiple nodes with no central administrator or centralized data storage. Any changes to the ledger are reflected in the various copies distributed around the network of peers. Moreover, the use of consensus algorithms to check the validity of the information that a node requires to add to the chain ensures the integrity of the network.

The security and accuracy of the ledger are cryptographically maintained according to the rules agreed upon by the network. This allows for the preservation of data confidentiality. However, some critics suggest that if no additional technical measures are employed to safeguard the confidentiality of online communication, decentralized infrastructure, intended to enhance privacy and independence, could be more susceptible to surveillance and scrutiny from governmental agencies or corporations compared to centralized systems.[376]

In this regard, many legal questions arise,[377] especially: *how should data protection law deal with the developments of this new paradigm?*[378]

At first glance, the core technical features of the Blockchain clash with the regulatory model informing the European Union's (EU) data protection legislation,

[376] P. De Filippi, *The interplay between decentralization and privacy: the case of Blockchain technologies,* in *Journal of Peer Production, Issue n.7: Alternative Internets*, 2016.

[377] A. D. Zetzsche, P. R. Buckley, W. A. Douglas, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain,* in *University of Illinois Law Review* 2017, no. 5, 2017, pp. 1363-1392; P. De Filippi, A. Wright (2018); C. Engels, M. Westermeier, *Blockchain and the GDPR: Conflict or Concordance*?, in *Computer Law & Security Review 34,* no. 6, 2018, pp. 1345-1357; K. Werbach (2016), pp. 839-908; D. Mazières, E. G. Sirer, *A decentralized model for data privacy*, in *Communications of the ACM* 62, no. 6, 2019, pp. 58-66.

[378] F. Zemler, M. Westner, *Blockchain and GDPR: Application scenarios and compliance requirements*, in *Proc. Portland Int. Conf. Manage. Eng. Technol (PICMET)*, 2019, pp. 1–8; A. Giannopoulou and V. Ferrari, *Distributed data protection and liability on Blockchains*, in *Internet Science (Lecture Notes in Computer Science)*, Springer, 2019, pp. 203–211; T. Buocz, T. Ehrke-Rabel, E. Hödl, I. Eisenberger, *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, in *Computer Law Security Review*, 2019, pp. 182–198.

which is the General Data Protection Regulation (GDPR), a far-reaching legislation designed to enhance personal data protection and give individuals greater control over their data.[379]

The GDPR, which today represents a global model for ensuring data protection rights,[380] was adopted on 27 April 2016, and after a two-year transition period, it came into force on 25 May 2018. It replaced the previous European Data Protection Directive[381] and was designed to strengthen and unify data protection for European citizens and empower individuals by granting them more control and certainty over their data when using Internet services.[382]

The GDPR has represented an extraordinary and, in some cases, an unwelcome new reality.[383] The philosophy underpinning the GDPR refers to a centralized ecosystem. The whole Regulation assumes, and almost takes for granted, the existence of a data controller which determines the purposes and means of the data processing and is able to identify, authorize and constantly monitor its data processors. Therefore, there seems to be no room for a decentralized and permissionless approach to data processing in a distributed framework. More interesting is that the GDPR performs several functions that data sovereignty models on Blockchain implement, most

[379] C. J. Hoofnagle, B. van der Sloot, F. Z. Borgesius, *The European Union general data protection regulation: What it is and what it means*, in *Information and Communications Technology Law*, 2019, pp. 65–98.

[380] K. Hjerppe, J. Ruohonen, V. Leppanen, *The general data protection regulation: Requirements, architectures, and constraints*, in *Proc. IEEE 27th Int. Requirements Eng. Conf. (RE*), 2019, pp. 265–275; C. J. Hoofnagle, B. van der Sloot, F. Z. Borgesius (2019); G. Almeida Teixeira, M. Mira da Silva, R. Pereira, *The critical success factors of GDPR implementation: A systematic literature review*, in *Digital Policy, Regulation Governance*, vol. 21, no. 4, 2019, pp. 402–418.

[381] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[382] J. Mc Nealy, A. Flowers, *Privacy Law and Regulation: Technologies, Implications and Solutions,* in *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*, 2015, p. 199.

[383] J. Brown, C.T. Marsden (2013), p. 59.

notably in giving back control of personal data to data subjects,[384] thereby arguably undermining many Blockchain business models.[385]

By restricting the transfer of personal data to Third Countries without adequate privacy protection,[386] the European Union has influenced other regional privacy laws. That determination of 'adequacy' overseen by the European Commission, in practice, requires other states to adequate their internal systems of protection to the one in force in the European Union. [387] The EU's influence in this regard extends far beyond the boundaries of the Union, which thus implies a significant impact of the GDPR for Blockchain use cases that do not expressly, intentionally, or directly involve personal data of EU citizens.

Considering the period between the birth of Bitcoin and the adoption of the Regulation, one might think that the GDPR already contains references to decentralized systems.[388] Instead, although the preparatory work for the GDPR began in 2012, the Blockchain was not considered in the conception of the Regulation, as Bitcoin was its only application and, more generally, the technology was not so widespread to represent an issue or a topic to reflect when the new European

[384] The GDPR has broadened the definition of *consent*, which must be explicit, freely given, specific, informed, and unambiguous. This renewed definition aims to enhance the protection of individual's personal data by ensuring that their consent is obtained clearly and transparently, cfr. para 4.2.1 of this chapter.

[385] Data subjects are granted greater control over their personal data. This includes the right to request information from the data controller on whether their personal data is being processed and, if so, for what purpose and where (art. 15 of the GDPR), cfr para 4.3.

[386] B. Van Alsenoy, R. Heyman, *The GDPR and the free flow of personal data outside the EU: Towards a human-centric approach to international data transfers*, in *Computer Law & Security Review*, 2019, pp. 35-51; M. Wacker, *The EU General Data Protection Regulation (GDPR): Implications for international data flows and the global data protection regime,* in *International Data Privacy Law*, 2017, pp. 67-75.

[387] See for reference art. 46 of the GDPR; J. Wagner, *The transfer of personal data to third countries under the GDPR: When does a recipient country provide an adequate level of protection?*, in *International Data Privacy Law*, *8*(4), 2018, pp. 318–337.

[388] R. El-Gazzar, K. Stendal, *Examining how GDPR challenges emerging technologies*, in *Journal of Information Policy*, Penn State University Press, 2021, pp. 238-275.

legislation on protecting personal data was pictured. Only a few users and nodes were active, and a little personal data was uploaded on the chain of blocks.
Ultimately, the GDPR was designed and shaped in the light of pre-existing and completely different systems, and now it represents a notable manifestation of the Blockchain regulatory conundrum since this technology entails fundamentally novel privacy concerns that need to be addressed.

The GDPR takes a neutral approach since it does not target a specific class of technology but applies to new technologies in general. In this sense, two solutions may be proposed: recommending a revision of the GDPR or asking for more regulatory guidance about how concepts must be applied in a Blockchain context.
Whereas it may seem that Blockchain technology is inconsistent with certain data protection principles outlined in the EU *acquis*, it is essential to note that Blockchain is also a disruptive technology with the potential to be configured in various ways to meet the needs of individuals and organizations. Therefore, the crucial consideration is whether an organization, public or private, needs to use Blockchain technology.

This chapter, following a brief background on the factors that led to the GDPR's creation, introduces the Regulation's primary concepts and examines its implications for Blockchain (section II). Given the rapid evolution of technology, we are aware that there would be a need to reassess the following considerations over time.

To guide the analysis, the table below summarizes the main findings of this research regarding the intersection between Blockchain technology and GDPR.
The articles and recitals of the Regulation cited are used to support the arguments made regarding the data protection implications of this technology.

TOPIC	GDPR ARTICLE/RECITAL	IMPLICATIONS FOR BLOCKCHAIN
Type of Blockchain (private vs public, permissioned vs permissionless)		This entails differences in accountability, material and territorial scope.
Territorial scope	Art. 3(1)/Recitals 22, 23	If the data is stored in multiple locations in and outside the EU, who is the data controller?
Personal data on the Blockchain	Art. 4(1), 6(4), 32; Recital 26	Is it possible to store personal data on the Blockchain, or must it be off-chain?
Lawful processing	Art. 6	Blockchain participants must carefully identify the lawful basis for processing and keep in mind their correlation to data subject rights.
Privacy by design vs Blockchain's core features	Art. 25 – Recital 78	Blockchain runs counter to data minimization, storage limitations and a determined data controller, raising whether it is in line with the principle of 'Privacy by design'.
Right to be forgotten	Art. 17, 6(1)(b,f) – Recital 69	Can data on Blockchain be deleted in compliance with the right to be forgotten? Could the functioning principle take over and allow for specific interpretations of the GDPR, as Blockchain is at its core designed not to be compliant to the right to be forgotten?
Data protection impact assessment	Art. 35	Through append-only function Blockchains often use very sensitive data, resulting in a high risk to the rights and freedom of the data subjects which renders a DPIA mandatory.

Ultimately, the questions that will guide the discussion in this chapter are:

(i) *Is it possible to store personal data encrypted on a Blockchain, and does the level of 'anonymity' provided by encryption render such data exempt from the GDPR?*

(ii) *In what ways does the territorial scope of the GDPR conflict with Blockchain technology?*

(iii) *Who is identified as the data controller and data processor in a Blockchain?*

(iv) *How do GDPR's right to rectification (Article 16) and right to be forgotten (Article 17) clash with Blockchain's immutability?*

(v) *How does GDPR's right to limitation of processing (Article 18) clash with Blockchain's distributed ledger?*

Those controversial points should be read in light of the principles set out in Chapter II, Article 5, of the GDPR that guide the lawful processing of personal data as they[389] are designed to give data subjects greater control over their personal data and ensure that personal data is processed lawfully and transparently.

Notwithstanding, before digging into those issues, it is first essential to delve into a legal analysis of the European data protection legislative framework to shed light on its - more or less - prominent inconsistencies with the technological advancement represented by Blockchain.

2. Data protection: a gold standard for Blockchain

2.1. Basic Terminology

To effectively analyze the GDPR principles, it is essential to comprehend the vocabulary used to describe different entities involved in the flow and processing of personal data.

The "Data Controller" refers to a natural or legal entity, whether public or private, responsible for determining the purpose, method, and specifications of personal data processing.

The "Data Processor" is a natural or legal entity, whether public or private, responsible for processing personal data based on the instructions provided by the

[389] J. C. Cannon, *The EU General Data Protection Regulation: A Primer and Future Implications*, in *Journal of Information Privacy and Security*, 2017, pp. 61-76; P. L. Poullet, *The Principles of the General Data Protection Regulation and the Challenges They Raise*, in *Computer Law & Security Review*, 2017, pp. 267-273.

Data Controller. It is possible for one entity to serve as both the controller and processor of data simultaneously.

"Personal Data" refers to any information that can be used, either directly or indirectly, to identify an individual (i.e. the data subject), such as location data, online identification, name, or identification number.

"Data Subject" refers to a natural person whose personal data is being processed by the Data Controller or Data Processor**.**

For a comprehensive list of basic terminology from the legal and technological domains, please refer to Essential glossary of terms.

2.2.Data protection key principles of data processing

To thoroughly understand the main groundwork of data protection legislation, it is necessary to outline its architectural principles, compliance with which is essential for any data processing that can be said to be legitimate.

Since we will often refer to the Data Protection Directive in a comparative perspective with the GDPR, it is important to note that finding an identity between the Directive and the Regulation is significant in that it makes the principles (in particular those possibly expressed by the Court of Justice) that have matured with regard to the interpretation of the Directive transposable to the Regulation.[390]

[390] Interestingly, we will also refer often to the "Law Enforcement Directive", that is, the EU Directive 2016/680, which is officially known as the "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA." This directive is part of the European Union's data protection framework and sets out rules for the processing of personal data by law enforcement authorities within the EU. It aims to balance the need for effective law enforcement with the protection of individuals' fundamental rights and freedoms, particularly concerning their personal data. The Law Enforcement Directive sets requirements for the collection, storage, and use of personal data by law enforcement agencies, and it includes provisions for data subjects' rights, data protection impact assessments, and the appointment of data protection officers within law enforcement

Article 5 of the GDPR[391] establishes the fundamental principles that form the basis for protecting personal data, which have remained largely unchanged for several decades, including those laid down in the 1980 OECD Guidelines[392] and the 1981 Convention 108.[393] These principles have demonstrated their ability to withstand the test of time and can be applied in various technical, economic, and social contexts. The GDPR does not fundamentally alter these principles but makes certain adjustments and additions.[394]

bodies. It harmonizes data protection rules across EU member states to ensure consistency and safeguard individuals' privacy when their data is processed for law enforcement purposes.

[391] Article 6(1) of the Data Protection Directive (DPD) contained principles almost identical to those in Article 5 of the GDPR. Although it was titled "Principles relating to data quality," it covered more than just data quality and included principles relating to the lawfulness and fairness of processing, purpose limitation, data minimization, the accuracy of data, and storage limitation. These principles were formulated very similarly to those in the GDPR. However, unlike Article 5 of the GDPR, Article 6 of the DPD did not include the principle of integrity and confidentiality, which was logical since this provision was specifically dedicated to data quality, even though certain principles went beyond the matter of data quality. On the other hand, Article 5 of the GDPR has a wider scope, being titled "Principles relating to processing of personal data." Provisions on the integrity and confidentiality of processing were found in Articles 16 and 17 of the DPD. Although no accountability principle was stated as such, Article 6(2) of the DPD clarified that "it shall be for the controller to ensure that paragraph 1 is complied with."

[392] Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23/09/1980 and amended on 11/07/2013, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

[393] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28/01/1981, https://rm.coe.int/1680078b37.

[394] The Court's role was also important in defining the principles of the GDPR. In the Bara case (Case C-201/14, *Bara*, paras. 34 et seq), the CJEU ruled that a public administration must inform data subjects when it transfers their personal data to another public administration to comply with the requirement of fair processing of personal data. The Court has also ruled in Schecke (Joined Cases C-92/09 and 93/09, *Schecke*, paras. 86–89) that a legal obligation to process personal data must respect the principle of proportionality, which is part of the requirement for a legitimate purpose. The CJEU has examined the respect for this principle in several cases, including the well-known Digital Rights Ireland case (Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*), where the Court found that relevant criteria should be established to determine the appropriate data for processing and the time limit for data retention. In the Tele2 case (Joined Cases C-203/15 and C-698/15, *Tele2*, para. 107), the Court went further and stated that legislation requiring general and indiscriminate retention of personal data exceeds the limits of what is strictly necessary and cannot be considered justified. Proportionality considerations are also relevant in the TK case (Case C-708/18, *TK*), where the Court assessed whether video surveillance is excessive or inappropriate under Article 6(1)(e) of the Data Protection Directive, especially when other measures could be taken to protect the legitimate interest in question.

The first principle is the *lawfulness, fairness and transparency* principle,[395] which means that personal data be "processed lawfully, fairly and in a transparent manner in relation to the data subject".[396] This typically means that either the processing is explicitly allowed under the law or the individual whose personal data is being processed has given consent after being informed of the process's reason, context, and purpose.

Article 6(1) of the GDPR outlines the cases when the processing of personal data is considered legal. Processing is only considered lawful if at least one of the following applies: (a) the data subject has given consent for the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary to protect the vital interests of the data subject or another person; (e) processing is necessary for the performance of a task carried out in the public interest or in the

[395] Similar to the Data Protection Directive, the requirement that data processing must be lawful in the GDPR essentially means that it must comply with all applicable legal requirements, such as the obligation of professional secrecy if applicable. However, Article 6 of the GDPR has been renamed "lawfulness of processing" rather than "criteria for making data processing legitimate," as in the previous Directive. This provision outlines the core conditions for processing to be considered lawful. Specifically, Article 6(1) of the GDPR states that processing shall only be lawful if at least one of the conditions it lists applies.

Similarly, Article 8 of the Law Enforcement Directive sets out the conditions necessary for lawful processing in this field. According to the European Union Agency for Fundamental Rights and the Council of Europe, the principle of lawful processing should also be understood with reference to the conditions for lawful limitations of the right to data protection or the right to respect for private life under Article 52(1) of the Charter of Fundamental Rights of the European Union and Article 8(2) of the European Convention on Human Rights. Therefore, for the processing of personal data to be considered lawful, it must be in accordance with the law, pursue a legitimate purpose, and be necessary and proportionate in a democratic society to achieve that purpose.

[396] See, to that effect, judgments of 22 June 2021, *Latvijas Republikas Saeima* (Penalty points), C-439/19, EU:C:2021:504, paragraph 96, and of 24 February 2022, Valsts ieņēmumu dienests (Processing of personal data for tax purposes), C-175/20, EU:C:2022:124, paragraph 50.
See also G. Malgieri, *The concept of Fairness in the GDPR: A linguistic and contextual interpretation*, in *FAT* 2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, pp. 154–166.

exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, especially when the data subject is a child.

In this context, fair processing of personal data means that the data has not been obtained or processed through unfair means, deception, or without the data subject's knowledge. The legislator decided to explicitly include the principle of transparency with the requirement of lawful and correct data processing for clarity. In contrast, before the GDPR, commentators had read the transparency requirement into the notion of fairness. The transparency principle is now explained in recital 39,[397] which states that it should be transparent to individuals that their personal data is being collected, used, consulted, or otherwise processed and that they should know to what extent their personal data is or will be processed. The information provided to data subjects should be of good quality, easily accessible, and easy to understand.

[397] "Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."

Moreover, the fairness principle requires special attention to the clarity of the language used when addressing information, especially to children.

The *purpose limitation principle* is considered a fundamental data protection requirement and a cornerstone of the field. It requires that data be collected for specific, explicit, and legitimate purposes, known as the "purpose specification" dimension, and not further processed in a way incompatible with those purposes, known as the "compatible use" dimension.

The purposes for processing personal data should be determined from the outset at the time of data collection. Processing personal data for undefined or unlimited purposes is illegal because it does not allow the scope of the processing to be clearly defined. Data processing purposes should be unambiguous and clearly expressed rather than kept hidden. Finally, the purposes must be legitimate, meaning that they should not involve disproportionate interference with the rights, freedoms, and interests at stake in the name of the data controller's interests.[398]

Determining what constitutes a legitimate purpose depends on the circumstances, as the objective is to balance all rights, freedoms, and interests involved in each case. This includes the right to personal data protection on the one hand and the protection of other rights, such as the interests of the data subject, controller, or society, on the other

[398] "(…) the purposes of the processing are to be identified at the latest at the time of the collection of the personal data, next, that the purposes of that processing are to be clearly stated and, finally, that the purposes of that processing are to guarantee, inter alia, the lawfulness of the processing of those data, within the meaning of Article 6(1) of Regulation 2016/679.", case C-77/21, *Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, para 27; see also C-175/20, *Valsts ieņēmumu dienests* (Processing of personal data for tax purposes), paras 64 to 66; case C-136/17, GC and Others (De-referencing of sensitive data), para 74; case C-553/07, Rijkeboer, para 33.

C. Burton, L. De Boel, C. Kuner, A. Pateraki, S. Cadiot and S. G. Hoffman, *The Final European Union General Data Protection Regulation,* in *Bloomberg Law: Privacy & Data Security,* 12 February 2016, p. 6.

hand. Processing data for a purpose, which is contrary to the law, cannot be considered as a legitimate purpose.[399]

The second dimension of the purpose limitation principle concerns the compatibility of data processing. Article 6(4) of the GDPR provides a set of criteria to determine whether processing for a purpose different from the original one is compatible with the initial purpose.[400] These include considering the link between the two purposes, the context of data collection, the nature of the personal data, the consequences for data subjects, and the existence of appropriate safeguards.

The GDPR clarifies that processing personal data for a different purpose than the one they were collected is allowed in certain circumstances. The final text of the GDPR softens the purpose limitation principle in cases where the data subject consents to the new purpose or if the processing is based on Union or Member State law.[401]

According to the *principle of data minimization,* personal data must be adequate, relevant, and limited to what is necessary concerning the purposes for which it is processed.[402] This means that data collection should be limited to the essential data

[399] C. Jasserand, *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation*, in *European Data Protection Law Review*, 4(2), 2018, pp. 152–167.

[400] This list is based on the one elaborated by the WP29: see WP29 2013, p. 40.

[401] The Law Enforcement Directive ("LED") also permits data processing by public authorities to prevent, investigate, or prosecute criminal offences, even if the data were initially collected for a different purpose under certain conditions. Certain data reuses are considered compatible, such as further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. These categories of further processing are narrower than before under the previous Directive, while the category of data processing for statistical purposes remains unchanged. It refers to the elaboration of statistical surveys or the production of statistical, aggregated results. Essentially statistics aim at analyzing and characterizing mass or collective phenomena in a considered population. The LED has also introduced the notion of archiving purpose in the public interest but has kept the wording of the Directive and Framework Decision 2008/977/JAI as regards 'scientific, statistical or historical' use. Article 4(3) LED states that processing falling within the scope of this text may include such uses for the purposes of prevention, investigation, detection or prosecution of criminal offences, providing appropriate safeguards for the rights and freedoms of data subjects are put in place.

[402] See to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points),* C-439/19, EU:C:2021:504, paragraph 98; judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*,

needed to provide the offered service or product. Unlike the previous Directive, which envisages this principle, the GDPR uses the phrase *"limited to what is necessary"* instead of *"not excessive"*.[403] However, the two formulations are both attributable to the principle of proportionality and can therefore be substantially overlapped.

In agreement with Recital 39 of the GDPR, personal data should only be processed if other means cannot reasonably fulfil the purposes. This necessity requirement pertains to both the quantity and quality of personal data. For instance, collecting an employee's complete medical file to assess their work capacity would be excessive. Similarly, collecting a single piece of data that would disproportionately interfere with the data subject's rights and interests, such as information about a job applicant's private drug consumption, would also be inappropriate. The "limited to what is necessary" criterion also requires that the period for which personal data is stored is kept to a minimum, as outlined in the storage limitation principle.

The *principle of accuracy* states that personal data should be precise and kept up to date as necessary. Appropriate measures should be implemented to ensure that any inaccurate data is promptly corrected or erased to maintain the data's accuracy.

The previous directive and Convention 108 required data to be accurate and, where necessary, kept up to date. The GDPR maintains this requirement: all inaccurate data should be rectified or erased. The controller must take all reasonable steps to ensure compliance with this accuracy principle, and the GDPR specifies that this intervention must be prompt.[404]

C-708/18, EU:C:2019:1064, paragraph 48; judgment of 24 September 2019, *GC and Others (De-referencing of sensitive data*), C-136/17, EU:C:2019:773, paragraph 73.

[403] The LED maintained the Directive's wording, as Article 4(1)(c) of the LED states that data must be "not excessive." Nonetheless, this difference in terminology is not expected to impact the data minimization principle's scope significantly.

[404] Article 7(2) of the Law Enforcement Directive (LED) requires competent authorities to take all reasonable measures to ensure that inaccurate, incomplete, or outdated personal data is not transmitted or made available. These authorities must verify the data's quality before communication, as far as possible. Article 7(2) LED goes a step further in the field of police activity, stating that necessary

Based on the *storage limitation principle*, personal data should be retained only for as long as necessary to fulfil the purposes for which it is processed.[405] Data can be kept longer if used solely to archive the public interest, scientific or historical research, or for statistical purposes.

The provision regarding the prohibition against storing personal data in a form that permits the identification of data subjects beyond the necessary time to achieve processing purposes remains unchanged from the Directive. However, Recital 39 of the GDPR introduces a new element that encourages controllers to establish time limits for erasure or periodic reviews to ensure that personal data is not kept longer than necessary.[406]

In addition, the storage limitation principle allows for storing personal data for longer periods for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

The essential security requirement is included in the fundamental data protection principles list under the *'integrity and confidentiality'* heading.[407] This principle mandates that personal data must be processed to ensure their appropriate security,

information to assess the accuracy, completeness, and reliability of personal data, as well as their up-to-date status, must be included in all transmissions of personal data, as far as practicable.

[405] It must be carefully considered that even initially lawful processing of data may over time become incompatible with Regulation 2016/679 where those data are no longer necessary for such purposes, see to that effect judgment of 24 September 2019, *GC and Others (De-referencing of sensitive data*), C-136/17, EU:C:2019:773, paragraph 74. Moreover, data must be erased when those purposes have been served, see judgment of 7 May 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, paragraph 33.

[406] Article 4(1)(e) of the Law Enforcement Directive (LED) includes the same prohibition and Article 5 of the LED mandates that appropriate time limits be set for erasure or periodic reviews of the need for data storage. Procedural measures must be taken to ensure compliance with these time limits. Additionally, Article 25 of the GDPR and Article 20 of the LED require controllers to implement suitable technical and organizational measures to ensure that the legitimate storage period of personal data is respected by default. These measures could include setting expiry dates for each set of data.

[407] Article 17 of the Data Protection Directive (DPD) reflects this principle, which is mirrored in the GDPR. Furthermore, the Law Enforcement Directive also contains the same articulation of the principle of integrity of data, which appears in the list of fundamental protection principles (Article 4(1)(f)), and provisions that further develop the security duty in a separate section (Articles 29-31).

including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures. Chapter IV of the GDPR is dedicated to controllers and processors and further develops the duty of security, which includes a new requirement to notify personal data breaches to the supervisory authority and, in certain cases, to the data subjects as well.[408]

The GDPR offers specific guidance on assessing security risks and determining which security measures may be appropriate.[409] Article 32(1) provides a non-exhaustive list of criteria to consider, such as the state of the art, implementation costs, the nature and purpose of the processing, and the likelihood and severity of risks to

[408] See case C-342/12, *Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT)*, see also joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*,.

[409] In 2014, the CJEU seemed to equate data security with the 'essence' of the right to data protection in *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*). In that case, the Court stated: *"Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data."*.

In 2013, the CJEU rendered a ruling on Article 17 of the DPD (which is equivalent to Article 32 of the GDPR) in the Worten case (Case C342/12). Worten, a private company in Portugal, implemented a restricted access system to the working hour records of its staff, which the national authority responsible for monitoring working conditions did not have access to. The Court clarified that an employer, as a controller of personal data, is obliged to provide the national authority responsible for monitoring working conditions with immediate access to the record of working time. However, this does not mean that the personal data contained in the record must necessarily be accessible to unauthorized persons. Thus, the requirement of security of processing under Article 17 of the DPD was not compromised.

The ECtHR has also issued rulings on the adequacy of data security obligations. In the Z v Finland case (ECtHR, *Z v Finland*, paras. 95–96), the Court held that domestic law must provide appropriate safeguards to prevent any communication or disclosure of personal health data that may be inconsistent with the guarantees in Article 8 of the European Convention of Human Rights (ECHR). Furthermore, in the I v Finland case of 2008 (ECtHR, *I v Finland*), the ECtHR ruled directly on security obligations related to data processing. The Court held that Finland violated Article 8 of the ECHR, which guarantees the right to respect for private and family life, as it failed to secure patients' medical data against unauthorized access at a public hospital due to the lack of adequate technical and organizational measures.

individuals' rights and freedoms. Furthermore, this article elaborates on the major risks to be mitigated, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

The GDPR doesn't mandate the use of any specific technology or technical standard for data security,[410] but Article 32(1) lists four types of security measures that controllers and processors should implement as deemed appropriate, including pseudonymization and encryption of personal data, ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems, restoring access to personal data in a timely manner in case of an incident, and regularly testing, assessing, and evaluating the effectiveness of security measures.

While these measures are not mandatory, Article 32 expresses a clear preference for them, making it likely that regulators expect data controllers and processors to use them whenever possible. The criteria for determining whether to carry out a data protection impact assessment (DPIA) pursuant to Article 35 GDPR also show some similarities to the criteria for assessing security risks under Article 32. The WP29 has emphasized the importance of data security in the context of DPIAs.

The list of fundamental data protection principles concludes by stating that the controller is responsible for complying with all the previous principles. Compared to the DPD, the GDPR introduces a new element where the controller must demonstrate that the processing complies with these legal rules, known as *accountability*.[411]

[410] See recital 15 GDPR, explaining that "the protection of natural persons should be technologically neutral and not depend on the techniques used".

[411] The term "accountability" is commonly used in English, with connotations of responsibility, answerability, and good governance. Understanding the term is considered a core issue in political science, as organizations may attempt to be "accountable" in multiple and conflicting senses, leading to what Koppel calls "multiple accountabilities disorder." To address this, Koppel has developed a typology of five accountability concepts: transparency, liability, controllability, responsibility, and responsiveness. See J.G.S. Koppell, *Pathologies of Accountability: ICANN and the Challenge of Multiple Accountabilities Disorder*, in *Public Administration Review,* 65(1), 2005, p. 95-96.

In data protection law, the term ‘accountability’ was originally used in the sense of responsibility, with the controller responsible for ensuring compliance with data protection rules, particularly those on data quality.[412] This meaning can be seen in the original accountability principle in the OECD Guidelines 1980, Article 6(2) of the DPD, and now Article 5(2) of the GDPR. However, its meaning has evolved to a new and more demanding concept of proactive and demonstrable compliance outlined in Article 24 of the GDPR and in the 2013 revision of the OECD Guidelines and Modernized Convention 108. The principle set forth in Article 24 of the GDPR is best understood as a term of art with its own specific meaning, such as "proactive and demonstrable organizational responsibility."

Examining its core statutory and commonly accepted elements in practice is helpful to understand the principle of accountability better. Accountability in data protection involves two key elements. First, controllers and processors must take responsibility for the personal data they handle, as set out in Article 6(2) of the DPD and carried over into Article 5(2) of the GDPR. Second, Article 24 of the GDPR requires controllers to assess and implement appropriate and effective measures to ensure compliance with the GDPR's principles and obligations, which are often referred to as "compliance programs" by the WP29.[413]

The final sentence of Article 24(1) states that the measures implemented by controllers must be reviewed and updated as necessary.[414] The term "appropriate" means that accountability can be scaled, allowing for the determination of specific measures depending on the processing activities, data types, and level of risk to data subjects. The second paragraph of Article 24 further emphasizes the importance of appropriate

[412] See, to that effect, case C-175/20, *Valsts ieņēmumu dienests* (Processing of personal data for tax purposes), paras 77, 78 and 81, and case C-553/07, *Rijkeboer*, ECLI:EU:C:2009:293, para. 48.

[413] Article 29 Working Party, *Opinion 3/2010 on the Principle of Accountability*, WP 173, 13 July 2010.

[414] The Commission Proposal initially suggested that, if proportionate, independent internal or external auditors should verify compliance. While this specific proposal was not adopted, audit remains a key element of the GDPR, as demonstrated in Article 28(3)(h), Article 39(b), and Article 47.

measures, requiring the implementation of data protection policies by the controller where proportionate in relation to processing activities. Good practice dictates that compliance policies should be reviewed regularly and updated following a review or changes in circumstances, such as changes in the organization of the controller, processor, or data recipients, or developments in the law or legal interpretation affecting processing by the controller.[415]

3. Legal requirements for Blockchain-based data processing

The insight into the founding principles of the GDPR was necessary since identifying which principles are involved in the protection of personal data and their actual meaning constitutes the knowledge ground to discern the potential conflict with the characteristics of the Blockchain.[416]

After this overview of data protection principles, one may glimpse why there seems to be a clash between data protection principles and the building blocks of the Blockchain. Distributed ledger technology (DLT), such as Blockchain, has several notable features, including immutability,[417] trustlessness, visibility/transparency, and resilience. While these properties offer potential benefits, they can also pose challenges when complying with data processing principles.

[415] Cfr. P. Balboni, M.T. Barata, A. Botsi, K. Francis, *Accountability and Enforcement Aspects of the EU General Data Protection Regulation: Methodology for the Creation of an Effective Compliance Framework and a Review of Recent Case Law*, in *The Maastricht Law and Tech Lab*, 2019, pp. 103-254.

[416] See P. Balboni, M.T. Barata, *Legal aspects of Blockchain technology*, in *Essentials of Blockchain Technology*, Chapman and Hall, 2019, pp. 293-348.

[417] Blockchains are intentionally designed to make it difficult to modify or manipulate information once it has been recorded on them, which is one of their essential features. Immutable registers are not a novel concept in the legal world; for instance, land registries never remove entries but only add new ones that may invalidate previous ones. The old entries still remain in the registry. The assessment of Blockchain technology must not only consider developments when collecting data but also when processing it, given the immutability of blockchains. The evaluation of the technology must also take into account future developments and the timeframe that needs to be considered, which could potentially be eternity as blockchains are designed to store data permanently.

However, it is also essential in this context to recognize that the GDPR serves two objectives: data protection and the free movement of data. While data protection is designed to serve humanity, innovation also serves humanity. Therefore, balancing innovation with fundamental rights when interpreting the GDPR is necessary because data protection is not an absolute right[418] and should be viewed on the basis of its function in society.

The connection between Blockchain and GDPR is also clearly identified in the Blockchain Strategy of the European Commission, which has been formulated to achieve specific goals while upholding and endorsing unambiguous "gold standards", including but not limited to data protection: *"Blockchain technology should be compatible with, and where possible support, Europe's strong data protection and privacy regulations*."[419] This intention stems from the idea that this issue concerns all Europeans, as the GDPR aims to safeguard European fundamental individual rights, while Blockchain technology seeks to transform basic social, economic, and political structures.[420]

As expected, the GDPR has been widely praised for modernizing certain aspects of the previous data protection framework.[421] The Regulation comprises a range of provisions to enhance privacy and promote privacy awareness across the European Union. With its provisions for informing consumers about the data collected about them, and its requirements for obtaining consent or facilitating data deletion, the GDPR seeks to empower individuals and give them control over their data. This is especially relevant in the growing prevalence of data collection, the emergence of data-driven businesses and business models, and the perception that individuals lack

[418] See Recital 4 of the GDPR. In this sense, see also joined Cases C-92/09 and C-93/09, *Schecke*, para. 48, and case C-268/21, *Norra Stockholm Bygg*, EU:C:2023:145, para 49.

[419] See https://digital-strategy.ec.europa.eu/en/policies/Blockchain-strategy.

[420] The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR*, 16 October 2018, p. 8.

[421] E. Gil González, P. de Hert, *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, in *ERA Forum*, 19(4), 2019, pp. 597–621.

control over their digital footprint. While the ability to opt out of data collection, delete personal data, or control its use are essential rights enshrined in the GDPR, they may conflict with certain business models and digital architectures. In such cases, businesses may be required to change their models to comply with the law. However, when the law clashes with hardware and software design, solutions are less clear and different perspectives need to be considered, as maintained in Chapter II of this thesis.[422]

Overall, what are the primary legal requirements of the GDPR relevant to the scope of this thesis? In other words, what characteristics should a Blockchain infrastructure have to trigger the application of the Regulation protecting personal data?

First, it has to be established whether personal data are involved.

Various data could reasonably be considered personal data, including the name, identification number, location data, online identifier, or other information relating to a person. The GDPR's definition of personal data may also include pseudonymized data if it can be indirectly associated with a person through cross-referencing with other datasets or other means.

Transactional data stored in blocks and public keys may also meet the definition of personal data under the GDPR, although this list is incomplete. Importantly, categories of personal data, such as data revealing a person's racial origin, religious beliefs, or sexual orientation, are defined as special category data and are subject to even greater protections under the GDPR.

Strictly related to this first evaluation, there is the assessment of the material scope of the application of data processed on a Blockchain. The GDPR applies to any personal data processing that occurs entirely or in part by automated means and personal data processing that is not automated but forms part of or is intended to form

[422] Chapter II, para 4.5.

part of a filing system. Blockchain-enabled data processing qualifies as data processing 'through automated means'. Existing case law[423] underlines that Article 2(1) of GDPR's reference to 'the processing of personal data' should be defined broadly to secure the full protection of data subjects.

Consequently, it has to be assessed whether the territorial scope of the GDPR applies to data processed on a Blockchain. This evaluation requires considering (i) whether controllers or processors are established within the EU (the "establishment test"), or (ii) if they are established outside the EU, whether they offer goods and services to data subjects within the EU (the "targeting test") or monitor the behavior of data subjects in the EU where that behavior occurs in the EU (the "monitoring test").

The GDPR applies only when the personal data definition and material and territorial scope conditions are met. If the GDPR applies, all personal data collection, storage and processing must be done per the Regulation's requirements, including that data on the Blockchain. Of course, this assessment cannot be made in general but on a case-by-case analysis, which means examining the single processing operation to understand if this is the case.

[423] Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann*; case C-101/01, *Bodil Lindqvist*; joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission of the European Communitie*; case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*; case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*; joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for Home Department v Tom Watson and Others*; case C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*; case C-25/17, *Proceedings brought by Tietosuojavaltuutettu (Jehovan todistajat);* case C-207/16, *Ministerio Fiscal;* case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others;* case C-272/19, *Land Hessen,* para 68; case C-245/20, *Autoriteit Persoonsgegevens*, para 25; case C-268/21, *Norra Stockholm Bygg,* para 26.

3.1.Does the GDPR apply to data stored on a Blockchain?

Before answering if the GDPR applies to data stored on a Blockchain, it is essential first to clarify whether this data can be, in general, classified as personal data.

The GDPR enhances the definition of "personal data" found in the previous Directive and introduces three more elements contributing to the "identifiability" of the natural person's data. An "identifiable natural person" is someone "*who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".[424] Therefore, a piece of data capable of identifying a natural person is within the area of GDPR. Moreover, the class of sensitive personal data, which requires additional protections and restrictions, is expanded to include genetic and biometric data.

The concept of personal data has been interpreted so broadly as to include every piece of information that can be related to a person,[425] using both objective and subjective criteria, regardless of how it is conveyed or its accuracy.[426]

Applying the objective criterion, a person is considered identifiable in relation to anyone if the controller or any third party can identify the data subject. Applying the subjective criterion, data qualifies as personal only in relation to those who can identify the data subject themselves.

What is sure is that the GDPR only applies to processing personal data; it does not regulate any activity involving data that does not fall within this category, such as anonymous data. Although the GDPR does not define anonymity, it can be logically deduced that anonymous data cannot render its data subject identifiable.

[424] GDPR, article 4.

[425] Greater protection is provided to a specific category of personal data, that is the data which can reveal sensitive information about an individual, such as political opinions or sexual orientation.

[426] Article 29 Working Party, Opinion 4/2007 *on the concept of personal data*, June 20, 2017, at p. 6-7.

Furthermore, albeit recitals are not, *per se*, legally binding, recital 26 of the GDPR defines anonymous information as *"information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".* Hence, personal data that has been irreversibly anonymized would not fall within the scope of the GDPR. This means that, allegedly, the GDPR would not apply. Consequently, while anonymous data[427] falls outside the scope of the legal framework as it is impossible to trace back information to a living individual, pseudonymous data is still personal data, as long as an identifier's indirect identification of a natural person remains possible.

Determining the level of identifiability is a matter of judgment and degree, and whether a particular piece of data makes a data subject identifiable will depend on the context and methods used. Therefore, a methodology is necessary to determine whether the identifiability criterion has been met.

The academic literature has engaged in a longstanding debate regarding the scope of identifiability.[428] Some argue for a relative approach, focusing solely on the data controller, while others support an absolute approach, encompassing any third party involved. Critics of the absolute approach contend that it disregards the need for context-specific risk management, forcing data controllers to assume worst-case scenarios even if they are irrelevant.

[427] Recital 26 GDPR. In its opinion on Anonymization techniques (05/2014, WP 216) adopted on 10 April 2014, the Article 29 Working Party guided the difference between pseudonymized and anonymized data, from which various legal consequences stem. According to the document, in order to qualify data as truly anonymous, each anonymization technique has to be analyzed in light of the following three questions: (1) is it still possible to single out an individual? (2) is it still possible to link records relating to an individual? (3) can information concerning an individual be inferred?

[428] For a brief overview of the relative and absolute approaches, see G. Spindler, P. Schmechel, *Personal Data and Encryption in the European General Data Protection Regulation*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2016.

Certain supervisory authorities have adopted a middle-ground stance, exemplified by the ICO's "motivated intruder" test,[429] which assesses the potential for re-identification by a reasonably competent intruder without specialized knowledge or equipment.

The Recital uses the phrase "the means reasonably likely," which suggests combining both approaches, where personal data is only considered if the identification risk is not remote or highly theoretical. On the other hand, the legislator also considers objective factors such as costs, time, and available technology during the processing, which could be seen as an attempt to limit the broad and absolute elements of the GDPR's scope.

In the review of key judgments, a leading case is the Breyer judgment,[430] where the Court of Justice ruled that a dynamic IP address is considered personal data in relation to a specific internet service provider. According to Advocate General Campos Sànchez-Bordona,[431] whose reasoning was followed by the CJEU in the mentioned case, the risk of identification of the data subject was prohibited by laws or practically impossible on account of the fact that it required a disproportionate effort in terms of resources (such as time, cost and manpower). It is important to consider that both data users and recipients may attempt to identify individuals from the data they receive. Defining personal data can be challenging because seemingly non-personal data can become personal with the application of technological advancements. The ability to infer information about individuals from various types of data makes it increasingly difficult to differentiate between personal and non-personal data.

The GDPR offers a non-exhaustive list of identifiers that are considered personal data, including a person's name, identification number, location data, online identifier, and

[429] Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice*, November 2012, p. 16

[430] Judgment of 19 October 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

[431] Opinion of Advocate General Campos Sánchez-Bordona, Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, delivered on 12 May 2016, ECLI:EU:C:2016:339.

various other factors related to their physical, physiological, genetic, mental, economic, cultural, or social identity. In addition, the GDPR's Recital 30 mentions other online identifiers, such as cookie identifiers and radio frequency identification tags.

It's worth noting that identifying a data subject can also be done indirectly. By analyzing retained data, it may be possible to draw precise conclusions about a person's private life, such as their daily habits, where they live or travel, their activities, social relationships, and their frequent environments.[432] For instance, returning to the *Breyer* case, the Court recognized that an IP address alone could not identify the person using the device connected to a network. However, it also maintained that "*an IP address is only considered personal data if the internet service provider has the legal means to identify the data subject*." Some authors interpreted this as the Court acknowledged a grey area where data could simultaneously be personal and non-personal.[433]

The Court avoided categorically labelling IP addresses as personal data based solely on the possibility of identification. This balanced approach prevented broadening the regulatory burden on data-processing entities and avoided disproportionate outcomes based on the actual risks to data subject privacy. The Court's approach is consistent with Recital 4 of the GDPR, which specifies that the right to personal data protection is not absolute and must be balanced against other fundamental rights in accordance with the principle of proportionality. In this regard, the Court implicitly acknowledged that the binary concept of personal data is overly simplistic and not very useful in the larger and more complicated context of data collection and information flows.

[432] Judgment of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12.

[433] A. El Khoury, *Dynamic IP Addresses Can Be Personal Data, Sometimes. A Story of Binary Relations and Schrodinger's Cat*, in *European Journal of Risk Regulation* (EJRR), 2017, pp. 191-197.

Although the infrastructure of Blockchain applications and internet protocol addresses differ, the Breyer case[434] provides legal reasoning that could be applied to other technological applications with similar personal data and identifiability dynamics. As a matter of fact, the Court's ruling defined IP addresses as personal data if there are legal means to obtain more information to identify the data subject. Therefore, the "legal means" were effectively defined as any possible channel that is not prohibited by law.

As illustrated in the previous chapter, Blockchain data may be fully encrypted and cannot directly link to a data subject. Nonetheless, decentralized architectures provide content-level privacy through encryption, but the metadata, an essential feature of such systems, remains publicly available. Such metadata may still be considered personal data capable of identifying the data subject as long as (i) there are no legal prohibitions on accessing the necessary information about the subject that makes - the otherwise non-personal data - personal, (ii) and the process of obtaining such information is not particularly complex.

Since pseudonymous data qualifies as personal data, the consequence might be that public keys are personal data under the GDPR. To determine the possibility of re-identification, the Working Party has proposed three criteria: (i) singling out an individual, (ii) linking records related to an individual, (iii) and inferring information about an individual.[435]

In a Blockchain structure, public keys serve as identifiers and are necessary for the functioning of the technology.[436] However, using one-time public keys can minimize

[434] The case involved Mr. Breyer seeking an injunction against the German government to prevent them from registering and storing the IP addresses and dates of his visits to government-run web pages. The Court of Justice referred to "legal channels" that allow online media service providers to contact competent authorities to obtain information from internet service providers to combat cyber-attacks.

[435] Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, at p. 3, 0829/14/EN WP 216 (Apr. 10, 2014).

[436] Commission Nationale Informatique & Libertés (hereinafter CNIL), *Blockchain: Solutions for a responsible use of the Blockchain in the context of personal data*, 6 November 2018, https://www.cnil.fr/sites/default/files/atoms/files/Blockchain_en.pdf.

the risk of re-identification through singling out, linkability, or inference methods when combined with additional data related to the Blockchain transaction, such as exchanged assets, qualifications, addresses, and financial data.

The French Data Protection Authority recommends not including additional data in plain form and using encryption techniques like commitment and keyed hash functions to protect personal information.[437]

Finally, it is important to consider that the quality of parameters used to assess the risk of identification, such as the 'legal means' test, may change rapidly with advanced and easily accessible technology. For instance, cloud computing technology provides access to complex computing services that may introduce a risk of identification achieved through legal means and are not particularly complex. Online identifiers provided by devices are another parameter that significantly affects risk assessment. According to Recital 30 of the GDPR, natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers, or radio frequency identification tags. This information may be used to create profiles of individuals and identify them. Hence, based on the logic applied to IP addresses and other online identifiers listed in Recital 30 of the GDPR, much data produced by the Internet of Things technologies may become personal data, even if it is 'attribute data' or sheer machine data.

3.1.1. The potential for risk identification and the concept of pseudonymity

The previous section's observations prompted us to delve further into the concept of pseudonymous data, which holds significant relevance for the scope of this thesis.

There is uncertainty regarding the extent to which the data stored in the Blockchain ledger should be anonymized or deleted to comply with the GDPR's principle of

[437] CNIL (2018) at p.6.

storage limitation under Article 5 (1)(e). The storage limitation principle states that personal data should not be kept longer than is necessary for the purpose for which it was processed. However, not all methods of anonymization are equally effective.[438] If the data subject can (no longer) be identified because the data are (or has been) fully anonymized, then the data is not considered personal data and is, therefore, outside the scope of data protection law. Notwithstanding, determining when data are fully anonymized can be difficult, as even seemingly anonymous data can sometimes be re-identified by combining it with other data sets.[439]

According to Pfitzmann and Hansen,[440] data subjects are anonymous if they cannot be identified within a set of subjects, known as the anonymity set. This means that the subject is "indistinguishable from the other subjects within the anonymity set," which refers to the set of what the authors called the "usual suspects." However, it is challenging to determine when the usual suspects will behave similarly in specific situations. Some authors emphasize that if human mobility trace patterns are unique, supposedly anonymous datasets may contain personal data related to data subjects.[441] This implies that in situations where the "usual suspects" are not acting in a typical or

[438] *See Guidelines on Anonymisation Techniques* at note 57.

[439] In that sense, "A study conducted by the Cambridge Institute of Technology (MIT), published in the journal Science in 2014, confirms that through the extraction and aggregation of non-identifying data, it is possible to trace a person's identity, de-anonymising them. The study was based on the analysis of credit card transactions made over the course of three months, an analysis from which it was possible to track the spending of 1.1 million people in 10,000 stores in a single country. The bank did not provide names, credit card numbers, store addresses or even the exact times of the transactions but only *metadata*: the amounts spent, the type of store (restaurant, gym, grocery store, etc.) and a code that represents each person. Because each individual's spending pattern is unique, the data detected very high 'uniqueness' making it suitable for what has been called a 'correlation attack'. In order to trace the identity of each individual, it was sufficient to relate the metadata to information about the person from external sources.", see C. Irti, *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. Senigaglia, C. Irti, A. Bernes, (eds) *Privacy and Data Protection in Software Services. Services and Business Process Reengineering*, Springer, 2022, pp. 52-53.

[440] A. Pfitzmann, M. Hansen, *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.

[441] A. Farzanehfar, F. Houssiau, Y.A. de Montjoye, *The risk of re-identification remains high even in country-scale location datasets*, in *Patterns (NY)*, 2021.

consistent manner, metadata about them can easily reveal personal information, even in vast, sparse, and rough mobility datasets.[442] Similarly, knowledge of time-stamped transactions, the store where the transaction occurred, and the transaction price can make data subjects using credit cards as identifiable as mobile phones. Such metadata may include information about the transaction amount, the assets being transferred, and the transaction time, which is unique enough to narrow down the "usual suspects" class for accurate identification. In fact, the vast amount of data associated with a public key is publicly available and provides as much information as the identity of the entities transacting with the original key holder.

It's important to recall that when data has been pseudonymized, it is still covered by the GDPR. Pseudonymization is only a security measure that prevents the directed attribution of personal data to a specific subject without additional information.[443] For instance, in databases storing personal details of data subjects, names are replaced with numbers, and the document containing the associations between names and numbers is stored elsewhere.

Pseudonymization techniques listed by WP 29 include encryption, hash-function, keyed-hash function with stored key, deterministic encryption or keyed-hash function with key deletion, and tokenization. Therefore, pseudonymization[444] involves

[442] Article 29 Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, WP 215, p. 9.

[443] M. Mourby, E. Mackey, M. Elliot, H. Gowans, S. E. Wallace, J. Bell, H. Smith, S. Aidinlis, J. Kaye, *Are 'pseudonymised'data always personal data? Implications of the GDPR for administrative data research in the UK*, in *Computer Law Security Review*, vol. 34, no. 2, 2018, pp. 222–233.

[444] The Albrecht Report and subsequent amendments introduced the concept of pseudonymous data as a new category. According to the Report, a pseudonym is a unique identifier specific to one given context and does not permit the direct identification of a natural person but allows the singling out of a data subject (Council Report 2015, A: Preparation of a general approach, 965/15, 11 June 2015). The intent behind the concept of pseudonymization was to provide some flexibility, with the processing of pseudonymous data being subject to lighter data protection obligations. The Albrecht Report also introduced a definition of anonymous data: *"any data that cannot be related, directly or indirectly, alone or in combination with associated data, to a natural person or where establishing such a relation would require a disproportionate amount of time, expense and effort, taking into account the state of the art in technology at the*

processing personal data so that it can no longer be attributed to a specific person without additional information, which is kept separately and subject to technical and organizational measures to ensure that the personal data is not attributed to an identifiable person. Data encryption[445] can be used for pseudonymization, where the pseudonym does not redirect to the data subject without knowing a decryption key. However, the data encryption issue is that individuals not authorized to use the decryption key may still be able to re-identify the data subject. The Article 29 Working Party takes a zero-risk approach, meaning that the risk of identification after rendering data anonymous should be zero. Anonymization involves processing personal data to prevent the data subject's identification irreversibly. However, some argue that a risk-based approach is compatible with recital 26 of the GDPR, which states that data becomes anonymous when the data subject is no longer identifiable, and a reasonable risk of identification does not exist.[446] This means that data can be treated as anonymous when the risk is negligible.

In that sense, it is important to note that the EU General Court recently clarified[447] when pseudonymized data is considered personal data. It held that pseudonymized data transmitted to a data recipient will not be considered personal data if the recipient does not have the means to re-identify the data subjects. The Court also

time of the processing and the possibilities for development during the period for which the data would be processed."

[445] The LIBE Committee's compromise text further modified the concept of pseudonymous data and introduced a new concept of encrypted data. Encrypted data refers to personal data rendered unintelligible to unauthorized access through security measures (article 4(2a) and (2b)). Both pseudonymous and encrypted data are still considered personal data under the GDPR but are subject to less stringent data protection requirements (Cfr. Position of the European Parliament adopted at first reading on 12 March 2014 with a view to the adoption of Regulation (EU) No. .../2014 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), P7_TC1-COD(2012)0011, 12 March 2014).

[446] Finck (2019), p. 19.

[447] Judgment of the General Court, Case T-557/20, *Single Resolution Board v European Data Protection Supervisor*, 26 April 2023.

clarified that an individual's opinions cannot be assumed personal data and that a case-by-case assessment is necessary.

In this context, it remains controversial whether the GDPR imposes a zero-risk approach, particularly with regard to technological developments as an objective factor for identifying a person. It is possible that future re-identification of previously anonymized data could be a foreseeable scenario if data assessment is understood as a dynamic and periodical process.[448]

Although WP 29 sets a high standard of near-zero probability for identification, it fails to clarify the point of a risk threshold, which some have criticized. Inevitably, these contradictory approaches become problematic. While recognizing the need for clarification on the acceptable levels of risk, this research views WP 29's concept of anonymization as an ideal that data controllers and processors should strive to achieve rather than an unrealistic zero-risk requirement. Some authors suggest[449] that a more precise way to describe anonymous data is that which has a minimal risk of reidentification, as zero risk is not practically attainable.

In light of this analysis, reconsidering the above examples against WP 29 standards raises the question of whether any data can ever be entirely and irreversibly anonymized. Stalla-Bourdillon-Knight argues that policymakers must accept the dynamic state of anonymized data[450] since none of the known anonymization techniques can provide such an assurance while preserving the utility of the data sets. Indeed, the risk of identification increases with the number of databases and possible correlations, resulting in an "accretion problem" in data anonymization.

[448] S. Stalla-Bourdillon, A. Knight, *Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal*, 2016, pp. 311–312.

[449] K. El Emam, C. Álvarez, *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, in *International Data Privacy Law*, 2015.

[450] S. Stalla-Bourdillon, A. Knight (2016), pp. 297–298.

Establishing a high threshold like a zero risk of identification may not be realistic in the medium- and long-term for processing personal data through Blockchain technologies. If a specific ledger is used for a specific period, it should be assessed for that time frame, and data controllers should reassess the risks regularly. However, since a ledger is an immutable record of transactions without a specific time frame, it may be possible to identify individuals by singling them out, linking records, or making inferences from the information available.

One practical solution could be to include personal data in the payload added to the Blockchain. It's important to consider from which perspective the likelihood of identifying natural persons should be examined, and it seems appropriate to consider that of the data controller.

Moreover, legal proceedings against a third party with additional information to make identifying the data subject possible may not be a reasonable option. In the Breyer case, the CJEU noted that online media service providers can identify data subjects with the assistance of the competent authority and internet service provider. The means may be understood as a state's political or legal power, and the competent authority can take the necessary steps to obtain information from the internet service provider and bring criminal proceedings.

It is unlikely that an individual who is not the data controller or the data processor would have the necessary means to initiate legal proceedings against a third party who possesses additional information that could enable the identification of the data subject. In such a situation, it appears improbable that the individual would have access to personal information. This is because the legal channels for obtaining such information are often limited to the data controller or data processor or competent authorities authorized under applicable laws. Therefore, data controllers and processors must take appropriate measures to ensure the protection of personal data and comply with GDPR requirements.[451]

Notwithstanding, as already maintained, it is important to consider that encryption leaves metadata accessible - such as the data controller entity, date, and time - which poses a risk of unintentionally disclosing personal data. When combined with other data, such as camera logs, this information can be used to single out individuals, particularly regarding health information. Researchers have found it difficult to maintain anonymity where network data on user behavior is available.

Essentially, on permissionless Blockchains, it seems impossible to fully and irreversibly anonymize data while preserving the nodes' ability to "understand" the transaction, which they must verify to yield consensus. This means that, the data on Blockchains may be pseudonymous within the meaning of the GDPR.

3.2. Personal Data on the Blockchain

Having discussed the general uncertainties surrounding the classification of personal, pseudonymous, and anonymous data, these concepts will now be applied to two types of data commonly processed through Blockchain and distributed ledger technology (DLT). The first category is the public keys used as user identifiers on these networks, and the second is transactional data.

[451] See G. Spindler, P. Schmechel, *Personal Data and Encryption in the European General Data Protection Reglation,* in *Journal of Intellectual Property, Info Tech, and e-commerce L. 163,* 2016, p. 173.

3.2.1. Public keys as personal data

In Blockchain technology, public keys[452] shall be assimilated to the identifier type mentioned in Recital 30 of the GDPR.[453] Blockchain relies on a two-step verification process that utilizes asymmetric encryption. Each user has a public key, a string of letters and numbers that represents their account and is shared with others to enable transactions. Additionally, each user holds a private key, a string of letters and numbers that functions as a password that must be kept confidential. The mathematical relationship between the public and private keys allows the private key to decrypt data that has been encrypted using the public key.

Public keys can obscure the individual's identity unless linked to additional identifiers. However, this is only when the public key relates to a natural person. In some DLT use cases, public keys do not pertain to natural persons. For example, if financial institutions use a Blockchain to settle end-of-day inter-bank payments for their own accounts, public keys will relate to the institutions rather than natural persons. Therefore, public keys in this scenario would not qualify as personal data subject to the GDPR.[454]

According to Article 4(5) of the GDPR, a public key is considered pseudonymous data, as it "can no longer be attributed to a specific data subject" unless it is matched with

[452] For an overview of public keys from a technical standpoint, see para 4.3, Chapter I of this thesis.

[453] E. Politou, F. Casino, E. Alepis, C. Patsakis, *Blockchain mutability: challenges and proposed solutions*, in *IEEE Transactions on Emerging Topics in Computing*, 2021; F. Molina, G. Betarte, C. Luna, *Design principles for constructing GDPR-compliant Blockchain solutions*, in *Proceedings of the 2021 4th IEEE/ACM International Workshop on Emerging Trends in Software Engineering for Blockchain*, IEEE, 2021; A. Kolan, S. Tjoa, P. Kieseberg, *Medical Blockchains and privacy in Austria - technical and legal aspects*, in *Proceedings of the 2020 International Conference on Software Security and Assurance*, 2020; V. Ferrari, J.P. Quintais, A. Giannopoulou, B. Bodo, *EU Blockchain Observatory and Forum Workshop on GDPR*, in *Data Policy and Compliance*, Research Nodes 2018/1, Blockchain & Society Policy Research Lab, Institute for Information Law, University of Amsterdam, 2018; T. Buocz, T. Ehrke-Rabel, E. Hödl, I. Eisenberger, *Bitcoin and the GDPR: allocating responsibility in distributed networks*, in *Computer Law & Security Review*, 2019, pp. 182-198.

[454] J. Bacon et al (2018), p. 62.

additional identifying information, such as a name or address.[455] There are many similarities between public keys and other pseudonymous strings of letters and numbers, such as unique identifiers in cookies, which are considered personal data.[456] As detailed in the previous section, pseudonymization, as defined by Article 29 Working Party, is "the process of disguising identities," which is precisely what public keys do, although not in an irreversible manner. In practice, public keys can identify a specific natural person. Combining such records with the public key could thus reveal the real-world identity hidden behind a Blockchain address.[457]

Furthermore, public keys can also expose a transaction pattern with publicly known addresses that could potentially identify an individual user through transaction graph analysis. This has been demonstrated on the Bitcoin Blockchain,[458] where encrypted data has been used to reveal a link between users and transactions, enabling transactions to be traced back to users. Academic research has also shown that public keys can be traced back to IP addresses, aiding identification. When users send a transaction to the network, they typically connect directly and reveal their IP address.[459]

[455] Article 29 Working Party, Opinion 04/2007 on the concept of personal data, WP 136.

[456] B. F. Zuiderveen, *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation,* in *Computer Law & Security Review,* 2016, at p. 260.

[457] For example, data subjects have been linked to public keys by voluntarily disclosing their public key to receive funds or through illicit means. Additionally, crypto asset exchanges may gather additional information to comply with regulatory requirements, such as Know Your Customer and Anti-Money Laundering duties and may store parties' real-world identities.

[458] P. L. Juhasz, J. Steger, D. Kondor, G. Vattay, *A bayesian approach to identify bitcoin users*, in *PLoS ONE,* 2018, pp.1-21.

[459] Law enforcement agencies worldwide have used forensic chain analysis techniques to identify suspected criminals based on their public keys, and various professional service providers offering related services have emerged (see for instance https://www.chainalysis.com/).

Given the above, it is no wonder that most (though not all)[460] of the authors assert that public keys may qualify as personal data under the GDPR,[461] highlighting that

[460] Some researchers oppose classifying public keys as personal data. Rampone argues that the definition of personal data provided in the GDPR does not apply to public keys used in Blockchain systems. He asserts that public keys are primarily used to address a technical challenge in establishing trust within a peer-to-peer network and are not designed to reveal personal identities. Therefore, Rampone suggests that public keys should not be considered personal or pseudonymous data, even though they could potentially be used in advanced digital forensic searches to identify the holders of private keys. He emphasizes that a public key may be associated with a natural person and a legal entity, making the equivalence of public keys and pseudonymous data incorrect. Rampone also points out that there is no readily available correspondence list mapping public keys to personal IDs, and acquiring such a list is not feasible under normal circumstances. Thus, he views a public key as merely an indication of specific credit availability. In payment scenarios where the debtor and creditor are known to each other, the correspondence would be contingent and limited to a specific ongoing transaction, with no extension to other transactions.

Similarly, Eichler et al. propose that public keys should not be considered personal data in two circumstances: when a key does not belong to a natural person or was not created on behalf of a natural person, and when a key cannot be reasonably linked to a natural person and is therefore truly anonymous. Like Rampone, they emphasize the essential role of public keys in Blockchain technology and argue that the legal framework needs to adapt to this new perspective on public keys.

These arguments highlight the viewpoint that public keys, as integral components of Blockchain systems, should be treated differently from traditional personal data due to their specific technical functions and characteristics.

See F. Rampone, *Data protection in the Blockchain environment: GDPR is not a hurdle to permissionless DLT solutions,* in *Ciberspazio e Diritto*, 2018, pp. 457-478; N. Eichler, S. Jongerius, G. McMullen, O. Naegele, L. Steininger, K. Wagner, *Blockchain, Data Protection, and the GDPR,* Technical Report VR 36105 B 27/661/52176, German Blockchain Association (Bundesblock), 2018.

[461] For instance, Finck highlights the potential of public keys in identifying individuals through various scenarios. 1) In the case of a house ownership transfer recorded on a Blockchain, the public nature of the Blockchain allows neighbors or observers to associate the public key involved in the transfer with the owner of the house. 2) Some users intentionally share their public keys online to receive donations. This voluntary disclosure can link their public key address to their real-world identities. 3) Regulatory requirements, such as KYC (Know Your Customer) and AML (Anti-Money Laundering) procedures performed by cryptoasset exchanges, may lead to the disclosure of real-world identities associated with public keys. This is done through the collection of additional information as part of these requirements. Furthermore, beyond these simple scenarios, the literature also discusses the risk of more advanced pattern analysis. If the same public key is consistently used by an individual in multiple transactions, patterns may emerge. These patterns can potentially be exploited to re-identify the individual behind the public key. These examples illustrate how the use of public keys, combined with various factors such as Blockchain transparency, intentional disclosures, and regulatory requirements, can potentially lead to the identification or re-identification of individuals in the digital realm. Cfr. D. G. Duarte, *An Introduction to Blockchain Technology from a Legal Perspective and its Tensions with the GDPR*, in *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law*, 2019, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3545331.

Koscina et al. took a more measured approach by acknowledging public keys as personal data, but their use within blockchains is seen as a way to achieve the utmost reduction of information (as stipulated in Article 5(c) of the GDPR). Similarly, Giannopoulou and Ferrari contended that, when combined with even if personal information only includes reference ID numbers, such identifiers are typically unique to a specific person, and additional information may be necessary to attribute information to the data subject, making it pseudonymized personal information.[462] The French Data Protection Authority and the European Union's Blockchain Observatory and Forum have also stressed the linkability risk of public keys and their potential to constitute personal data under the GDPR.

Although a case-by-case analysis is necessary, it is clear that public keys that relate directly or indirectly to an identified or identifiable natural person may qualify as personal data under the GDPR. As mentioned, linkability, singling out, and inference can lead to identifying a natural person through public and permissionless as well as private and permissioned Blockchains. According to the guidance provided by the Article 29 Working Party, if a public key serves to identify a data subject explicitly, its classification as personal data is always given.

Therefore, implementing a Blockchain should be consistent with deploying measures that prevent public keys from being related to an identified or identifiable natural person. This can be done by employing technical and organizational measures that create hard barriers between the Blockchain and other databases that may contain additional information for linkage. Using one-time public keys is also a good practice in this regard. However, their existing governance mechanisms and institutional structures may make this easier to implement on private and permissioned Blockchains.

In essence, one of the most significant challenges in creating a Blockchain system that fully complies with the GDPR is the considerations around public keys. These

necessary privacy-enhancing mechanisms, public keys could meet the data minimization requirements outlined in the GDPR (see M. Koscina, M. Lombard-Platet, C. Negri-Ribalta, *A Blockchain-based marketplace platform for circular economy*, in *Proceedings of the 36th Annual ACM Symposium on Applied Computing, ACM*, 2021, pp. 1746-1749).

[462] M. Berberich, M. Steiner, *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, 2016, at p. 422.

keys are an integral part of Blockchain technology and cannot be easily moved off-chain like other data. Nevertheless, the literature offers techniques for anonymizing public keys, such as ring signatures and zero-knowledge proofs (ZKPs), which can be employed to address this challenge, which will be explained in paragraph 6.

3.2.2. Transactional data

The term "transactional data" describes other types of data that can be used on Blockchains besides public keys. This refers to data that pertains to the transaction itself. According to the French Data Protection Authority, this could include data "contained 'within' a transaction (e.g., diploma, property deed)." For instance, transactional personal data may consist of a name, address, or date of birth in a particular transaction.

A case-by-case analysis is necessary also for this data to determine whether transactional data qualifies as personal data under the GDPR. In certain situations, transactional data may not be considered personal data. For example, if a Blockchain is used as a data infrastructure to share non-personal data, such as climate sensor data. Similarly, a crypto asset transferred from one party to another may not qualify as personal data unless combined with additional information that specifies the product or service purchased, which could lead to identification.

However, in other cases, such data may qualify as personal data. For example, if a group of banks use DLT to share Know Your Customer data, such data would likely qualify as personal data. The French Data Protection Authority has emphasized that if such data pertains to natural persons, who may be identified directly or indirectly, it would be considered personal data.[463]

[463] The CNIL acknowledges that anonymization tends to make identifiability "practically impossible" F. Martin-Bariteau, *Blockchain and the European Union General Data Protection Regulation: the CNIL's Perspective*, Working Paper, Blckchn.ca, 2018.

When assessing whether transactional data qualifies as personal data, it is important to remember that EU data protection law has adopted a broad definition of personal data to ensure the complete protection of data subjects, as discussed earlier.[464]

Public keys and transactional data can be stored on the Blockchain in plain text, encrypted form, or hashed. If personal data is stored in plain text, it remains personal data and does not require further analysis. However, it is crucial to understand that encryption or hashing alone is not enough to render personal data anonymous under the GDPR. Even when data is encrypted, it is still possible for the decryption key holder to re-identify each data subject, as the personal data remains present in the encrypted dataset. Therefore, encrypted data remains personal data, at least for the decryption key holder, who can identify such data. The Article 29 Working Party has clarified in its opinion on cloud computing that while encryption "may significantly contribute to the confidentiality of personal data if implemented correctly," it does not make personal data irreversibly anonymous.[465]

Notwithstanding, some commentators have suggested that sufficiently well-encrypted data, where the provider has no access to the decryption key, should not be considered personal data, and the same goes for sufficiently anonymized data. This implies that a distinction may need to be made between those with access to the decryption key and those without access. This seems indeed confirmed by a recent and already mentioned ruling of the EU General Court,[466] which held that pseudonymized data transmitted to a data recipient would not be considered personal data if the recipient does not have the means to re-identify the data subjects.

[464] We observed a general consensus in the literature, which highlights that transactional data pseudonymized via encryption or hash functions should still be considered personal data. See J. Erbguth, *Five ways to GDPR-compliant use of Blockchains,* in *European Data Protection Law Review*, 2019, pp. 427-433; D. G. Duarte (2019); M.T. Giordano, *Blockchain and the GDPR: new challenges for privacy and security*, in B. Cappiello, G. Carullo (eds), *Blockchain, Law and Governance, Springer*, 2021, pp. 275-286; A. Giannopoulou, V. Ferrari (2019); F. Molina et al (2021), cit.

[465] Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, WP 196, 01037/12/EN.

[466] Judgment of the General Court, Case T-557/20, *Single Resolution Board v European Data Protection Supervisor*, 26 April 2023.

Moreover, as detailed in Chapter I, Blockchain technology relies on hashing, which consists of generating a code of a fixed length for a given piece of digital information. Hashing is important because it permits someone to verify, by recalculating the hash, that a given piece of digital information is identical to the digital information that was originally hashed. This permits document authentication proof that a given document is the same as originally hashed, as a hash cannot be reverse engineered to discover the original document. The process only works in one direction, from the original document to the hash. Yet, in spite of this, as mentioned above, the Article 29 Working Party considers in its Opinion 05/2014 that hashing is a technique of pseudonymization, not anonymization.[467] Therefore, it is sufficient for a hash to permit records to be linked, so-called "linkability", [468] for a piece of information to constitute personal data.[469] The Spanish DPA provides a more absolute approach regarding hash functions and reported that whether to consider hashed data as anonymized or pseudonymized depends on a variety of factors ranging from the entities involved to

[467] It is unclear whether using salted and peppered hashes can effectively prevent the identification of a data subject. While a salted hash can lower the chances of determining the original input value, the Working Party emphasized that it cannot guarantee anonymous data, as it may still be possible to calculate the original attribute value with reasonable effort. On the other hand, peppered hashes involve an additional secret key, which makes it much harder for an attacker to replay the function without knowing the key. The Working Party recognizes that peppered hashes offer stronger guarantees but does not explicitly state whether they can be relied upon for anonymizing data under the GDPR. This determination needs to be made on a case-by-case basis, considering all the reasonable means available to protect the data.

[468] This is confirmed by the '*Joint paper of the Spanish data protection authority, Agencia española de protección de datos (AEPD), and the European Data Protection Supervisor (EDPS) on hash techniques in data processing activities as a safeguard for personal data'*, October 2019, according to which "With regard to the confidentiality of information represented in the hash, the fact of having a linked identifier adds an additional vulnerability to the existing weakness of the relevant hash, since, from that ID number, information may be obtained which reduces the effective message space for that particular hash.", https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, at 13.

[469] Consequently, a hash that represents a person's ID card or medical record would likely be considered personal data even though the hash itself is impossible to reverse engineer into the original personal information. By contrast, a hash that represents a bill of lading would not be considered personal data, but for reasons linked to the bill of lading, not to the hash, as the bill of lading does not contain personal data.

the type of data at hand.[470] Similarly, the UK's DPA Information Commissioner's Office once advised on its website that personal data that has been pseudonymized, for instance key-coded, can fall within the scope of the GDPR based on how difficult it is to attribute the pseudonym to a particular individual.[471] Notwithstanding, this conservative opinion seems to have changed as the ICO clearly stated that "pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data".[472]

It is important to bear in mind that, generally speaking, storing personal data on the chain is unnecessary because the nodes do not need to know each other's personal data. Instead, personal data can be stored in an off-chain database and merely linked to the distributed ledger through a hash. Undoubtedly, off-chain storage is the most discussed concept in the reviewed literature for GDPR-compliant processing of personal data on Blockchain.[473] Storing data "off-chain" means that the data, in this case, the personal data or in general the payload, is not kept inside the Blockchain network, but stored outside, e.g., in a traditional database.[474] Essentially, only a reference (for instance, a hash value) to the outside storage location where the actual data is stored is saved on the Blockchain, a so-called hash-pointer.[475]

[470] A. Giannopoulou, *Data protection compliance challenges for self-sovereign identity*, in *Blockchain and Applications: 2nd International Congress, Springer*, 2020, pp. 91-100.

[471] See ICO, *Overview of the General Data Protection Regulation (GDPR)*, 2017, https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf.

[472] See https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/#pd4.

[473] For an interesting solution to the Blockchain trilemma, see S. Reno et al. (2023), cit.

[474] C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K. R. Choo, *Blockchain: A Panacea for healthcare cloud-based data security and privacy?* in *IEEE Cloud Computing*, pp. 31–37; L. D. Ibáñez, K. O'Hara, E. Simperl, *On Blockchains and the General Data Protection Regulation,* available online at *https://eprints.soton.ac.uk/422879/1/Blockchains_GDPR_4.pdf*.

[475] M. Finck, *Blockchains and Data Protection in the European Union,* in *European Data Protection Law Review*, 2018, at p. 17; M. Berberich, M. Steiner (2016), at p. 425; M. Steichen, F. Beltran, R. Norvill, W. Shbair, R. State, *Blockchain-based, decentralized access control for IPFS*, in *IEEE International Conference on Blockchain*, 2018.

That often implies the reintroduction of a trusted third party which ensures the confidentiality and integrity of the data. This provides a certain degree of control to a centralized party, which seems to be a violation of the principles of Blockchain.[476]
Notwithstanding, these considerations may not apply to public keys, as they cannot be stored off-chain in most cases.

In any case, off-chain storage seems to permit the correction and deletion of personal data stored off-chain in appropriate databases in light of articles 16 and 17 of the GDPR, as will be discussed hereinafter. Off-chain solutions are encouraged by some researchers. For instance, Alessi et al.[477] proposed the development of modules that enable the storage of personal data in a centralized cloud environment while preserving only the business logic on a Blockchain network.
Discussions within specific domains also highlight varying perspectives. Kolan et al.[478] argued against the direct storage of personal medical data on blockchains. Likewise, Zheng et al.[479] presented a solution that avoids storing health information on blockchains. In a similar vein, Ma et al. focused on personal data managed by banking systems and proposed a data privacy classification for data storage. Their approach suggests that only public information should be stored on the Blockchain without restrictions. Sensitive information is not stored on the Blockchain by default setting. However, customers have the option to put their sensitive information on the

[476] To enable secure outsourcing of data, Eberhardt and Tai propose the adoption of content addressable storage for off-chain storage. This type of storage saves files not by their names but by their hash values. This approach offers the benefit of trustless outsourcing since any modification of the data would result in a modification of its hash value and, consequently, its storage location: see J. Eberhardt, S. Tai, *On or off the Blockchain? Insights on off-chaining computation and data*, in F. de Paoli, S. Schulte, E. Broch Johnsen (Eds.), *Service-oriented and cloud computing*, Springer International Publishing (Lecture Notes in Computer Science), pp. 3–15.

[477] M. Alessi, A. Camillò, E. Giangreco, M. Matera, S. Pino, D. Storelli, *A decentralized personal data store based on Ethereum: towards GDPR compliance*, in *Journal of Communication Software and System*, 2019, pp. 79-88.

[478] A. Kolan et al (2020), cit.

[479] X. Zheng, R.R. Mukkamala, R. Vatrapu, J. Ordieres-Mere, *Blockchain-based personal health data sharing system using cloud storage*, in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services*, 2018, pp. 1-6.

Blockchain if they choose to do so. Additionally, the banks themselves decide to store sensitive information owned by banks, primarily confidential operational data. These domain-specific discussions highlight the need for tailored approaches when considering the storage of personal data on blockchains, taking into account the specific requirements and sensitivities of different industries and sectors.

Notwithstanding, the status of the hash remains an open question. The data in off-chain storage is connected to the database through a hash, and if the off-chain data is deleted, the hash will remain on the ledger. The means reasonably likely to provoke identification need to be examined to determine whether this hash remains personal data. Nevertheless, there is uncertainty about how to make this determination, and this research suggests that regulatory guidance be provided on this issue.

3.3. The material scope of application of the GDPR

Article 2 of the GDPR determines the *material* scope of the GDPR and covers the public and private sectors.[480]

The first paragraph[481] applies to processing personal data wholly or partly by automated means and other than by automated means when the personal data form part of a filing system or are intended to form part of such a system. It also provides a number of exemptions,[482] such as the household exemption. The scope outlined in the initial paragraph is effectively restricted by the second paragraph, which specifies

[480] Some authors condemned that having tailor-made rules for the public sector would have been better, see P. Blume, C. W. Svanberg, *The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus*, in *Cambridge Yearbook of European Legal Studies,* 2013, p. 27.

[481] To fully understand the material scope, refer to articles 4(1), (2) and (6) GDPR, that contain the definitions of 'personal data', 'processing' and 'filing system'.

[482] The other exclusions in paragraph 2 are linked to policy areas for which the EU has no or only limited competence or for which specific Union rules apply. This includes the processing of personal data by competent authorities in the law enforcement area, which is covered by the LED. These exclusions reflect the former EU pillar structure, which was, in principle, abolished with the entry into force of the Lisbon Treaty in 2009.

exclusions of certain processing activities from the scope of the GDPR. Notably, the processing of data for personal or household activities is explicitly excluded from the scope.

Since Article 2 GDPR follows to a large extent the equivalent provision in the Data Protection Directive ('DPD'), namely Article 3, many of the conclusions that the Court of Justice reached for the previous Directive still apply to the GDPR. Indeed, in its first two rulings on the Data Protection Directive in 2003, the CJEU was confronted with questions about the scope of the data protection rules. In those occasions, the CJEU considered that the recourse to an internal market legal basis does not presuppose the existence of an actual link with the free movement between the Member States in every situation referred to by the measure founded on that basis. A contrary interpretation, according to the Court, could make the limits of the field of application of the DPD particularly unsure and uncertain.

Channelling these considerations to the public Blockchain sphere, it can be arguably affirmed that Blockchain falls within the material scope of the GDPR, as it implies processing personal data by automated means. The term 'processing' encompasses practically any activity involving personal data; automated data processing concerns any personal data processing carried out using a device (e.g., computer).[483] From this broad interpretation, it steams that adding personal data, storage, and any further operation on the Blockchain constitute personal data processing.[484] It has indeed to be taken into consideration that a Blockchain is an append-only ledger. This means that, once the data are stored on the Blockchain, it is almost impossible to delete them since they continue to be stored there for as long as

[483] See European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, 2018, p. 99.

[484] See M. Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?*, 2019, at 10.

it functions. Moreover, to validate the new transactions, the past transactions need to be verified and, then, processed.

The household exemption has already been mentioned. It entails that the GDPR does not apply to the processing of personal data carried out by a natural person during a purely personal or household activity, which is thus non-commercial/non-professional. The Commission Nationale de l'Informatique et des Libertés (CNIL) has accordingly submitted that natural persons who use a Blockchain for reasons unrelated to their profession or commercial activity do not assume the role of controllers, therefore *"a natural person who buys or sells Bitcoin, on his or her own behalf, is not a data controller"*.[485]

However, the Court of Justice,[486] as well as the Article 29 Working Party,[487] have broadened the scope of application of this exemption by requiring a further condition: the diffusion of personal data being restricted to a limited number of persons.

Consequently, by directly applying and not contextualizing the Court's rulings, we could argue that even those who use the Blockchain for personal purposes might be qualified as data controllers since the data is accessible to an indefinite number of people. In theory, in public permissionless blockchains, the information stored therein can be accessible to anyone, even if it is pseudonymized information.

Nonetheless, this turns out to be an assertion with no concrete basis in practice since making information publicly available on social media is unlike on-chain, as only through on-chain data it is not possible to identify a natural person.[488]

In that sense, the CNIL point of view can be embraced, as it is more pertinent to the Blockchain context.

[485] See Commission Nationale de l'Informatique et des Libertés, *Solutions for a Responsible use of Blockchain in the context of Personal data*, 2018.

[486] Case C-101/01 *Lindqvist*, 2003, para 47; case C-73/07 *Satukunna Markkinaporssi and Satamedia*, 2008, para 44; case C-212/13 *Ryne*, 2014, paras 31 e 33; case C-345/17 *Buivids*, 2019, para 43; case C-25/17 *Jehovan todistajat*, 2018, para 42.

[487] Article 29 Data Protection Working Party, Opinion 5/2009 on *Online Social Networking*, 12 June 2009.

[488] See J. Erbguth (2019), pp- 427-431.

3.4. The extensive territorial scope of application of the GDPR

The territorial scope of the GDPR determines the conditions under which the Regulation applies to the processing of personal data, even if the controller or processor is not established within the European Union. This is important for determining which supervisory authority is competent to oversee the processing activity, which is strictly related to the concept of extraterritoriality.[489] As it will clearly stem from the following analysis, the concept of extraterritorial application is particularly relevant in the realm of personal data protection rights. These rights are governed by diverse regulations across jurisdictions worldwide. The processing of personal data can trigger the extraterritorial application of a specific jurisdiction's requirements to ensure higher protection. This extraterritorial application can be viewed as an expression of the Digital Sovereignty of the regulating entity, typically a country. By extending its regulations to govern personal data processing beyond its borders, the country aims to safeguard data protection rights within its domestic market and protect the rights of its citizens, including their digital integrity. As already anticipated, in the domain of data, this dimension of sovereignty can be described as "personal data sovereignty," which encompasses aspects such as personal data ownership, the right to a secure connection, and the adherence to European values and principles in this field.

[489] From a legal standpoint, when a state exercises extraterritorial jurisdiction, it means that a particular provision established by that jurisdiction applies beyond its geographical boundaries and jurisdictional limits. This includes provisions concerning external behaviors, such as actions originating from foreign entities or connected to foreign jurisdictions, which have an impact on the regulation of a domestic market, the preservation of fundamental values within the jurisdiction, or even the territorial integrity of a state. These provisions may also serve to safeguard individuals against violations of their fundamental rights resulting from harmful behaviors originating in foreign jurisdictions. In other words, extraterritorial jurisdiction enables a state to extend its legal reach and enforce its regulations beyond its own territory to address situations that have cross-border implications or effects. This allows the state to protect its interests, preserve its values, and provide remedies for individuals affected by harmful actions originating from abroad.

Under the GDPR, the territorial scope is defined in Article 3.[490] Unlike the previous Data Protection Directive, which determined the applicable national law for a processing activity under Article 4, the GDPR establishes two alternative connecting factors that trigger the application of the Regulation: the establishment of a controller or processor within the European Union and the targeting and monitoring of individuals located in the European Union.[491]

The first connecting factor means that if a controller or processor is established within the EU, regardless of whether the processing occurs within or outside the EU, the GDPR applies. Thus, regardless of the actual location of the personal data processing, for example, in a third country where the parent company has its headquarters, when a corporation has a subsidiary in a Member State of the European Union, the GDPR may apply to the subsidiary.

The GDPR differs from the Data Protection Directive because it covers the data controller and processor. This extension of coverage broadens the scope of the GDPR. As a result, a processor operating on behalf of a controller located outside the European Union and within the EU must comply with EU law to prevent the Union from becoming a haven for data.

[490] According to Article 3(1) of the GDPR, the processing of personal data must be linked to the activities of a controller or processor established in the European Union, regardless of where the processing actually occurs. This is similar to the criterion under the Data Protection Directive, which focused on the location of the controller or processor within the EU. As a result, if a corporation has a subsidiary in a Member State of the EU, the GDPR may apply to the subsidiary's processing activities, regardless of where the actual processing takes place, such as in a third country where the parent company is headquartered. However, the GDPR adopts a functional approach to determine what constitutes an "establishment". Recital 22 of the GDPR defines an establishment as an actual and effective exercise of activity through stable arrangements. This definition is flexible because the degree of stability and effectiveness of the arrangements in another Member State must be assessed in light of the specific economic activities and services provided.

[491] See C. Kuner, *The Extraterritorial Application of the EU Data Protection Regulation*, in *International Data Privacy Law*, Vol. 6, No. 2, 2016, pp. 83-96; P. De Hert, V. Papakonstantinou, *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*, in *Computer Law & Security Review*, Vol. 32, No. 2, 2016, pp. 179-194; K. Eichner, *The Territorial Scope of the General Data Protection Regulation*, in *Journal of Data Protection & Privacy*, Vol. 1, No. 2, 2017, pp. 122-140; L. Caccia, *The Extraterritorial Reach of the General Data Protection Regulation: A Critique of the Establishment Criterion*, in *Common Market Law Review*, Vol. 56, No. 1, 2019, pp. 63-100.

To determine the existence of an establishment in the EU, it is important to consider any real and effective activity carried out on a stable basis, abandoning the formalistic approach,[492] according to which companies are only established where they are registered.[493] As per GDPR Recital 22, an establishment is defined as the effective and actual exercise of activity through stable arrangements. This definition provides flexibility because the degree of stability of structures and the effective exercise of activities must be interpreted in the context of the specific nature of the economic activities and services provided. However, this interpretation does not imply that the concept of an establishment has no limits. In the *Verein für Konsumenteninformation* case,[494] the Court of Justice (CJEU) recognized that simply having a website accessible in the EU does not necessarily mean that a non-European entity has an establishment in the EU. This ruling can be applied to a Blockchain context where the validation and participating nodes, which may be considered controllers or processors, are outside the EU. Access to the Blockchain network within the EU does not automatically

[492] See, case C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság Weltimmo v NAIH*, 2015, para 29, and case C-131/12, *Google Spain*, para 53.

[493] In this regard, the so-called 'economic unit' theory is worth mentioning, which can be summed up as the functional meaning that the concept of 'undertaking' assumes in competition law. First, the concept "focuses on the type of activity performed rather than on the characteristics of the actors which perform it" (see Opinion of the Advocate General Jacobs in joined cases *AOK Bundesverband and Other;* see also, inter alia, case C-41/90, *Höfner and Elser* , para 21); joined case C-159/91 and C-160/91, *Poucet and Pistre*, para 17; case C-218/00, *Cisal*, para 22; case C-49/07, *MOTOE*, para 21.
Second, "the classification of an activity as economic – and therefore of an entity as an undertaking – for the purposes of the application of competition law depends on the context examined. Similarly, the identification of the entities within the scope of the undertaking depends on the subject matter of the contested infringement." (see Opinion of the Advocate General Pitruzzella in case *Sumal, S.L. v Mercedes Benz Trucks España, S.L.*, C-882/19, delivered on 15 April 2021, para 25; and also, cases 6/73 and 7/73, *Istituto Chemioterapico Italiano and Commercial Solvents* v *Commission,* para 41, in which the concept of undertaking, for the purposes of the application of Article 102 TFEU, was applied only to the action that the two accused companies had brought jointly against a third company which they supplied; see, case 170/83, *Hydrotherm Gerätebau*, para 11, in which the Court held that, in competition law, the concept of undertaking 'must be understood as designating an economic unit for the purpose of the subject matter of the agreement').

[494] Case C-191/15, *Verein fuř Konsumenteninformation v. Amazon EU Sàrl*, 2016.

constitute an establishment in the Union, particularly in the case of a public and permissionless Blockchain.

When assessing the 'stable basis' for the provision of services online, the threshold is relatively low from the moment that the presence of even only one representative could be deemed to be enough.

Notwithstanding, one cannot affirm that an establishment exists only because the undertaking's website is accessible in the Union.[495] Yet, to evaluate if the establishment criterion can be used to apply the GDPR to blockchains, one should be able to identify who the data controller is. As it will be analyzed in section 4.1, it is a problem that recurs whenever the data protection implications of Blockchain are discussed.

As a general statement, we can argue that it is not possible to single out a specific and stable establishment for the provision of Blockchain services since there is no official headquarters.[496] In any case, even if that were the case, in most situations, the controller is identified relying on the criterion of a natural person's residence.

A challenging concept to interpret is whether the processing of personal data by a data processor or controller takes place "in the context of activities of" an EU establishment. This issue was addressed in the *Google Spain* case,[497] where the Court established that a connection must exist between the company's data processing activities and its subsidiary located in the EU. Personal data processing is deemed to occur in the context of an EU establishment's activities when the controller's activities in a non-EU country are "inextricably linked" to the activities conducted by an establishment in an EU Member State.

[495] *Ibidm,* para 76.

[496] For instance, taking into consideration the Ethereum platform, the Ethereum Foundation cannot be considered the responsible entity, since 'its role is not to control or lead Ethereum, nor are they the only organization that founds critical development of Ethereum-related technologies', in About the Ethereum Foundation (March 30, 2021), available at https://ethereum.org/en/foundation/.

[497] Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014.

For example, if a social network parent company located in a non-EU country has a subsidiary in the EU that sells food products with no connection to the social network, there is no relationship in the context of activities.[498] Conversely, if there is a connection between the economic activity of the establishment and the data processing, whether within or outside the EU, the GDPR applies.

The Google Spain case found a relationship existed between Google Inc. in the US and Google Spain SL in Spain because the advertising space offered by Google Spain made the search engine profitable. Some have criticized the broad interpretation of personal data processing "in the context of activities" of an establishment in an EU Member State as it may cover situations with little connection to the EU.[499] However, the CJEU recently confirmed[500] that the activities of Google France related to advertising space are inextricably linked to the processing of personal data for operating the search engine, indicating that Google France's activities fall within the scope of the Directive and the GDPR. Particularly, the judgment demonstrates the Court's attempt to determine the legality of global de-referencing. By affirming that EU law does not prohibit worldwide de-listing and that Member States retain the authority to compel

[498] Article 29 Data Protection Working Party, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain*, 176/16/EN WP 179 update, Annex 2 (Dec. 16, 2015).

[499] See L. Moerel, *The long arm reach of EU data protection law: does the Data protection Directive apply to processing of personal data of EU citizens by websites worldwide?*, in *International Data Privacy Law*, 2011, pp. 40-45; C. Kuner, T*he Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges", in* B. Hess, C. M. Mariottini (eds.), *Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55,* in *LSE Law, Society and Economy Working Papers 3/2015,* pp. 28-31.

[500] Case C-507/17, Google LLC, successor in law to Google Inc. v. Commission Nationale de I'informatique et des Libertés (CNIL), 2019, para 72 : «Lastly, it should be emphasised that, while, as noted in paragraph 65 above, EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights (see, to that effect case C-617/10, *Åkerberg Fransson,* para 29, and case C-399/11, *Melloni,* para 60), a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine."

search engine operators to globally de-reference under specific conditions, the Court leaves room for France's CNIL and other national Data Protection Authorities (DPAs) to enforce global de-referencing when they deem it appropriate.

The significance of this decision also revolves around examining whether the EU can extend its data protection and privacy standards beyond its borders, which has been a subject of interest. As companies expand their global operations and handle personal data on a larger scale, the conflict between national regulatory bodies and these companies is expected to intensify.

In the absence of comprehensive international standards governing the processing of private information, individual jurisdictions are likely to attempt to implement regulations with global impact, seeking to extend their own privacy standards universally to safeguard the rights of their citizens in relation to personal data processing. Consequently, the Court's decision carries legal significance in reinforcing the role of the GDPR as a benchmark for international data protection, impacting companies worldwide.[501]

In this context, on the other hand, the European Data Protection Board advises that the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law.[502]

It is worth noting that the GDPR applies to the processing of personal data within the context of activities of a data controller or processor established in the European Union, regardless of the location or nationality of the data subject. Identifying a controller's location in a public and permissionless Blockchain can be challenging.

[501] Cfr. M. Samonte, *Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law*, in *European Papers*, 2019, pp. 839-851.

[502] EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation*, Nov. 12, 2019.

According to case law, a broad interpretation of establishment would imply that the GDPR applies to nodes operating as controllers located within the EU. This approach presents difficulties because determining the hierarchy of controllers for nodes located in third countries is impossible. One possible solution would be to consider the location of full nodes[503] that keep the entire ledger, and if they are located within the EU, the GDPR should apply. However, this approach does not solve the problem of a lack of reference to a "main establishment."

In contrast, identifying the establishment of a data controller would be simpler if a recognizable individual or entity operates or establishes the Blockchain. This is the case with a private and permissioned Blockchain, such as a consortium of banks or a financial entity that establishes a Blockchain to manage clients' data.

The first connecting factor of the GDPR is the establishment of controllers and processors in the European Union. Companies that do not have any establishment in the EU but process the personal data of individuals in the EU would be exempt from complying with the GDPR. Notwithstanding this, legal convergence[504] has been extensively used in reference to the phenomenon of global diffusion of the EU standards for data protection and we are witnessing a wide adoption of the Regulation, often considered a blueprint for data privacy. The phenomenon in question, commonly known as the "Brussels Effect"[505] has been widely discussed in

[503] A full node is a Blockchain node that stores the Blockchain data, passes along the data to other nodes, and ensures that newly added blocks are valid and authentic.

[504] A. R. Young, *The European Union as a global regulator? Context and comparison,* in *Journal of European Public Policy*, 2015, pp. 1233–1252.

[505] The term itself originates from the renowned work by Anu Bradford, who coined it while examining this particular phenomenon, cfr. A. Bradford, *The Brussels Effect*, in *Northwestern University Law Review,* 2012, pp. 1-68; M. Gal, O. Aviv, *The Competitive Effects of the GDPR*, in *Journal of Competition Law and Economics*, 2020, pp. 1-37; A. Renda, *Single Market 2.0: The European Union as a Platform*, in *The Internal Market 2.0*, edited by S. Garben and I. Govaere, Hart Publishing, pp. 187–212; A. Renda, *Beyond the Brussels effect – Leveraging digital regulation for strategic autonomy*, FEPS – Foundation for European Progressive Studies, 2022.

both mainstream media and academic circles. Essentially, this means that not only is the GDPR influencing the behavior of foreign companies and governments, but it also impacts their access to the European Single Market. Disregarding European citizens' digital privacy would pose significant risks to non-EU entities, including organizations that heavily rely on big data (which encompasses virtually all commercial and non-commercial entities). Such disregard could endanger their profits and potentially exclude them from the largest consumer market worldwide.

As a result, this market power drives regulatory convergence towards European privacy standards. This convergence occurs through the formal adoption of privacy laws by national jurisdictions and the informal implementation of corporate codes of conduct inspired by EU principles.

Going further with the assessment of the connecting factors of the GDPR, the targeting and monitoring criterion for individuals in the EU has also been established to address this issue.[506] It entails that if a controller or processor processes the personal data of individuals located in the EU, even if the controller or processor is not established within the EU, the GDPR applies if the processing relates to the offering of goods or services to those individuals or the monitoring of their behavior within the EU. Notably, some versions of the GDPR use the term "residents" in the EU, implying that protection is limited to EU residents only.[507] In contrast, other versions

[506] Compared to the rules established in the repealed Directive, the GDPR represents an evolution. The Data Protection Directive concentrated on the equipment used for processing personal data by a controller not established in the EU. This approach was deemed excessive and a source of legal ambiguity because it could cover situations lacking a connection to the EU. For instance, it could apply to third-country citizens who are not residents of the EU.

[507] The term "residents" is used in the Spanish version and Portuguese versions of the GDPR, specifically in Article 3(2). The Spanish version can be found in Reglamento (UE) 2016/679 Del Parliamento Europeo y del Consejo de 27 de abril de 2016, while the Portuguese version is in Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Both versions relate to the protection of personal data and the free movement of such data, and they replace Directive 95/46/CE (General Data Protection Regulation, 2016 O.J. (L 119) 1). However, it is more appropriate to understand that

refer to data subjects "who are" in the EU, in line with GDPR recital 14, which covers "natural persons, whatever their nationality or place of residence."[508] The fact that the GDPR was amended in some versions compared to the Commission's proposal supports the latter interpretation.[509] Despite some language versions of the GDPR, it

protection must be applied to natural persons, regardless of their nationality or place of residence, as stated in GDPR recital 14.

[508] The English version of the GDPR, as well as the German, French, and Italian versions, use the phrase "data subjects who are" in the European Union in accordance with GDPR recital 14. The English version of the GDPR can be found in the GDPR, as cited before. The German version can be found in Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/45/EG (Datenschutz-Grundverordnung), 2016 O.J. (L 119) 1. The French version can be found in Règlement (UE) 2016/679 DU Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/45/CE (règlement general sur la protection des données), 2016 O.J. (L 119) 1. Finally, the Italian version can be found in Regolamento (UE) 2016/679 Del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), 2016 O.J. (L 119) 1.

[509] In this context, it is worth mentioning the issue of divergences among different language versions and how the Court of Justice applies methods of interpretation to reconcile diverging texts. First, it has to be considered that in EU law, discrepancies may occur between various versions of primary or secondary law, as well as, in the case of directives between a language version of a directive and the norm transposing into national law that directive in the same language. Essentially, such discrepancies may be either textual or conceptual. The CJEU has a substantial body of case law addressing linguistic discrepancies in different language versions of EU law (e.g., *ex pluribus* case 29/26 *Erich Stauder v City of Ulm, Sozialamt*, para 3; case 30/77, *Regina v Pierre Bouchereau*, para 14; case 283/81, *Cilfit*, para 18; case C-404/16, *Lombard Ingatlan Lízing*, para 21; case C-48/16, *ERGO Poist'ovňa*, para 37; joined cases C-443/14, *Ibrahim Alo* and C-444/14, *Amira Osso*, para 27; case C-74/13, *GSV*, para 27; case C-558/11, *Kurcums Metal* para 48). This issue was first addressed by the Court half a century ago, and since then, a standardized approach has been adopted. The CJEU consistently emphasizes that EU law should be interpreted and applied uniformly by considering all the language versions of the EU legislative text. In cases where discrepancies exist, the provision in question should be interpreted in light of the overall structure and purpose of the relevant rules. This obligation also extends to national courts when they apply and interpret EU law, as clarified in the landmark Cilfit judgment (case 283/81, para 18). The standardized approach allows the CJEU flexibility in assessing cases of linguistic discrepancy to ensure a consistent interpretation across all language versions. To achieve this goal, the CJEU employs two primary methods: a literal interpretation method, which involves comparing and reconciling the wording in different language versions, and a teleological-systematic method, which relies on the overall scheme and purpose of the rules under consideration. These methods are not mutually exclusive and can be combined in the interpretation process for a particular provision. For insight on this topic, see S. van der Jeught, *Current practices with regard to the interpretation of multilingual EU Law: how to deal with diverging language versions?* in *European Journal of Legal Studies*, 2018, pp. 5-38.

is more appropriate to maintain that protection must be applied to natural persons, regardless of their nationality or place of residence.

The processing of personal data of users to whom goods and services are directed is the determining factor that subjects the processing obligations of controllers and processors to the GDPR. Therefore, including clients or users residing in the EU indicates that the controller intends to offer goods and services to data subjects whose personal data is being processed in the EU.

Offering goods and services does not necessarily require payment by the data subject. The difficult task is determining when a controller or processor intends to provide services to data subjects in the EU. However, certain types of information are insufficient evidence to indicate that a trader is directing its commercial activity to an EU Member State where the consumer has their habitual residence.[510]

In this regard, the *Pammer* case provides a list of criteria that can offer guidance for interpreting Article 3(2)(a) of the GDPR. This list is not exhaustive but can help analyze whether a controller or processor intends to offer services to data subjects in one or more EU Member States. For example, a trader's email, geographical address, or telephone number without an international code does not indicate that a trader intends to conduct its activity in an EU Member State.[511]

Furthermore, it is worth mentioning that in a recent ruling involving the concepts of 'third country' and 'third State' (case C-632/20 P, *Spain v Commission*) the CJEU pinpointed that "according to settled case-law, the wording used in one language version of a provision of EU law cannot serve as the sole basis for the interpretation of that provision, or be made to override the other language versions" and that "Provisions of EU law must be interpreted and applied uniformly in the light of the versions existing in all the languages of the European Union and, where there is any divergence between those various versions, the provision in question must be interpreted by reference to the general scheme and the purpose of the rules of which it forms part (see, to that effect, C-422/19 and C-423/19, *Hessischer Rundfunk*, paragraph 65 and the case-law cited, and C-59/18 and C-182/18, *Italy and Comune di Milano* v *Council (Seat of the European Medicines Agency)*, paragraph 67 and the case-law cited)".

[510] See recital 23 GDPR: the mere accessibility of a website, an email address or other contact details or the use of a language generally used in the third country where the company is established is insufficient to ascertain such intention.

[511] See Joined Cases C-585/08 and C-144/09, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG & Hotel Alpenhof GesmbH v. Oliver Heller*.

On one hand, GDPR Recital 23 states that simply having a website accessible in the EU or using a language and currency generally used in one or more Member States is insufficient to establish that processing activities are related to offering goods or services in the EU. On the other hand, it is clear that when processing activities are related to the offering of goods or services, and the consumer or user can order goods and services by selecting a language and currency, then such activities are directed to one or more Member States.

Another relevant factor is the inclusion of clients or users domiciled in the EU. Additionally, the use of a top-level domain name other than that of the Member State in which the controller or processor is established, or the use of neutral top-level domain names such as ".com" or ".eu,"[512] can be further evidence that the controller intends to offer goods and services to data subjects in the EU. Therefore, when it is apparent from the evidence that the controller or processor intends to offer goods or services to data subjects in the EU, they must comply with the GDPR.

The offering of services also includes the offering of information society services,[513] regardless of whether a payment by the data subject is required in exchange.[514]

Considering only the user perspective who is using a Blockchain to broadcast a transaction to the network,[515] some of the Blockchain platforms may be considered an information society service as described by point (b) of Article 1(1) of Directive (EU) 2015/1535,[516] which is referred to by Article 4 (25) GDPR. In fact, it is a service normally

[512] *Ibidem,* para 83.

[513] Article 1(1) point (b) Directive (EU) 2015/1535: *"any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".*

[514] See Case C-352/85, *Bond van Adverteerders and Others vs. The Netherlands State*, 1988 para 16; Case C-109/92 *Wirth*, para 15.

[515] Nodes and miners are not taken into account, as their activity on the Blockchain constitutes part of the service.

[516] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241.

provided for remuneration, without the parties being simultaneously present, through electronic means and through data transmission on individual request.

Based on this assumption, it can be arguably affirmed that article 3(2) GDPR will apply to every public permissionless Blockchain, given that their purpose is to offer a service globally accessible. Moreover, although anyone can register an account on these blockchains, users are required to be subject to the terms and conditions of the intermediaries (wallets and exchanges) they contract with. However, the terms and conditions of the platforms that support public and permissionless blockchains do not usually address data protection. For example, the Bitcoin Core privacy policy's legal basis for processing data is unclear as there is no indication of any applicable law, and it was updated in July 2016.[517] In contrast, Ethereum's standard-form terms refer to their privacy policy,[518] which states compliance with the Swiss Federal Act on Data Protection ("FADP"), the Swiss Ordinance to the Federal Act on Data Protection ("OFADP"), and the GDPR. Ethereum contractually ensures that personal data protection always corresponds to that in Switzerland and the EU by using standard contractual clauses and complying with the GDPR. Nonetheless, the fact that the terms of use of the Ethereum website can change at the sole discretion of the Ethereum Foundation and are effective immediately could have a negative impact on users. This situation contrasts with private and permissioned blockchains and may make it difficult for Europeans to register on the platform and avoid being subject to the GDPR.

The final criterion for applying the GDPR is based on situations where Member State law applies by public international law, even if the controller is not established in the EU (Article 3(3) of the GDPR). This provision is not new and was already

[517] *See Privacy Policy*, BITCOIN, https://bitcoin.org/en/privacy (last access November 2023).

[518] *See Privacy Policy*, ETHEREUM, https://ethereum.org/privacy-policy/ (last updated 20 October 2023).

included in Directive 95/46. An example provided in GDPR recital 25 is a Member State's diplomatic mission or consular post.

4. Data Protection Concerns with Blockchain: Different Ontologies

The presentation of the basic concept of Blockchain technology and the overview of the GDPR requirements for processing personal data highlighted that conflict situations may arise when personal data is processed on Blockchain.

Distributing data among all participants in a network and making changes impossible are fundamental concepts of Blockchain technology. These features pose several challenges in relation to privacy regulations. As previously noted, the processing of personal data must adhere to the principles outlined in Article 5 of the GDPR.

Initially, some academic research publications highlighted the potential benefits of this technology in enhancing privacy protection, such as decentralized identity management, data sharing with trusted parties, and new solutions for cross-border data transfers.[519] However, subsequent literature publications delved deeper into the challenges posed by Blockchain to data protection,[520] with some concluding that public Blockchain features are "on a collision course with EU privacy law"[521] and are profoundly incompatible at a conceptual level with the principles of the EU General Data Protection Regulation (GDPR).[522] Some even warn of the risk of rendering Blockchain operation unlawful due to data protection legislation, thus stifling the

[519] G. Zyskind, O. Nathan & A. Pentland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data,* in *IEEE CS Security and Privacy Workshops*, 2015; M. Mainelli, *Blockchain could help us reclaim control over our personal data*, in *Harvard Business Review*, 2017; S. Sater, *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows, Tulane University*, 2017; D. Connor-Green, *Blockchain in Healthcare Data*, in *Intellectual Property & Technology Law Journal*, 2017; M. Mainelli, *Blockchain Will Help Us Prove Our Identities in a Digital World*, in *Harvard Business Review*, 2017.

[520] S. Schwerin, *Blockchain and Privacy Protection in the Case of The European General Data Protection Regulation (GDPR): A Delphi Study*, in *The Journal of The British Blockchain Association*, 2018, p. 19; T. Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 2017.

[521] D. Meyer, *Blockchain technology is on collision course with EU privacy law*, IAPP, 2018.

[522] M. Finck, *Blockchains and data protection in the European Union,* in *Max Planck Institute for Innovation and Competition Research Paper (MPI Paper)* No. 18-01, 2017, p 1.

development of innovative technology with great promise for the Digital Single Market.[523] Consequently, there has been a growing call for an urgent revision[524] to address the compatibility of Blockchain with the European Data Protection Legislation.

Although this will be discussed in detail below, it can be argued that the "mismatch" between Blockchain technology and the GDPR leads to an initial conceptual difficulty regarding whether these rules effectively apply to this technology and, if so, how they should be applied.

These conflicts essentially arise from two primary factors based on two distinct philosophies regarding protecting data privacy.
First, the Regulation, hinging the EU's perspective, views centralized governmental authority as essential for safeguarding consumers and their data against the abuses of private actors, particularly large data-driven tech companies. In contrast, Blockchain identity solutions emerged from the crypto-libertarian ethos of Bitcoin, which rejects centralized authority and believes that privacy rights are best protected through advanced cryptography and distributed networks that no entity can control.

Second, the GDPR seeks to enhance personal privacy by reordering and consolidating power within an established paradigm, while Blockchain seeks to achieve the same goal by fundamentally changing the paradigm. As a result, these approaches can lead to some fundamental inconsistencies in form, but not necessarily in substance, as they pursue different paths towards resolving the same issue.

[523] These concerns were fueled by statements from industry stakeholders, including Jan-Philipp Albrecht, the MEP responsible for coordinating the Parliament's input for the GDPR, who noted that Blockchain applications may not be GDPR-compliant due to the requirement for individuals to delete their data: "Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subjects' rights] based on their architectural design. This does not mean that Blockchain technology, in general, has to adapt to the GDPR, it just means that it probably can't be used for the processing of personal data.", see D. Mayer (2018), at 115.

[524] S. Ward, *Blockchain to Clash with New EU Privacy Law*, 2018, www.bestvpn.com/privacy-news/Blockchain-clash-new- eu-privacy-law; O. Avan-Nomayo, *Parity forced to shut down ICO passport service (Picops) due to GDPR*, 2018, bitcoinist.com/parity-forced-to-shut-down- picops-due-to-gdpr/.

The mentioned seeming inconsistency has been referred to as the Blockchain-GDPR Paradox.[525] Blockchain technology's challenges to GDPR compliance include immutability,[526] public accessibility (in the case of public blockchains), and the decentralized peer-to-peer organizational structure. Immutability and public accessibility conflict with the principle of data minimization and the rights of data subjects, such as the right to rectification (Article 16 GDPR), the right to be forgotten (Article 17 GDPR),[527] and the right to restriction of processing (Article 18 GDPR). Additionally, the peer-to-peer structure of blockchains creates difficulties in identifying the roles of the GDPR in a Blockchain environment,[528] such as controllers, joint controllers, processors, and data subjects.[529] Undoubtedly, identifying an individual or an entity as a Data Controller is significant because the GDPR assigns them the primary responsibility of implementing appropriate technical and organizational measures to safeguard personal data. Considering the nature, scope,

[525] A. Van Humbeeck, *The Blockchain-GDPR paradox,* in *Journal of Data Protection and Privacy*, *2*(3), 2019, pp. 208–212; A. Mirchandani, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR,* in *Fordham Intellectual Property, Media and Entertainment Law Journal*, *29*(4), 2019, p. 1201.

[526] Some authors do not agree with the idea of Blockchain as technology guarantying immutability: "Blockchain does not move from a system where trust is necessary to another based on code where trust is unnecessary. The literature usually refers to a "trusted" record, which suggests users begin to place confidence in the actors that make Blockchain infrastructure possible. Without confidence in the developers or in the intermediaries that act as service providers, users would not use a Blockchain system.", G. Jimènz, S. Briseida, *Risks of Blockchain for data protection: A European approach,* in *Santa Clara High Technology Law Journal*, 2020, p. 295.

[527] B. Sobkow, *Forget me, forget me not—redefining the boundaries of the right to be forgotten to address current problems and areas of criticism*, in E. Schweichhofer et al (eds), *Privacy technologies and policy, 5th Annual Privacy Forum*, APF 2017, Vienna, Austria, 7–8 June 2017, Revised selected papers, Springer, p. 36.

[528] The purpose of the Regulation is to ensure that information and access rights are exercised efficiently, primarily for the benefit of data subjects and secondarily for the benefit of controllers. The GDPR does not establish or define substantive rights but rather outlines technical and procedural requirements for the flow of information between controllers and data subjects. Essentially, it can be inferred that the substantive rights of data subjects can only be effective if clear, proportionate, and effective procedures support them. Therefore, the Regulation sets out conditions for informing data subjects, both actively and passively, about processing their personal data, including how and when such information should be provided.

[529] C. Lambrinoudakis, *The general Data Protection Regulation (GDPR) era: Ten steps for compliance of data processors and data controllers*, in *Proceedings of the International Conference on Trust Privacy and Digital Business*, Springer, 2018, pp. 3–8.

context, and purposes of data processing and associated privacy risks, the Data Controller must adopt proportional measures and ensure processing is conducted under GDPR standards and principles. [530]

In addition, there has yet to be a consensus on how to anonymize personal data stored on public networks, and the potential for re-identification raises concerns about the necessity, minimization, and privacy by design principles of the GDPR.[531]

Furthermore, article 25 of the GDPR outlines the legal requirements for "Privacy by Design" and "Privacy by Default." These terms signify that any data processing system must be designed and developed with data protection and privacy considerations in mind from the outset.[532] During the early stages of technology development, a company initiating the technology must implement adequate technical and organizational measures to ensure data confidentiality, integrity, and availability by default. The underlining idea is that data protection standards are best upheld when integrated into the technology during its creation. [533]

4.1.Roles and responsibilities for GDPR compliance in the Blockchain context

As mentioned, the GDPR and Blockchain have conflicting founding principles, creating tensions between the value of having a centralized entity responsible under the law and eliminating the need for a central authority under the technology.

In particular, allocating responsibility for various functions is complex within Blockchain technology. The absence of clear legal guidelines and discrepancies in interpretation among regulatory bodies in the European Union has led to a perception

[530] P. Voigt, A. von dem Bussche, *The EU general data protection regulation (GDPR): a practical guide*, Springer, 2017.

[531] M. Hintze, K. El Emam, *Comparing the benefits of pseudonymisation and anonymisation under the GDPR*, in *Journal of Data Protection and Privacy*, 2018, pp. 145–158.

[532] A. Cavoukian, *Evolving FIPPs: proactive approaches to privacy, not privacy paternalism*, in S. Gutwirth, R. Leenes, P. de Hert (eds), *Reforming European data protection law*, Springer, 2015.

[533] D. A. Tamburri, *Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation*, in *Information Systems*, 2020, p. 91.

of a loosening of regulations on Blockchain.[534] Moreover, the decentralized nature of the Blockchain makes it difficult to determine who is responsible for fulfilling the roles and duties outlined in the GDPR.[535] In other words, while the Data Protection Regulation emphasizes the importance of roles and responsibilities, the decentralized nature of Blockchain makes it hard to assign those roles.[536]

Blockchain decision-making and data processing challenge the obligations placed on data controllers by the GDPR, which identifies them as the primary responsible party for implementing measures to protect personal data, especially regarding security measures in response to a data breach.

Based on this presumption, some argued that distributed structures require the rethinking of legal categories since the notions of the 'author of an action', 'content' or 'object' are no longer tangible units but aggregated, open-ended and evolving fragments.[537]

The first step to identifying GDPR obligations is to determine the role that the different Blockchain actors take concerning the processing. Determining who acts as the controller is a crucial requirement since data subjects (i.e. individuals whose personal data is recorded on the Blockchain) must be informed about which entity

[534] See Chapter II of this thesis.

[535] The controller is responsible for implementing suitable technical and organizational measures to demonstrate compliance with GDPR requirements. This may involve adopting appropriate data protection policies, complying with data protection by design and by default requirements, and maintaining a record of processing activities that include information on processing purposes, data subject and personal data categories, recipient categories, personal data transfers, and time limits for erasure, as well as details on technical and organizational security measures. Additionally, at the time of personal data collection, the controller must provide the data subject with information, including its own identity and contact details. This emphasizes the pivotal role of the controller in EU data protection law, as it is responsible for implementing data protection measures from the outset and acts as the main point of contact for data subjects seeking to assert their rights.

[536] U. Tatar, Y. Gokce, B. Nussbaum, *Law versus technology: Blockchain, GDPR, and tough tradeoffs,* in *Computer Law & Security Review*, 2020, pp. 1-11.

[537] M. Dulong de Rosnay, *Peer-to-Peer as a Design Principle for Law: Distribute the Law,* in *Journal of Peer Production,* 2015, at p. 6.

they can refer to in order to exercise their rights effectively, and data protection authorities[538] must have a contact point which can be held accountable for the processing carried out: the first and foremost role of the controller is to be responsible for compliance with data protection rules and ensure data subjects can exercise the rights in place.[539]

According to the GDPR, entities processing personal data are classified as controllers, processors or joint controllers.[540] These categories were created when data management was centralized despite being neutral with respect of specific technologies.[541] Essentially, an entity[542] acts as a controller if it determines the means and purposes of processing personal data, while it is a processor if it processes data on behalf of a controller.[543] When the purposes and means are determined *jointly* by two or more subjects,[544] we are in the realm of joint controllers. There is, in practice,

[538] An identified data controller enables supervisory authorities to exercise their investigative and corrective powers under Article 58 of the GDPR, which may involve notifying controllers or processors of alleged infringements or any other communication necessary to fulfil their duties.

[539] R. Mahieu et al, *Responsibility for Data Protection in a Networked World. On the question of the controller, "effective and complete protection" and its application of data access rights in Europe*, in *Journal of Intellectual Property, Information Technology and E-commerce Law*, 2019, https://www.jipitec.eu/issues/jipitec-10-1-2019/4879.

[540] See Y. Ivanova, *Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World*, in M.Tzanou (ed.), *Personal Data Protection and Legal Developments in the European Union*, IGI Global, 2020.

[541] For an assessment of the GDPR claim to be technologically neutral, see paragraph 2 of Chapter IV.

[542] Article 4(7) GDPR says "a natural or legal person, public authority, agency or other body (…)".

[543] In Convention 108 there was a different definition, which included specific examples of what constitutes "control" in order to be recognized as a controller. This could involve factors such as identifying who has the authority under national law to determine the purpose of an automated data file, which categories of personal data should be retained, and which operations should be performed on them. Consequently, the traditional understanding of a controller, as defined by the Council of Europe Convention, played a more limited role in comparison to the broader and more dynamic scope of a "controller" under EU law.

[544] Recital 26 of the GDPR: "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects."

no legal rule for what happens when joint controllers fail to define the extent of their joint operations or properly allocate their obligations for GDPR compliance. In this context the Fashion ID ruling[545] raises the issue of whether the Court's new phase-oriented approach will be the exclusive means of delineating joint controllership or if other methods, such as evaluating whether they pursue common macro-objectives as suggested by WP29 or as implied by the Yehovah's witnesses' judgement, can also be employed. [546]

Determining the roles in the data protection ecosystem is based on factual evidence and the classification is specific to the processing being performed: an organization may act as a controller for a particular process related to a specific set of personal data while simultaneously acting as a processor for a different process related to the same set of personal data. Essentially, identifying the relevant data controller in relation to each personal data processing operation requires a thorough *case-by-case analysis* that considers all pertinent technical and contextual factors. This underlines that the concept of controllership is autonomous and should be interpreted solely based on EU data protection law. It is also functional, as its purpose is to allocate responsibilities based on factual influence rather than formal analysis.[547] Therefore, formal identification of a controller in a contract or terms and conditions is not decisive and may be superseded by a court decision that determines controllership based on factual considerations rather than formal ones.[548]

[545] Case C-40/17, *Fashion ID*, para. 67 (noting that 'since, as Article 2(d) of Directive 95/46 expressly provides, the concept of "controller" relates to the entity which "alone or jointly with others" determines the pur- poses and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing'). See further Case C-210/16, *Wirtschaftsakademie*, para. 29; Case C-25/17, *Jehovan todistajat*, para. 65.

[546] R. Mahie et al (2019) at p. 85.

[547] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, adopted on 7 July 2021.

[548] It is important to consider that the distinction between (joint) controllers and processors is crucial as it aims first and foremost to allocate different data protection responsibilities that have been further enhanced by the new accountability principle – one of the most important changes introduced with the GDPR with a view to bridging the existing compliance gap. That principle essentially aims to foster data protection in practice by obliging controllers to put in place appropriate and effective measures

Nonetheless, it cannot be hidden that there is legal uncertainty in how to apply these concepts, as the first major challenge is the inconsistent interpretation of the notions of (joint) controller and processor given by the EDPB and the CJEU. Moreover, this contradiction is even further complicated as companies may also be subject to divergent interpretations given by the national DPAs regarding their legal capacity and the scope and nature of their responsibilities.

How could GDPR roles be addressed in a decentralized environment?

When we described the technical features of Blockchain technology in the previous chapters, we specified that in the decentralized system, each node represents a participant and stores a copy of the ledger, but none have complete control over the technology. [549] However, each node impacts the outcome of a block, which amends or corrects the chain, making the technology decentralized and distributed. Notwithstanding, since nodes have limited influence over the broader ledger that each of them retains, it would be neither fair nor practical to impose all the obligations outlined by the GDPR for data controllers.[550] This means that the architecture and math of the Blockchain replace the trusted person or organization responsible for data.

for compliance with the GDPR and to be able to demonstrate, thus ensuring *de facto* effective compliance with existing principles and obligations and moving data protection from 'theory to practice'.

[549] T. K. Sharma, *Advantages and disadvantages of permissionless Blockchain*, Blockchain Council, Oct. 3, 2018, https://www.Blockchain-council.org/Blockchain/advantages-and-disadvantages-of-permissionless-Blockchain/; T. Buocz and others (2019), p. 182.

[550] In addition to initiating transfers, individuals running full nodes on the Blockchain network also participate in the storage of Blockchain transfers by verifying new transfers against the rules of the protocol. They are responsible for checking various aspects of the transfers, such as the correct digital signatures and data format. As a result, the household exemption under GDPR does not apply to full node since they contribute to disclosing transfers to an undefined public with an intensity that goes beyond what is typically considered a personal or household activity. Instead, given their level of activity, full node should be compared to businesses. Full node play a crucial role in the proper functioning of the Bitcoin network. However, they do not have the authority to determine the purposes or means of their activities independently. Consensus-building functions are automated and follow the rules outlined in the Blockchain code. Since individual users running full nodes of the Blockchain network cannot change the protocol by themselves or choose a different protocol within the respective Bitcoin client, they cannot be considered controllers.

While code and cryptography may be more reliable than traditional third-party data controllers in some ways, they are less human, less accountable, and less adaptable than their counterparts.

Can every node be a data controller?

According to the technological design described earlier, complying with the GDPR requirements is challenging.[551] Particularly, determining the purposes and means of processing involves technical and organizational considerations. Therefore, one may infer that if an entity chooses to use a Blockchain for personal data processing instead of another decentralized database, it has decided about the means of processing and is likely to be considered the data controller.[552]

Notwithstanding, the above considerations require a premise, leading to first investigating and asking *whether every node can be considered a data controller* and, before that, whether the individual members of the distributed network rather than the network as one partnership can be held responsible. In peer-to-peer settings, responsibility can be assigned to different combinations of individual peers (one peer, peers of a specific sub-group, all peers), all of which raise serious legal concerns. When responsibility is assigned to an individual or a sub-group of peers, those peers are accountable for particular outcomes instead of everyone being responsible for all outcomes. If, in a unique situation, these peers cannot be identified separately from the others (even if only by designation in the network), it would be difficult to justify holding them accountable from a legal perspective.

[551] "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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

[552] For instance, a consortium that uses Blockchain to manage its accounts or an insurance company that employs Blockchain for automated client payments will likely be data controllers as they determine the purposes for which the technology is needed. Consequently, they are responsible for complying with GDPR obligations related to the personal data processed through such systems.

Another approach is to assign responsibility to all peers, regardless of their specific impact on the network's actions. However, since the network composition is constantly changing, identifying the person behind a network node can be exceedingly challenging. Furthermore, since distributed networks are transnational, potentially spanning different jurisdictions, assigning responsibility becomes even more complicated and might result in excessive shared responsibility.

In this context, instead of defining these roles in theory, it may be essential to carefully assess them for each Blockchain system on its own merits. This evaluation may, therefore, distinguish between the participants who determine the data processing objective at the application layer instead of those involved in processing at the infrastructure layer. In general terms, participants who provide personal information to a Blockchain platform at the application layer may more likely be classified as controllers since they determine the purpose of the data processing to execute a transaction and the technical and organizational aspects of processing at the application layer. On the other hand, nodes and miners who only process data on behalf of users at the infrastructure layer ma more likely be considered processors rather than controllers, as their role might be seen as a 'facilitator' of the network's operation.

Interestingly, the activity of (full) nodes in a Blockchain system can be likened to Internet hosting, which receives information and routes it independently to another node until it reaches its destination. Users have little control over how autonomous systems route packets, and the processing performed by Blockchain nodes is arguably similar. The sole purpose of nodes is to ensure the integrity of the Blockchain and verify the addition of new blocks.

Likewise, as maintained above, miners who contribute to validating blocks by proof-of-work do not fall within the household exemption because they provide disclosing transfers to an undefined public in a way that goes beyond simple private or household activities.

Although miners also make essential contributions to the functioning of the network, they cannot determine the purposes or means of these activities by themselves; instead, they are subject to the so-called 'consensus protocol'.[553] Therefore, individual miners cannot be considered controllers either.[554] It is more likely that they qualify as data processors, although some commentators oppose that users neither know the miners nor have a contractual relationship with them.[555]

Against this backdrop, another question arises. In the framework described, *could users qualify as controllers when they decide to use a Blockchain for a specific transaction, whereby the individual would be both a data subject and a data controller?* The controversy stems from the consideration that users decide what information is included in a transaction and, by this means, determine the details of processing.

The most compelling argument regarding the user's role revolves around the idea that when a user decides to utilize a Blockchain or Blockchain-based application, they effectively become the determinants of both the "purposes" and "means". As a way of example, Duarte[556] asserted that when a user opts for a Blockchain network, even in

[553] R. H. Weber, "*Rose is a rose is a rose is a rose" – what about code and law?',* in *Computer Law & Security Review*, 2018, at p. 701; L.F.M. Ramos, J.M.C. Silva, *Privacy and data protection concerns regarding the use of Blockchains in smart cities,* in *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, ACM,* 2019, pp. 342-347.

[554] Some authors hold a different perspective. Ibáñez et al. put forth the argument that miners could potentially be regarded as controllers, as they exert influence over why and how their individual local versions of the block are processed. Additionally, other researchers have concurred that, in theory, every miner participating in a public Blockchain network could meet the criteria to be considered a controller. See L.-D. Ibáñez, K. O'Hara, E. Simperl (2018); D. Hofman, V.L. Lemieux, A. Joo, D.A. Batista, *The margin between the edge of the world and infinite possibility": Blockchain, GDPR and information governance,* in *Record Management Journal*, 2019, pp. 240-257; R. Herian, *Regulating disruption: Blockchain, GDPR, and questions of data sovereignty*, in *Journal of Internet Law*, 2018, pp. 8-16.

[555] M. Schellekens, *Conceptualizations of the controller in permissionless Blockchains,* in *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 2020, pp. 215-227.

[556] D. G. Duarte (2019), cit.

the presence of various payment methods and platforms, they are essentially deciding the "means" of making a transaction and by extension, determining the "purpose." Conversely, Buocz et al.[557] presented a contrasting viewpoint: despite users having practical control over the process by being able to connect to the Blockchain and disengage at will, it remains uncertain whether they possess the authority to dictate both the means and the purpose of the processing. Moreover, another issue seems to be represented by the difficulty/impossibility for a user to fulfil the responsibilities of a controller, exercising the necessary control over the full nodes and deleting data from the Blockchain.[558] In this respect, some commentators recommended the use of a contract that would include the terms and conditions to be agreed upon whenever a user, a node, or a miner first uses a Blockchain system.[559]

In light of the above discussion, labelling users as controllers within a public Blockchain system may not be warranted.

The issue of understanding the role and responsibility of users in platforms is not a new issue. In fact, the internet (especially social media networks) had previously posed a comparable dilemma, which has already been adequately resolved within the EU's data protection framework. The fundamental issue was articulated by the International Working Group on Data Protection in Telecommunications back in 2008:[560]

> *With respect to privacy, one of the most fundamental challenges may be in the fact that most of the personal information published in social networks is being published at the initiative of the users and based on their consent. While 'traditional' privacy regulation is concerned with*

[557] T. Buocz et al (2019), cit.

[558] M. Schellekens (2020), cit.

[559] M. Al-Abdullah et alt (2020), cit.

[560] International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services – Rome Memorandum* (2008), https://www.gpdp.it/documents/10160/10704/1531476 , p 1.

> *defining rules to protect citizens against processing of personal data by the public administration and businesses.*

Social media networks contended that they were not responsible (i.e., did not meet the criteria for being a controller) for processing personal data that data subjects themselves had published on their platforms. This raised the question of whether EU data protection laws were intended to safeguard data subjects from their own actions. The Working Party 29 provided clarity on this matter in its 2009 opinion on the application of EU data protection law to social networks:[561]

> *Social Network Service (SNS) providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the 'basic' services related to user management (e.g. registration and deletion of accounts) and SNS should ensure privacy-friendly and free of charge default settings.*

Using this rationale in the context of Blockchain, the responsibility for providing the "means for processing user data" lies with the organization that offers the Blockchain, whether independently or in collaboration with others. Consequently, this organization is accountable for ensuring that these "means" are created in accordance with privacy-by-design principles. This essentially leads to maintaining that stakeholders cannot merely introduce new technologies and evade responsibility for their usage.[562] But, *would that mean that Blockchain developers are the most suitable for the role of controllers?* To answer this question, it is first essential to enquire who determines the content of the code, the so-called 'governance of the infrastructure'. We maintain that although only a group of a few so-called 'core developers' have control over inputs within the Blockchain network, they cannot, in practice, decide

[561] Art. 29 Data Protection Working Party, Opinion 5/2009 on online social networking (2009), http://collections.internetmemory.org/haeu/20171122154023/http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf , p. 5.

[562] C. Wirth, M. Kolain, *Privacy by Blockchain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data*, Reports of the European Society for Socially Embedded Technologies (2018), https://dl.eusset.eu/server/api/core/bitstreams/44cc37bc-635e-4bef-a547-18bee83bcba3/content, p 5.

what version of the code will be used since anyone can alter it at any time in the permissionless Blockchain.[563] Therefore, the capacity of developers is limited to developing tools, and it is up to participants of the Blockchain system to decide how those developed tools are used.[564] For instance, the core developers of the Bitcoin protocol determine the content of this proposal,[565] but cannot decide how data will be processed within the Blockchain network.[566] Bitcoin Core is indeed best understood as a proposal for a set of rules.

Moreover, it is interesting to draw some observations on the responsibilities of smart contract developers. Some researchers have contended that smart contract developers

[563] For instance, taking into consideration Bitcoin, to understand who determines which set of rules are used in the Bitcoin protocol, one needs to examine situations where these rules change. There are two ways in which consensus on the Bitcoin protocol can be broken. If the rule set is restricted, a "soft fork" may occur, which is backward-compatible with the old rules. On the other hand, if the rule set is relaxed, a "hard fork" may occur, which is not compatible with the old rules and results in a permanently divergent Blockchain, essentially creating a new cryptocurrency out of the new part and splitting the network. Attempts have been made to create hard forks to increase the block size limit of 1 Megabyte, such as Bitcoin XT, Bitcoin Unlimited, and Bitcoin Classic, but they did not receive enough support from the network to establish a new branch of the Blockchain. However, Bitcoin Cash, Bitcoin Gold, and Bitcoin Private did succeed in creating a new branch. See J. Atik, G. Gerro, *Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice*, in *Stanford Journal of Blockchain Law & Policy*, 2018.

[564] N. Eichler et al (2018), cit.

[565] The hard fork scenario does not provide new insights into determining the controller of Bitcoin because it splits the network rather than changing the rules within the existing Bitcoin network. Soft forks, on the other hand, illustrate how new rules are adopted within the existing Bitcoin network. Those who have the ability to carry out a soft fork also have the power to determine the Bitcoin protocol rules, thereby determining the purposes and means, or the "why" and "how," of data processing.

To successfully implement a soft fork, a combination of users running full nodes and miners is required. Full nodes are responsible for enforcing the new rules, while miners create blocks that comply with these new rules. If all miners adopt the new rule proposal but no full nodes verify transfers against the new rules, mining becomes pointless and has no chance of economic survival. Similarly, if all full nodes adopt the new rule set but no miners create blocks that comply with these rules, transfers cannot be added to the Blockchain. *Therefore, a combination of users running full nodes with sufficient economic power and miners with sufficient processing power is necessary*. These specific majorities determine the purposes and means of the data processing conducted in the Bitcoin network. Mining pools that aggregate and increase their processing power through off-chain pooling are especially capable of providing this combination of users running full nodes and miners. See T. Buocz, T. Enrke-Rabel, E. Hodl, I. Eisenberger (2019), at p.196.

[566] See J. Erbguth, J. G. Fasching, *Wer ist Verantwortlicher einer Bitcoin-Transaktion?*, in *Zeitschrift für Datenschutz*, 2017, at p. 564, who argue that the developers cannot influence the use of the software or what data is to be stored in the transfers.

should be categorized as data processors, as they handle personal data on behalf of data controllers, as stipulated in Article 28 of the GDPR.[567] Ramos and Silva[568] advanced the argument that miners could similarly be seen as processors since they adhere to the data controller's directives when verifying whether a transaction complies with the established technical criteria. Dutta et al.[569] pointed out that both smart contract developers and the smart contracts themselves could potentially fall under the classification of data processors.

As a consequence, core developers cannot be considered controllers, either.

Are nodes in a Blockchain network joint controllers?

Furthermore, it lasts to assess whether a Blockchain network constitutes joint controllership. Some academics have argued against it, claiming that the rules of a Blockchain network do not arise from an agreement of the nodes but merely from the sum of their independent behavior.[570] However, the fact that nodes have equal influence and liberty to choose (or initiate) a particular Blockchain network and

[567] J. Erbguth (2019), cit;

[568] L.F.M. Ramos et al (2019), cit.

[569] Dutta et al (2020), cit.

[570] A.E. Dekhuijzen, *Call for action on the EDPB to provide guidance concerning GDPR and Blockchain: Is public Blockchain sustainable under the GDPR?*, in *Computer Law Review International,* 2019, pp. 33-36; J. Ahmed, S. Yildirim, M. Nowostawski, M. Abomhara, R. Ramachandra, O. Elezaj, *Towards Blockchain-based GDPR-compliant online social networks: challenges, opportunities and way forward,* in *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC)*, vol. 1, Springer (2020), pp. 113-129.

modify the rules with the necessary majority or through a fork[571] suggests otherwise.[572] While the need for an intention to agree may be debatable, these points make a compelling argument for treating Blockchain networks as a subset of a joint controllership, necessitating a transparent agreement on responsibilities for compliant usage (with possible sanctions for non-compliance). This would compel Blockchain developers to consider data protection liability during the design phase, adding another layer of privacy considerations. The described approach could significantly impede the adoption of Blockchain networks and hinder the innovative potential of decentralization underlying Blockchain technology. It could lead to a situation where a supervisory body can select any node of a (permissionless) Blockchain network and penalize them for the collective behavior of thousands of other anonymous users.

In the framework described, other relevant concerns involve the identification of *the legal responsibilities of controllers,* which undoubtedly face significant challenges. The distributed nature of Blockchain networks and the absence of identifiable managing partners and clear allocation of responsibilities make enforcement issues unclear.[573] The absence of statutory representatives within a collective entity poses

[571] Forking refers to the process of updating a cryptocurrency protocol or code by dividing a chain of blocks into branches. This occurs when members of a community cannot reach a consensus on the consensus algorithm and new transaction validation rules. In software development, a fork is the creation of a distinct program from the original or legitimate program by using the source code of the existing one. This practice is commonly employed in open-source or free software projects. In Blockchain networks, forks are utilized to establish new projects that begin from a previous one and replace it. For a deeper analysis see F. Schär, *Blockchain forks: A formal classification framework and persistency analysis*, in *Singapore Economic Review*, 2020, pp. 1-11; T. Neudecker, H. Hartenstein, *Short Paper: An Empirical Analysis of Blockchain Forks in Bitcoin*, in *Lecture Notes in Computer Science*, pp. 84–92.

[572] Jaccard and Tharin argued that when a number of full nodes form more than 50% of all mining power, they should qualify as joint controllers (see G. Jaccard, A. Tharin, *GDPR & Blockchain: the Swiss take, jusletter IT*, https://lawded.ch/wp-content/uploads/2019/07/Jusletter-IT_gdpr-Blockchain-t_5aebbf8be4_en.pdf).

[573] M. Finck (2018); C. Lima, *Blockchain GDPR privacy by design: how decentralized Blockchain Internet will comply with GDPR data privacy*, 2018, https://Blockchain.ieee.org/images/files/pdf/Blockchain-gdpr-privacy-by-design.pdf; G. M. Riva, *What happens in Blockchain stays in Blockchain. A legal solution to conflicts between digital ledgers and privacy rights,* in *Frontiers in Blockchain*, 2020.

ambiguities for legal enforcement authorities. Determining how responsible parties should address Blockchain security, especially in the event of a data breach, remains a difficult question. Furthermore, according to the GDPR, data subjects should have a contact person to exercise their rights, such as the right to access and the right to object to data processing. Decentralized and automated Blockchain systems lack a single point of contact for such requests.[574]

One possible solution could be assigning responsibilities to all Blockchain network peers.[575] However, the fact that peers continually change makes identifying the individuals behind network nodes very challenging. To address these challenges, it may be an obligation to identify a person or entity as the representative of all users in a given Blockchain network before joining the system.[576] Notwithstanding, this approach would theoretically require numerous agreements in place, and it may be practically unfeasible to establish joint agreements among all participants and the node operators.[577]

4.1.1. Interim results and the implications of Blockchain technology for data protection

The previous paragraph's analysis revealed that data processing in the Blockchain network is not determined by individuals running nodes nor miners, who essentially carry out their activities based on the rules outlined in the protocol created by the developer community. However, only a collective of users running full nodes and miners with sufficient economic and processing power can adopt and enforce the protocol. This entails that determining the purposes and means of data processing in

[574] R. Teperdjian (2020).

[575] T. Buocz et al (2019).

[576] U. Tatar et al (2020).

[577] S. Wrigley, *"When people just click": Addressing the difficulties of controller/processor agreements online*, in M. Corrales, M. Fenwick, H. Haapio, (eds), *Legal Tech, Smart Contracts and Blockchain*, 2019, pp. 221-252.

the (permissionless) Blockchain network lies with this collective, which may be considered the controller under Article 4(7) GDPR, or its members may be joint controllers under Article 26 GDPR.

Even if this network were to be regarded as a partnership and, therefore, a controller within the meaning of Article 4(7) GDPR, there would still be enforcement challenges. The network differs from traditional centralized partnerships in that it has numerous partners without identifiable managing partners, and the partners are often unknown to each other.[578] Additionally, contrary to traditional partnerships, interactions between partners occur primarily on a remote and virtual basis.

Finally, the peer-to-peer network is based on shared responsibility without representation. Holding a collective responsible without statutory representatives would require legal enforcement bodies to select them.

An alternative approach would be to consider individual members responsible as joint controllers under Article 26 GDPR. On the one hand, joint determination of the purposes and means of data processing would require a clear and transparent allocation of responsibility, which is not typical of nodes' relationships.

On the other hand, Article 26 of GDPR does not mandate a "clear and transparent allocation of responsibility" as a defining characteristic of joint controllers. Instead, it requires that they determine their respective responsibilities transparently. Otherwise, persons carrying out data processing could circumvent obligations under the GDPR simply by setting up unclear and non-transparent structures within their partnership. Even so, the group of joint controllers is continually evolving, identities are difficult to establish, and causal relationships need to be clarified. Proving that a particular node was active during a GDPR violation would be challenging.

[578] As a matter of fact, lawful processing of personal data would require all nodes holding personal data to be known by the users as joint controllers, which is impossible for public Blockchain systems. Cfr. L. Campanile, M. Iacono, A.H. Levis, F. Marulli, M. Mastroianni, *Privacy regulations, smart roads, Blockchain, and liability insurance: putting technologies to work*, in *IEEE Security and Privacy*, 2020, pp. 34-43.

Additionally, identifying individuals behind a network peer would be complex, given that millions of users worldwide operate under pseudonyms.

Thus, both proposed solutions - considering the partnership as the controller under Article 4(7) GDPR and individual members as joint controllers under Article 26 GDPR - encounter similar challenges. In both cases, the controller is responsible for complying with the GDPR's principles of personal data processing and implementing appropriate technical and organizational measures to ensure lawful processing. A critical responsibility is ensuring that personal data processing is lawful, as the GDPR operates on a "prohibition with permit reservation" system. Unless one of the legal grounds under Article 6(1) GDPR applies, personal data processing is unlawful. For the Blockchain network, possible legal grounds include consent,[579] contract performance, public interest, or legitimate interests of the controller(s) or a third party.[580] The controller must also facilitate the data subject's exercise of data protection rights, which may be difficult to guarantee in a decentralized network.

As this discussion highlighted, the identification of data protection roles and responsibilities is undoubtedly one of the main battlegrounds in the debate between GDPR and Blockchain.

4.2. Applying the principles of lawfulness, fairness and transparency

The decentralized nature of Blockchain networks poses a challenge to the principle of lawfulness of processing, particularly in cases where personal data is processed based on consent.[581] Extensive research has been conducted on managing consent in

[579] See, EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, adopted on 4 May 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[580] Article 6 of the GDPR.

[581] P. Van Eecke, A.-G. Haie, *Practitioner's corner • Blockchain and the GDPR: the EU Blockchain observatory report*, in *European Data Protection Law Review*, 2018, pp. 531-534.

public blockchain systems while ensuring compliance with legal requirements. This subsection summarizes such studies and explores an alternative lawful basis for processing known as "legitimate interest." Moreover, it recalls the discussion on transparency in public blockchains.

4.2.1. Consent management

Several researchers have proposed smart contracts to manage data subject consent in different contexts effectively.[582].

These smart contracts enable the translation of privacy preferences into automated rules, allowing individuals to control and verify access to their personal data by third parties.[583] While the specific contexts may vary, the underlying strategy of using smart contracts for GDPR-compliant consent management remains consistent across these studies. The goal is to prevent unauthorized data access,[584] provide evidence of

[582] For instance, smart contracts have been suggested in the healthcare and financial sectors to protect sensitive personal data according to GDPR regulations. Education is another area where smart contracts can facilitate the secure transfer of personal data among educational stakeholders, including educational and professional records. Additionally, smart contracts have been proposed as a solution to address consent management challenges in online social networks.

[583] J. Erbguth (2019); C. Wirth, M. Kolain, *Privacy by Blockchain design: a Blockchain-enabled GDPR-compliant approach for handling personal data*, in *Proceedings of 1st ERCIM Blockchain Workshop*, 2018; F. Molina, G. Betarte, C. Luna (2021); U. Pagallo, E. Bassi, M. Crepaldi, M. Durante, *Chronicle of a clash foretold: Blockchains and the GDPR's right to erasure*, in *Legal Knowledge and Information Systems*, 2018, pp. 81-90; K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou, *Blockchain-based consents management for personal data processing in the IoT ecosystem*, in *Proceedings of the 15th International Joint Conference on E-Business and Telecommunications*, 2018, pp. 572-577.

[584] Heiss et al. delved into the realm of consent violation detection within a publicly verifiable framework. Their ingenious solution, grounded in smart contracts, was meticulously crafted to assist service providers in fulfilling three specific obligations: creating an auditable repository of consent policies, implementing robust technical measures to ensure and demonstrate the legally sound processing of personally identifiable data, and promptly reporting any consent breaches to the supervisory authority. See J. Heiss, M.-R. Ulbricht, J. Eberhardt, *Put Your money where Your mouth is – towards Blockchain-based consent violation detection*, in *Proceedings of the 2020 International Conference on Blockchain and Cryptocurrency, IEEE*, 2020.

Similarly, in the architectural framework proposed by de Sousa and Pinto, the evidence of a data subject's consent found its sanctuary within the Blockchain. This ingenious design allows regulators to seamlessly navigate the Blockchain when the need arises to validate consent. In another notable work by the same authors, the storage of proof for consents was introduced as a guardian of persistent privacy violations and individuals with greater control over their personal information.[585]

4.2.2. Legitimate interest

Legitimate interest serves as a lawful foundation for processing personal data, affording data controllers and processors flexibility under specific conditions. This flexibility is applicable when personal data is used in predictable ways, resulting in minimal privacy implications, or when a compelling rationale exists for the processing.

consents and evaluations. The interesting aspect of this approach lies in its ability to ensure the unwavering integrity of consents, offering a novel layer of protection for data privacy. See H.R. de Sousa, A. Pinto, *On the feasibility of Blockchain for online surveys with reputation and informed consent support Ambient Intelligence – Software and Applications*, in *9th International Symposium on Ambient Intelligence,* 2018, pp. 314-322; H.R. de Sousa, A. Pinto, *Blockchain based informed consent with reputation support*, in *Blockchain and Applications: International Congress*, Springer, 2019, pp. 54-61.

Another study echoed the advantages of immutably recording user consents and updates within the Blockchain. This innovative approach tethered consents to the data, bolstering data privacy. Moreover, the study contrasted its solution with traditional text-based methods, illustrating the transformation of consents into easily manageable switchable buttons. This intuitive design empowers users to express their consents effortlessly by toggling the button preference on or off. See X. Pei, X. Li, X. Wu, L. Sun, Y. Cao, *UDPP: Blockchain based open platform as a privacy enabler*, in *Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference,* 2020, pp. 500-505. Wirth and Kolain embarked on a slightly different path, where smart contracts gained access to a securely hosted decryption function. In their envisioned framework, the data subject emerged as the sole guardian of the decryption key, enabling them to receive real-time notifications whenever their personal data was accessed. See C. Wirth, M. Kolain (2018).

[585] Neisse et al. proposed three models with different contract structures based on the number of data subjects and controllers. In the first model, privacy preferences of data subjects are embedded in specific smart contracts deployed in the Blockchain for each controller or processor receiving their data. The second model involves creating smart contracts for each data item to be shared among multiple data controllers, allowing control at the granular level. Finally, the third model enables each controller to express their privacy conditions in a smart contract with an interface that allows users to join (give consent) or leave the contract (withdraw consent), see R. Neisse, G. Steri, I. Nai-Fovino, *A Blockchain-based approach for data accountability and provenance tracking,* in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017.

Numerous research endeavors have explored the legitimate use of Blockchain systems, often presented as a counterargument against the right to be forgotten requirement, as the research will explore in the following pages.

In this regard, it could be contended that individuals deciding to participate in a Blockchain are essentially aware that their personal data will be processed for the entire duration of the Blockchain's existence, which, theoretically, could extend indefinitely.[586] Therefore, it could be claimed that, as long as data subjects are well-informed regarding this perpetual duration and understand that each member's personal data is vital for the intended data processing, the right to erasure does not apply.

A comparable perspective was articulated by other researchers,[587] who posited that when users provide their consent for their data to be permanently recorded on the Blockchain, the irreversible nature of this opt-in mechanism does not run afoul of the GDPR.

An alternative viewpoint centres on the adaptable interpretation of data deletion as prescribed by the GDPR. This perspective argues that considering the fundamental principles of Blockchain operation, data stored within blockchains remains necessary for processing purposes, as these systems are inherently designed to be immutable.[588] According to these studies, such arguments offer legal grounds for permanently processing personal data within blockchains.

Other researchers[589] asserted that the legitimate interests of independent users should take precedence over the privacy requests of a single data subject to ensure network functionality and data integrity. However, it was emphasized that this

[586] S. Daoui, T. Fleinert-Jensen, M. Lemperiere, *GDPR, Blockchain and the French data protection authority: many answers but some remaining questions*, in *Stanford Journal Blockchain Law & Policy*, 2019, pp. 240-251.

[587] R. Mannan, R. Sethuram, L. Younge (2019).

[588] M. Berberich, M. Steiner (2016).

[589] N. Walters, *Privacy law issues in Blockchains: an analysis of PIPEDA, the GDPR, and proposals for compliance*, in *Canadian Journal of Law and Technology*, 2019, pp. 276-305.

argument can only hold if the design of the public Blockchain adheres to specific privacy standards. On the other hand, Zemler[590] cautioned that due to the absence of legal precedents in this domain, these legal arguments should be approached carefully as they might be deemed illegal by a court in the future.

Fundamentally, the inclusion of 'legitimate interests' within the GDPR allows for substantial flexibility in interpreting the regulation to accommodate Blockchain-based data protection solutions. We will return to this topic again in the following analysis.

4.3. How could data subject rights be upheld in the Blockchain context?

The GDPR was designed to give control back to individuals. It achieved this by strengthening individuals' rights against data controllers and introducing new rights.

Articles 15 to 22 of the GDPR grant data subjects specific rights. Data controllers are responsible for facilitating the exercise of these rights and cannot delegate this duty to processors. Some of these rights do not pose any specific issues in the context of Blockchain technology, while others present technical and legal challenges. The solutions to these challenges depend partly on the data controller's identity and their control over Blockchain data. Applying these data subject rights to distributed ledgers can only be thoroughly evaluated through a case-by-case analysis considering each personal data processing operation's specific technical and contextual circumstances.

In addition to minimizing risks to individuals, how data is registered on a Blockchain can also facilitate the exercise of individual rights.

Certain rights are well-suited to a Blockchain environment. For instance, the right to be informed can be met by requiring the data controller to provide concise and easily

[590] F. Zemler, *Concepts for GDPR-compliant processing of personal data on Blockchain: a literature review,* in *Anwendungen und Konzepte der Wirtschaftsinformatik,* 2019, pp. 96-107.

accessible information in clear terms (e.g. through a so-called privacy policy) before the data subject submits their information. Similarly, the right to access and data portability can also be facilitated in the Blockchain context.
On the contrary, some rights pose unique challenges due to the immutable nature of blockchains. These include the right to erasure, the right to object, and the right to rectification on which the analysis will focus, along with the other data subjects' rights.

4.3.1 The right to Access

The right to access is foundational in European data protection law because it enables and often serves as a prerequisite for exercising data subject rights and other fundamental rights. By accessing their personal data, data subjects can understand what data is being processed by the data controller, which is often necessary before exercising any other right. For example, the right to access allows data subjects to verify the accuracy of personal data, which may prompt them to exercise their right to rectification under Article 16 of the GDPR. Thus, Article 15 of the GDPR[591] is a pivotal right critical to the overall structure of European data protection law.

[591] "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative

When a data subject requests access, the controller must search all its electronic and paper-based records to provide the requested information. Therefore, if a data controller uses a Blockchain to process personal data, it must determine whether the database contains information about the data subject. While there are generally no impediments to implementing Article 15 of the GDPR in the context of blockchains, since the data is available to the members of the network,[592] it is essential to have adequate governance mechanisms in place to enable effective communication and data management.

Data subjects can direct requests for access to the data controller or any joint controllers as per Article 26(3) of the GDPR. However, along with the already mentioned difficulties in identifying the data controllers, it has been highlighted the challenge nodes face in knowing exactly which data is stored on a Blockchain, making it difficult to provide data subjects with information about processing their personal data.[593] In this respect, some authors[594] suggested that in order to comply with the right of access in a Blockchain system, policies should be provided to data subjects, explaining the technical details of how the network functions. This thesis is based on

costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

[592] F. Molina et al (2021), cit; D. Schmelz, G. Fischer, P. Niemeier, L. Zhu and T. Grechenig, *Towards Using Public Blockchain in Information-Centric Networks: Challenges Imposed by the European Union's General Data Protection Regulation*, in *2018 1st IEEE International Conference on Hot Information-Centric Networking*, 2018, pp. 223-228; M. Poelman and S. Iqbal, *Investigating the Compliance of the GDPR: Processing Personal Data On A Blockchain*, in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy* (CSP), 2021, pp. 38-44.

[593] For instance, nodes typically only see encrypted and hashed data, which means they may be unable to determine whether the distributed ledger contains personal data related to the data subject initiating the access request. This creates challenges in fulfilling the requirement to provide a copy of the personal data undergoing processing to the data subject under Article 15(3) of the GDPR. Therefore, organizations that use Blockchain technology to process personal data must ensure that appropriate governance arrangements are in place to effectively exercise the right to access. See, D. G. Duarte (2019).

[594] M. Al-Abdullah (2020).

the idea that controllers in a Blockchain system only handle encrypted or hashed versions of data rather than the actual data itself.

On the other hand, the EU Blockchain Observatory and Forum and other experts raise concerns about the enforcement of the right of access in public Blockchain systems, as data subjects do not have a designated contact person to whom they can request information regarding the processing of their data and the purposes behind[595] it nor is it a precise mechanism for data subjects to exercise their right of access.[596]

These perspectives highlight the challenges associated with ensuring the right of access in Blockchain systems, including the need for clear policies and agreements, the difficulty in identifying the data stored on the Blockchain, and the absence of a designated contact person (i.e. the controller) for data subjects to approach.

4.3.2. The right to rectification

Blockchains are designed to make the deletion and modification of data complex and ensure data integrity and trust in the network. This challenges the GDPR's requirement that data be 'accurate' and 'up to date', which, however, needs more precise definitions for data accuracy, up-to-dateness, and completeness. There is indeed a shortage of literature and case law addressing the concept of data accuracy in data protection law.

To date, the interpretation of the concept of data accuracy has been provided by the Article 29 Working Party, now known as the European Data Protection Board

[595] T. Lyons, L. Courcelas, K. Timsit, *Blockchain and the GDPR: a Thematic Report Prepared by the European Union Blockchain Observatory and Forum*, Thematic Report European Union Blockchain Observatory and Forum, 2018, https://www.euBlockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

[596] G. M. Riva (2020).

(EDPB).[597] According to the Article 29 Working Party, accuracy is defined as data that is 'accurate as to a matter of fact.' Inaccuracy in factual data refers to information that is not objectively precise and does not align with reality. Additionally, legal principles and case law have established that accuracy depends on purpose and context. This implies that data must be accurate enough for the specific processing purpose but not excessively precise. Therefore, there is a certain level of flexibility in determining the required degree of accuracy for the data.

Regarding non-factual data, there is ongoing discussion about whether the principle of accuracy extends to non-factual information, such as inferences or opinions. Some authors argue that applying the accuracy principle to non-factual data is challenging, as it is difficult to determine their accuracy or inaccuracy. In contrast, others maintain that accuracy applies to inferential data because they still qualify as personal data.[598]

Blockchains often cannot support reversibility, which creates difficulties in rectifying data, such as when a customer requests a service provider using Blockchain to correct information in their record. Private and/or permissioned blockchains can facilitate such requests by altering the relevant transaction record by re-hashing subsequent blocks, subject to the technical and governance set-up.

Rectifying data on public and/or permissionless blockchains is significantly more complicated, and individual actors may need help to comply with such requests.

Some authors maintained that Article 16 of the GDPR[599] allows incomplete data to be completed by providing a supplementary statement, which is easier to implement in

[597] Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-131/12, (WP 225, 26 November 2014), p. 15.

[598] Cfr. D. Hallinan, F. Zuiderveen Borgesius, *Opinions can be incorrect! In our opinion: on data protection law's accuracy principle,* in *International Data Privacy Law*, 2020.

[599] The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

distributed ledgers since any party with writing rights can add new data to the ledger to rectify previous information. It has also questioned whether adding new information on-chain could be a satisfactory means of achieving compliance with the right to rectification, mainly if there is a strong case for the data to be removed and replaced, such as in scenarios where a data subject cannot rely on the right to erasure since none of the grounds in Article 17(1) of the GDPR apply.

In the *Nowak* case, it was argued that the right to rectification should be judged by reference to the purpose for which the data was collected and processed.[600] Thus, providing a supplementary statement might only sometimes be satisfactory, mainly where a data subject cannot rely on the right to erasure. Conversely, where Article 17(1) of the GDPR does not apply, the mere provision of additional information may be sufficient, and the data subject may not be interested in data erasure.

Undoubtedly, requests of rectification, where the addition of supplementary information would be sufficient to rectify the data, could be complied with the data subject on its own or by any node through the broadcasting of new transactions to the network. Yet, rectification by substituting erroneous data with correct data will remain problematic due to the difficulties in changing the Blockchain history.

Essentially, while single nodes could modify their version of the ledger, this would only result in their version differing from the actual version shared by at least 51% of nodes in the network. Additionally, changing data stored in past blocks and making the change effective for most nodes would require a hard fork. However, an "old" chain version containing erroneous data would still exist, potentially leading to data inconsistency and confusion, and other miners and nodes who disagree with the hard fork could continue using it. In any case, it is incorrect to assume that compliance with these requests could be achieved by a periodical Blockchain fork, as suggested by

[600] Opinion of AG Kokott in Case C-434/16, *Peter Nowak*, para 35.

some scholars,[601] because erroneous data could continue to be processed in the old version.

4.3.3. Right to erasure through the prism of Blockchain

The right to erasure under the GDPR is a crucial tool for achieving greater control over personal data that pertains directly or indirectly to data subjects. Article 17 of the GDPR allows data subjects to request the "erasure" of personal data from data controllers if one of the grounds listed in the provision applies.

Applying the right to erasure to blockchains has proven challenging for many, as deleting data from decentralized systems is burdensome due to the purposeful design of these networks, which makes the unilateral modification of data difficult, which generates trust in the network by ensuring data integrity. Technical factors and governance design further burden compliance with Article 17 of the GDPR. Even if there were a technical means of ensuring compliance, it might be organizationally difficult to get all nodes to implement related changes on their own copy of the database, particularly in public and permissionless blockchains.

To thoroughly understand the relationship between distributed ledgers and the GDPR's right to erasure, it is first essential to define what "erasure" means according to Article 17 of the GDPR since neither this article nor the explanatory recitals offer further clarification on this interpretation. Without precise guidance on interpreting

[601] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?,* at 73: "However, even if all nodes, miners and users were considered to in fact qualify as the data controllers liable to implement data subject rights, 'this would not necessarily provide effective protection for data subjects'. This is so as even though all nodes could agree (through a contract or another form of agreement) to 'fork' to a new version of the Blockchain in periodic intervals to reflect requests for erasure, this level of coordination has been said to be 'difficult to achieve among potentially thousands of nodes'".

this concept, it is difficult to assess whether erasing personal data from blockchains is possible. While it may be reasonable to adopt a common-sense understanding, the term's precise scope remains ambiguous. From this perspective, erasure could be considered synonymous with data destruction.

Notwithstanding, erasing data from blockchains, especially public and permissionless ones, is far from straightforward. Article 17 GDPR does not necessarily require data to be entirely destroyed, as indicated by the case of Google Spain, where the delisting of information from search results was regarded as an act of erasure. In this case, the claimant did not have control over the original data source, an online newspaper publication and their request was directed solely at Google.

This suggests that GDPR obliges data controllers to make every effort to achieve a result as close to data destruction as possible within the limits of their factual possibilities. National and supranational regulators have also suggested alternatives to outright data destruction to comply with the erasure obligation. For instance, the destruction of hardware in cloud computing was considered potentially qualifying as erasure, according to the Article 29 Working Party's opinion.

Additionally, some data protection authorities have recognized that erasure does not necessarily mean destruction. Data anonymization was acknowledged as a means of achieving erasure by the Austrian Data Protection Authority. Similarly, the UK Information Commissioner's Office has advocated 'putting data beyond use' as a satisfactory erasure method. However, all Member States have no uniform consensus on this matter.

In the case of *Nowak*, the CJEU seemed to suggest[602] that erasure equates to the destruction of personal data, stating that a candidate in an examination has the right

[602] CJEU, *Nowak*, C-434/16, EU:C:2017:994, paras 55: "Moreover, as stated by the Advocate General in point 37 of her Opinion, it cannot be ruled out that a candidate may, under Article 12(b) of Directive 95/46, have the right to ask the data controller to ensure that his examination answers and the examiner's comments with respect to them are, after a certain period of time, erased, that is to say, destroyed. Pursuant to Article 6(1)(e) of that directive, personal data is to be kept in a form which

to request the data controller to ensure the erasure, or destruction, of their examination answers and the examiner's comments after a certain period of time. Nevertheless, it is unclear if this statement can be universally applied to all erasure cases, given that the specific context of the *Nowak* case did not directly pertain to the right to erasure. The case-by-case approach and the uncertainty about the real implication of the expression 'erasure' may indicate that controllers should do all they can to obtain a result as close as possible to destroying data within the limits of their possibilities.

Similar to data minimization, selecting an appropriate cryptographic method for data storage can enable data subjects to exercise their rights more effectively.
While it is technically impossible to erase data registered on a Blockchain at the request of a data subject, there are ways to make the data practically inaccessible. For example, if the data recorded on the Blockchain is a commitment, a hash generated by a keyed-hash function, or a ciphertext obtained using state-of-the-art algorithms and keys, the data controller can make the data difficult to access by deleting the data off-chain and the corresponding key, used for generating the hash value, which is stored on-chain. Also, the CNIL considered data inaccessibility as an approach close enough to erasure, which, however, would necessitate encrypting the data and deleting the corresponding private key.[603]

permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is subsequently processed. Taking into consideration the purpose of the answers submitted by an examination candidate and of the examiner's comments with respect to those answers, their retention in a form permitting the identification of the candidate is, a priori, no longer necessary as soon as the examination procedure is finally closed and can no longer be challenged, so that those answers and comments have lost any probative value."

[603] F.W.J. van Geelkerken, K. Konings, *Using Blockchain to strengthen the rights granted through the GDPR*, in *7th International youth science forum «Litteris et Artibus»*, Ukraine, 2017, pp. 458–461; J. P. Jussila, *Reconciling the conflict between the 'immutability' of public and permissionless Blockchain technology and the right to erasure under Article 17 of the General Data Protection Regulation*, 2017, https://www.semanticscholar.org/paper/Reconciling-the-conflict-between-the-%E2%80%98immutability%E2%80%99-Jussila/cbf04ff2d19f2c55e308b3d659d90f4069ae6efd.

Complying with an erasure request would be practically impossible if the data were stored in plain text. Moreover, following the analogy of Google Spain, it has been suggested that users might direct their requests to intermediaries like block explorers to remove data from their indexes. Therefore, intermediaries storing encrypted data on the Blockchain at the application layer can allow the erasure request to be met by simply deleting the private key. Furthermore, locating data on a Blockchain is not as straightforward as in regular databases since specific knowledge of what and where to search for is necessary, and general searches using keywords are impossible. This characteristic of Blockchain searching may reduce the adverse impact on the data subject whose data is to be erased, making the complete takedown of the Blockchain an even more disproportionate measure.

When data are stored in plain text or are publicly accessible, complying with an erasure request becomes problematic, requiring either the takedown of the entire Blockchain or its transformation into a permissioned one.

In view of the GDPR, this concept must be seen critically. First, it is possible that today's encryption algorithms are no longer considered secure in the future, so it might be possible to decrypt the data without knowing the original encryption key.[604] Second, as deepened in the previous paragraphs, encryption must be considered a form of pseudoymization; therefore, it only guarantees confidentiality over a specific period, while anonymization should last indefinitely.

In conclusion, at the moment, there is no explicit legal assurance that utilizing cryptographic references tied to personal data on the Blockchain aligns with GDPR requirements for processing personal data. Even if data is referenced, it could still be considered pseudonymized personal data from a legal standpoint, and performing erasure or rectification on such data might pose technical challenges.

[604] L.D. Ibáñez, K. O'Hara, Kieron, E. Simperl (2018); N. Eichler, S. Jongerius, G. McMullen, O. Naegele, L. Steininger, K. Wagner (2018).

Notwithstanding, it is essential to note that the legal perspective on this matter could evolve over time based on the interpretation of the main concepts and the technical solutions[605] involved, potentially altering the current circumstances.

4.3.4. Right to restriction of processing

Article 18 of the GDPR[606] grants individuals the right to request a restriction of processing their personal data in various circumstances, regardless of the specific

[605] Some technical solutions are already under development. For instance, *State tree pruning*, analogous to automatic memory management for volatile resources, is a technique employed to eliminate data from the Ethereum Blockchain. However, a drawback of this method is that it aims to reduce the states in the block by removing unused records, regardless of whether participants demand their removal. The sole approach to deleting code from the Blockchain is when a contract at that address executes the "self-destruct" operation. This operation removes both the storage and code from the state. Nevertheless, even if a contract is deleted through "self-destruct," it remains part of the Blockchain's history and is likely retained by most Ethereum nodes. Consequently, "self-destruct" does not mean deleting data from a hard disk (see https://blog.ethereum.org/2015/06/26/state-tree-pruning).
Moreover, the concept of employing *"chameleon" hash functions* to create an editable Blockchain, also known as a redactable Blockchain, has been explored. In this approach, the hash of the data stored in the Blockchain is used to ensure the integrity of the data. If any changes are made to the data, the hash of that data in the block is altered, which indicates data tampering. Consequently, this change affects the block header hash, disrupting the link between subsequent blocks. These "chameleon" hash functions are also called trapdoor hash functions, as they come with an additional secured private key, known as the trapdoor key. The original data can be updated and added to the Blockchain with this key. Remarkably, the updated data possesses the same hash value as the original data. This feature enables the implementation of GDPR's right to erasure and right to rectification, allowing users to rewrite or delete past blocks of information without compromising the integrity of the Blockchain (see N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, *From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again*, in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 2012, pp. 326–34, available: http://doi.acm.org/10.1145/2090236.2090263).
Finally, a novel mutable Blockchain named *µchain* has been introduced by researchers. The key features of µchain include the ability to maintain alternative versions of data records, employing a consensus mechanism to validate a legitimate history, and its inherent capacity to conceal alternative versions of history. In the context of a given set of transactions, only one transaction is designated as "active," while all the other transactions represent alternative "inactive" versions. The set of transactions can be extended to include new versions of transactions. Consequently, senders can update transactions, specifically the "active" one, if rectification is necessary. To ensure data security, decryption keys are exclusively available for the "active" transactions, while the inactive transactions are hidden through encryption. This setup empowers data subjects by offering them the option to exercise their right to rectification (see I. Puddu, A. Dmitrienko, S. Capkun, *µchain: How to Forget without Hard Forks,* 2020, https://eprint.iacr.org/archive/2017/106/1591084586.pdf).

[606] "1.The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a

technology employed for the processing, including Blockchain technology. When distributed ledgers are utilized, EU data protection law mandates that data subjects have the option to obtain a restriction of processing, such as when they dispute the accuracy of their personal data.

Determining whether any potential controllers within a given Blockchain network can fulfil the requirements of Article 18 GDPR necessitates a case-by-case examination of the technical and governance arrangements in place. Two major challenges to compliance with this obligation can be identified.

Firstly, there are likely technical obstacles to restricting processing in the context of automated systems like blockchains. These systems are often designed to make a direct intervention in data processing cumbersome, aiming to enhance data integrity and trust in the network. Particularly with public and permissionless ledgers, halting data processing within a block poses difficulties. This holds true not only for the distributed ledger at the application layer but also for blockchain-based applications.

Secondly, governance issues arise concerning the ability of various potential joint controllers to carry out such interventions within the network. As per recent case law on joint control, any party exercising some control over the means and purposes of personal data processing qualifies as a joint controller. However, specific data controllers in the Blockchain network, such as nodes or users, may lack the capacity to intervene in a manner that effectively triggers a restriction of processing. This

period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. 2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. 3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted."

recurring theme highlights the crucial significance of establishing both technical and governance arrangements that enable data controllers to comply effectively with Article 18 of GDPR.

A possible solution may be to implement smart contracts to limit the use of data when necessary.[607] The first step for this solution is to establish which nodes have access to personal data. This solution has already been implemented[608] where the restriction was performed by the consent smart contract limiting the personal data that can be collected.

4.3.5. Data controllers' communication duties

Article 19 of the GDPR[609] mandates that the data controller must inform the 'recipients' to whom personal data has been disclosed about any rectification, erasure, or restriction of processing. The definition of 'recipients' becomes a complex issue when considering scenarios involving blockchains, often used to coordinate records among multiple parties, potentially resulting in many 'recipients' for each personal data processing operation on the distributed ledger.

In private and/or permissioned systems, data controllers typically maintain a record of parties authorized to access and read the data. This makes it relatively straightforward to inform these parties about any actions taken under Articles 16-18 of GDPR.

[607] M. Poelman, S. Iqbal (2021).

[608] C. Daudén-Esmel, J. Castellà-Roca, A. Viejo, J. Domingo-Ferrer, *Lightweight Blockchain-based platform for GDPR-compliant personal data management*, in *Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy*, 2021, pp. 68-73.

[609] "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."

On the other hand, public and/or permissionless blockchains allow access to personal data without requiring explicit permission. In such cases, the parties overseeing the networks cannot know who has gained access to the related personal data, either by directly engaging with the network or using tools like block explorers. Consequently, complying with the communication obligations of Article 19 GDPR in these circumstances may be deemed 'impossible' or 'disproportionate' in effort. Thus, this scenario might fall under the exceptions envisioned in Article 19 GDPR, allowing the data controller to be exempted from fulfilling their notification duties ("unless this proves impossible or involves disproportionate effort").

4.3.6. The right to data portability

The right to data portability is a significant advancement in the GDPR compared to the previous Directive. It empowers data subjects by allowing them to transfer their data from one data controller to another under certain conditions.

The goal is to enable individuals to move, copy, or transmit their personal data between different IT environments. [610] When data subjects make a valid request for portability under Article 20 of the GDPR,[611] controllers must provide the data in a structured, commonly used, and machine-readable format that is also interoperable.

[610] Article 29 Working Party, *Guidelines on the Right to Portability*, WP 242 rev.01, 5 April 2017, at p. 4.

[611] "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

To be eligible for data portability, several conditions must be met: the right applies only to personal data, the data must have been provided by the data subject to the controller, processing must be based on consent or contract, and the processing must be automated.

The CNIL finds that Blockchain technologies generally present few compliance issues concerning the portability requirement. However, Article 20 of the GDPR emphasizes the importance of ensuring interoperability among various DLT solutions. For example, in social media networks, data portability may lose its purpose if there are no connections (e.g., "friends") on the new platform.[612] This concern also applies to Blockchain networks, where network effects play a role at the infrastructure and application layers. Therefore, encouraging the interoperability of different solutions is crucial for effective data portability enforcement.

Notably, the link between accountability and control should be taken into consideration.[613] The European Court of Justice's current stance on controllership raises the risk of entities being classified as controllers even if they cannot fulfil the portability requirements mandated by the GDPR. As seen in the previous paragraphs, a node in a Blockchain network may, for instance, be deemed a data controller,[614] even though it can only access hashed or encrypted data, making it practically unusable for data subjects in many cases.

[612] L. Edwards, *Law, Policy and the Internet,* Oxford: Hart Publishing, 2018, at p. 109.

[613] Giordanego asserted that moving data between providers would imply the erasure of data held by the old provider, which is not possible in public Blockchain, see A. Giordanengo, *Possible usages of smart contracts (Blockchain) in healthcare and why No one is using them*, in *MEDINFO 2019: Health and Wellbeing E-Networks for All*, IOS Press, 2019, pp. 596-600.

[614] Furthermore, the lack of precise and identified data controllers was seen as another barrier to this right, see G. M. Riva (2020).

4.3.7. The right to object

Article 21 of the GDPR[615] grants data subjects the right to object to processing their personal data when such processing is based on either public interest or legitimate interests. If a data subject exercises this right, the data controller must halt the processing of the personal data unless they can demonstrate "compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims."

Many of the key points mentioned earlier, which are of general significance, also apply to complying with Article 21 of the GDPR. These points include controllers' limited influence over data processing due to the nature of distributed ledgers and the challenges in stopping data processing when it occurs automatically.

However, one aspect that requires particular attention when dealing with Article 21 GDPR is the interpretation of "compelling legitimate grounds" that would justify the data controller's refusal to comply with a data subject's request to restrict data processing. Specifically, there might be a question of whether the data controller's interest in maintaining the integrity of DLT records qualifies as such a legitimate

[615] "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. 3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. 4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. 5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications. 6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest."

ground. This point could benefit from further clarification through regulatory guidance to establish legal certainty.

4.3.8. Article 22 GDPR and solely automated data processing

As per Article 22(1) of the GDPR, data subjects have the right 'not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or significantly affects them in a similar manner.' This right is particularly relevant in Blockchain technology, such as smart contracts that can be seen as making 'decisions' under certain circumstances.

The Article 29 Working Party defines solely automated decision-making as the capacity to arrive at decisions using technological means without human involvement.[616] Consequently, a decision is considered 'based solely' on automated processing when there is no human participation in the decision-making process. Furthermore, it's important to note that Article 22 GDPR specifically targets 'decisions' made through solely automated data processing. On the other hand, Recital 71 of the GDPR mentions a "decision, which may include a measure."

This raises the possibility that Blockchain-based smart contracts could be considered decisions, especially when their outcomes align with those resulting from human decision-making processes in the analogue world.[617] In such cases, if the smart contract's effects have legal implications or significantly impact individuals, Article 22 GDPR would apply. Examples could be seen in scenarios where a smart contract determines insurance premium payments, enforces consumer rights, or releases payment for goods or services.

[616] A29 WP, *Guidelines on Automated Individual Decision-Making and Profiling*, 2018, at p. 8.

[617] See M. Finck, *Smart contracts as a form of solely automated processing under the GDPR,* in *International Data Privacy Law*, 2019, pp. 78-94.

The use of purely automated decision-making resulting from a smart contract, with legal or significant effects, is restricted to specific scenarios outlined in Article 22(2) of the GDPR. According to this provision, solely automated data processing is permissible only in three cases: (i) when it is necessary for a contract between the data subject and the controller, (ii) when it is authorized by EU or Member State law, or (iii) when it is based on the explicit consent of the data subject. At first glance, these requirements might appear applicable in the context of smart contracts, just like in other situations. However, in-depth research reveals specific challenges.

In cases where automated processing is justified under Article 22(2)(a) or (c), specific protective measures must be observed. In the case of smart contracts related to a legal contract, it may not always be a contract between the data subject and the controller, which could create issues regarding the applicability of Article 22(2)(a) of the GDPR. Moreover, consent might have limited value in this context because EU data protection law stipulates that data subjects must be able to withdraw their consent. This can be difficult to achieve when the data processing cannot be stopped upon the data subject's request, as is often the case with smart contracts due to their automation. These measures include the right to human intervention (as stated in Article 22(3) of the GDPR) and the right to be informed (as covered in Articles 13 and 14 of the GDPR). Additionally, the Article 29 Working Party has emphasized that in situations where automated processing poses a high risk, conducting a Data Protection Impact Assessment (DPIA) may be advisable.

Based on the analysis above, it is evident that smart contracts cannot automatically qualify as lawful under Article 22 of the GDPR, but they can be utilized if they fulfil one of the scenarios described in Article 22(2) and adhere to the protective requirements stated in Article 22(3). Achieving compliance might necessitate some distance from the original motives of automated processing and addressing the challenge of limited human intervention in these tools. Nonetheless, these efforts can align with the ongoing development of more sophisticated smart contracts, ensuring their compatibility with legal principles. This approach allows us to harness the advantages of automated execution while maintaining compliance with real-world requirements and the GDPR.

In a broader sense, the research findings underscore the GDPR's potential to encourage meaningful innovation. By ensuring that the benefits of automated data processing, such as improved efficiency and resource savings, are balanced with the safeguarding of fundamental rights, the GDPR fosters a framework that stimulates responsible and innovative data practices.

4.4. Is a Data Protection Impact Assessment (DPIA) necessary?

In situations where data processing poses a potentially high risk to fundamental rights, the controller is required to take proactive measures and conduct a Data Protection Impact Assessment (DPIA) to evaluate the impact of the processing on personal data protection.

DPIAs are evaluations carried out by data controllers to assess the effects of planned processing operations on data subjects, particularly when the nature, scope, context, and purposes of processing present high risks to individuals' rights and freedoms. This is particularly applicable when new technologies are employed.

Under Article 35 of the GDPR, DPIAs are required, especially in the following cases: (i) when there is a systematic and extensive evaluation of personal aspects of individuals based on automated processing, including profiling, leading to decisions that have legal or similar significant effects; (ii) when sensitive data or data related to criminal convictions and offences are involved; or (iii) when systematic monitoring of a publicly accessible area on a large scale is undertaken. If a DPIA reveals that the processing poses a high risk to data subjects and insufficient measures can be implemented to mitigate the risks, the controller must inform the supervisory authority.

As stated in Article 35(7) of the GDPR, the DPIA must include a systematic description of the purposes and processing activities, an assessment of the necessity and proportionality of the processing concerning its purpose, an evaluation of the risks and the rights and freedoms of data subjects, as well as proposed measures to address these risks.

It's crucial to emphasize that the requirement for a DPIA is not primarily based on a specific technology but on the risk associated with the processing itself. For instance, DPIAs are necessary when processing a large scale of special categories of data or data related to criminal convictions or offenses or when systematically monitoring a publicly accessible area on a large scale, regardless of the technology used.

However, merely using new technology may be perceived as inherently entailing a high risk. For instance, the ICO[618] asserts that a DPIA must be conducted whenever a new technology is employed.

Defining what exactly qualifies as a new technology remains a challenging task as innovations invariably build upon previous ones.

Even though Blockchain can be considered "new," it draws upon several innovations dating back many decades, as mentioned in the first chapter. Moreover, it raises questions about how long a technology can be considered "new." Notably, the first Blockchain, Bitcoin, is over ten years old.

Consequently, in this context, it would be beneficial for regulatory guidance concerning blockchains and the GDPR to clarify whether the mere use of blockchains inherently presents a high risk to fundamental rights or if risk assessments should be conducted on a case-by-case basis, as the following sections intend to address.

[618] UK DPIA, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/.

5. Addressing the Human Rights Impacts of Blockchain Technologies

As previously mentioned, the advancements in Blockchain technology may pose potential risks to universal human rights. This section explores measures Blockchain developers and implementers can undertake to mitigate these risks.

Companies' response to human rights impacts will vary depending on their level of involvement. If a company is responsible for causing an effect, it is expected to take steps to cease or prevent it. In cases where a company contributes to an impact, it should cease or prevent its contribution and leverage its influence to mitigate the effects as much as possible. Businesses should also proactively work towards preventing or mitigating adverse human rights impacts that are directly linked to their operations, products, or services, even if they are not directly responsible for those impacts. They should utilize their leverage with business partners to achieve this. If a company lacks the necessary leverage to prevent or mitigate adverse impacts and cannot increase it, it should consider terminating the relationship. Additionally, businesses are responsible for providing effective remedies for human rights harms associated with their products and services.

The corporate responsibility to respect human rights exists regardless of whether governments enforce laws that align with human rights principles. In certain instances, companies may be required to uphold higher standards than national legislation mandates. The relationship between the corporate responsibility to respect human rights and governments' existing human rights obligations is intricately interconnected and mutually influential.

We argue that many of the Blockchain's use cases described aim to utilize it to promote and enhance respect for human rights within their respective sectors. Entities, such as companies, governments, or NGOs that deploy these technologies should also undertake due diligence on human rights. This includes evaluating whether

Blockchain implementation can genuinely deliver the anticipated positive human rights outcomes it purports to achieve.

A detailed examination of these aspects would go beyond the scope of this thesis; however, it is worth at least defining and clarifying which elements should, in our opinion, help create a framework to mitigate the risks that Blockchain poses for human rights.[619]

First of all, it is of pivotal importance to identify the human rights impacts and risks of Blockchain. In that sense, the risk assessment methodology already adopted for data protection-related matters could be very useful. Therefore, as summarized in the previous section, assessing the human rights impacts of the company's products and services would be necessary. From the result of this risk assessment, which has to be considered as an ongoing process baked into the operations made by developers, an internal structure for identifying and reviewing processes should be implemented.

To ensure efficiency in that process, developers may be assisted by external and independent advisors from a wide range of disciplines.[620] Moreover, in order to make this process transparent, developers and organizations should, whenever possible, implement their solutions using open-source software and publicly communicate the remedy plan[621] they have implemented.

[619] For a detailed overview, see W. Crumpler et al, *The Human Rights risks and opportunities in Blockchain,* A Joint Report of the CSIS Strategic Technologies Program and Human Rights Initiative, 2021; A. Bag, S.M. Aamir Ali, A. Ghose, P. Mishra, B. P. Singh, S.Datta, *The Role of Blockchain Technology on Human Rights Management and Business Ethics—Utopia or Dystopia*, in: S. Yadav, A., Haleem, P.K. Arora, H. Kumar (eds), *Proceedings of Second International Conference in Mechanical and Energy Technology. Smart Innovation, Systems and Technologies*, Springer, 2023, pp. 359-365; A. M. Lopez Rodriguez, *Blockchain and its Impact on Human Rights,* in *Legal Challenges in the New Digital Age*, 2021, pp. 231–252.

[620] Developers and those implementing solutions should contemplate the establishment of external advisory panels aimed at offering autonomous oversight and guidance concerning the adoption and implementation of Blockchain technology in practical scenarios. This encompasses considerations about its potential impacts on human rights. Enterprises should formulate a systematic procedure for referring matters to these panels for consultation. All discussions and considerations should be made transparently accessible to the public, conceivably with a time delay to address any potential commercial sensitivities.

[621] In the context of Blockchain solutions, the question of providing remedies becomes especially significant due to the unique properties and limitations of the technology. The immutability of

Given what is at stake, it is important to consider that mitigating privacy risks has to be the beacon that guides any implementation of new technologies because, no matter how much humanity may adapt to technological innovation, the protection of human rights must remain the hard core of any project in any field of knowledge.

6. Could 'redactable Blockchain' solve the challenges in ensuring data subjects' rights?

Redactable Blockchain, a relatively new concept introduced by Ateniese et al. [622] in 2017, challenges the traditional notion of Blockchain's immutability. In this context, "redactable" means the ability to rewrite previously written blocks on the Blockchain, compress existing blocks into a smaller number, and insert new blocks into the chain. Initially, immutability seems to contradict one of the fundamental Blockchain principles. However, Ateniese et al. argue that immutability might not be suitable for all Blockchain technology applications. Specific use cases, such as file storage or the management of personal health records, require the flexibility to delete data in cases of errors or to comply with legal requirements, possibly under regulations like the GDPR. Considering that in these scenarios, the ability to modify or remove data becomes crucial, the concept of redactable Blockchain comes into play.

The immutability of a Blockchain derives from the collision resistance of the hash values linking each block to its predecessor. To introduce mutability into a Blockchain, the concept employs a specialized form of a "chameleon hash function," which

Blockchain records presents challenges for certain forms of remedy, such as the deletion of false or privacy-threatening data, which may be rendered impossible. It is crucial for developers and implementers to take into account how Blockchain technology can shape the possibilities for offering remedies and to take necessary precautions to prevent situations where such failures may occur. When it comes to personal information, as previously analyzed, this consideration is paramount, and it should never be directly logged onto a Blockchain, even when encrypted.

[622] G. Ateniese, B. Magri, D. Venturi, E. Andrade, *Redactable Blockchain – or – Rewriting history in Bitcoin and friends*, in *2017 IEEE European Symposium on Security and Privacy*, 2017, pp. 111–126.

operates similarly to a regular hash function but possesses a unique characteristic - a trapdoor. This trapdoor can be utilized to generate collisions deliberately. By leveraging these collisions, it becomes possible to modify transactional data without altering the corresponding hash value of the block.

As a result, the connection to its successor is maintained seamlessly. Ateniese et al. illustrate this process as adding a lock to the linkage between two blocks, which can be unlocked with the appropriate key, thereby allowing for selective mutability within the Blockchain. This facilitates modifications to the foundational data for which the hash has already been incorporated within the decentralized framework, enabling the rectification of (human) mistakes or deliberate (fraudulent) inaccuracies within the Blockchain. As a result, it becomes feasible to uphold individuals' rights under GDPR, such as the right to rectification and the right to erasure.

It is worth noting that the immutability of a Blockchain is reinstated when the key to the hash function's lock is lost or destroyed, as this prevents any further modifications to the blocks. Hence, managing the trapdoor key is crucial in Redactable Blockchain. In a Private Blockchain network, the key could be entrusted to the central authority, while in a Consortium Blockchain, it could be shared among all the network participants.

Among the analyzed literature, only a few authors, such as Finck,[623] Ibáñez et al.,[624] Pagallo et al.,[625] and Moerel [626] have recognized the potential use of the Redactable Blockchain concept in resolving the conflict between Blockchain and GDPR. Nevertheless, some real-world applications[627] of a Redactable Blockchain was identified in the reviewed literature.

[623] M. Finck (note 87).

[624] L. D. Ibáñez, K. O'Hara, E. Simperl (2018).

[625] U. Pagallo, E. Bassi, M. Crepaldi, M. Durante (2018).

[626] L. Moerel, *Blockchain & Data Protection ... and Why They Are Not on a Collision Course*, in *European Review of Private Law*, 2019, pp. 825–852.

[627] For instance, cfr. B. Luo, C. Yang, *AeRChain: An Anonymous and Efficient Redactable Blockchain Scheme Based on Proof-of-Work*, in *Entropy,* 2023, pp. 270 e ss; J. Ma, S. Xu, J. Ning, X. Huang, R. H. Deng,

The Redactable Blockchain presents an intriguing solution to the mentioned conflict, although the concept also faces certain obstacles.

Firstly, integrating redactability into an existing Blockchain is not feasible, meaning the decision to adopt this concept must be made before setting up the network. Secondly, even with redaction, old copies of the Blockchain will still contain the redacted data, although compliant Blockchain nodes will accept the redacted data and delete the old copies. Lastly, there is a risk of a party redacting the Blockchain to benefit their own interests.

In the context of the GDPR, the concept of Redactable Blockchain appears to offer a solution to the challenges posed by storing personal data on the Blockchain while adhering to data privacy regulations. Deleting or modifying data after it has been stored on the Blockchain is a significant advantage. All participants in the Blockchain network should comply with the GDPR, ensuring that redactions are promptly performed and old copies are securely deleted. External audits could be employed to verify this process.

However, it may be argued that granting a single entity the ability to redact data on the Blockchain goes against the fundamental principles of the technology and that even the general possibility of altering data stored on the Blockchain contradicts the core concept of immutability that underpins Blockchain technology. Does this imply that, as suggested for the concept of deletion, the idea of immutability should also be re-evaluated to fit data privacy requirements?

Largely, the trust in a Blockchain application hinges on the consensus among the network regarding the content of a block and the subsequent immutability of said

Redactable Blockchain in Decentralized Setting, in *IEEE Transactions on Information Forensics and Security*, 2022, pp. 1227–1242; G. Tian, J. Wei, M. Kutylowski, W. Susilo, X. Huang, X. Chen, *VRBC: A Verifiable Redactable Blockchain with Efficient Query and Integrity Auditing*, in *IEEE Transactions on Computers*, 2023, pp. 1928–1942; J. Xu, K. Xue, H. Tian, J. Hong, D.S.L. Wei, P. Hong, *An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks*, in *IEEE Transactions on Vehicular Technology*, 2020, pp. 6688–6698.

content. When considering the removal of this immutability, alternative measures must be adopted to uphold or cultivate an adequate level of trust in the Blockchain application, enabling both individuals and organizations to adopt it as a reliable repository for their transactions. Sustaining trust in a Blockchain application might involve strategies such as conferring the authority to make alterations solely to a singular trusted entity, akin to the exclusive governmental authority over specific modifications in governmental public registries. Alternatively, a rigorous alteration management process could be introduced, potentially encompassing a consensus mechanism that verifies the legitimacy of any proposed modification. Changes must be meticulously noted in any scenario to ensure they remain subject to future examination and elucidation.

7. Applying questions of jurisdiction in a borderless ideology

As already mentioned,[628] determining the appropriate jurisdiction in the digital ecosystem is vital for entities to uphold their Digital Sovereignty[629] and exercise associated rights.

Chapter V of the GDPR establishes limitations on transferring personal data from the European Union to third countries. It stipulates that such transfers are allowed

[628] Cfr. Chapter II, para 5.

[629] Digital Sovereignty is founded upon a set of core values, principles, and regulatory frameworks that support its key characteristics. These frameworks exist within one or multiple jurisdictions.

For a country to establish and enforce regulations, it is essential that both natural and legal persons, whether acting independently or through intermediaries, and utilizing any object or system (including data, software, and hardware) under their control, are unambiguously subject to a specific jurisdiction. This jurisdiction is referred to as the "competent" jurisdiction. Regulations within a jurisdiction, whether at the national, regional, or international level, establish rights and obligations, formulate rules, facilitate transactions, and enable ownership in the digital realm. These regulations also impose specific requirements on individuals responsible for and accountable for certain objects or systems within the jurisdiction to be identified and safeguarded in cyberspace. To determine the applicable legal framework, such as establishing ownership of health data or virtual objects in the metaverse, connected or purely digital entities must be subject to the competent jurisdiction. In light of these considerations, all social, economic, and political interactions that occur in the digital world are inherently governed by a specific jurisdiction. Therefore, the Digital Sovereignty of any entity is fundamentally supported by the competent jurisdiction under which it falls.

only under specific circumstances: (i) if the third country benefits from adequacy decisions, (ii) if appropriate safeguards are in place, or (iii) based on derogations.

This is particularly relevant in Blockchain technology, as the multiple nodes that store the ledger can be located in various jurisdictions, both within and outside the European Union. In a permissioned network, the location of nodes can be controlled, but in a permissionless system, anyone can access the network without prior authorization from a central gatekeeper.

According to Article 45 of the GDPR, transfers of personal data to third countries are permitted based on an adequacy decision. When the European Commission determines that a third country, territory, or specific sector in a third country (or an international organization) ensures adequate data protection, data transfers to that destination do not require additional authorization. The European Commission assesses various factors, such as the respect for the rule of law, human rights, fundamental freedoms, relevant legislation and practices, an independent supervisory authority, and the third country's international commitments regarding data protection. If the Commission finds that the jurisdiction provides an adequate level of protection, it issues an implementing act in the form of an adequacy decision, which is periodically reviewed at least every four years.

Adequacy, in this context, means a level of protection equivalent to that ensured within the European Union. This implies that foreign rules must comply with a core set of GDPR principles, the Charter of Fundamental Rights, and relevant international instruments, including the Council of Europe's Convention 108. When an adequacy decision is in place with a third country, personal data can flow freely between these jurisdictions, irrespective of whether Blockchain or other personal data processing technologies are used.

When personal data needs to be transferred to a jurisdiction that lacks an adequacy decision, the controller or processor must ensure that appropriate safeguards are in place. According to Article 46 of the GDPR, transfers to third countries are permissible if the controller or processor has implemented suitable measures and provided that data subjects have enforceable rights and effective legal remedies available to them. These safeguards do not require specific authorization from a supervisory authority and can include various options, such as:

(i) Legally binding and enforceable agreements between public authorities or bodies.

(ii) Binding corporate rules in accordance with Article 47 of the GDPR.

(iii) Standard data protection clauses adopted by a supervisory authority and approved by the European Commission.

(iv) Binding codes of conduct and enforceable commitments from the controller or processor in the third country to adhere to these safeguards.

(v) Approved mechanisms and enforceable commitments from the controller or processor in the third country to comply with these measures.

Binding corporate rules refer to personal data protection policies followed by a controller or processor established in a Member State for transferring personal data to a controller or processor in one or more third countries within a group of undertakings or enterprises engaged in a joint economic activity.[630]

These rules can be in the form of contractual clauses or administrative arrangements, subject to prior approval from the competent supervisory authority. These clauses can be integrated into broader contractual frameworks.

In compliance with the *Schrems* judgment, data subjects have the right to lodge complaints with DPAs if they question the compatibility of a data transfer outside the EU with the EU's data protection regulations. The relevant DPA must diligently investigate such claims.

[630] Art. 47 GDPR.

When personal data is transferred to a third country using any approved mechanisms mentioned earlier, the data subject must be informed of this transfer. Article 13(1)(f) of the GDPR requires the data controller to inform the data subject at the time of data collection whether their data will be transferred to a third country. Article 15(2) of the GDPR also mandates that when data is transferred to third countries, the data subject must be informed of the appropriate safeguards applied to the transfer.

In the context of Blockchain, where the chain is independent of territoriality and nationality of nodes, data subjects must be aware of international transactions.

Smart contracts can help ensure accuracy in the chain and facilitate data transfer among existing nodes. Alternatively, external databases can be used to keep data within the EU.

Private and consortium blockchains may also be suitable for international data transfers since the controller's location is known.

As cross-border data processing is always involved, nodes must proceed cautiously in public blockchains, especially where no central authority runs the chain.

In view of the ever-increasing importance of the topic of data transfer abroad, especially in light of recent rulings by the Court of Justice[631] and guidance of the

[631] Judgment of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, the Court held that "there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country." (paragraph 71); Judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650: "The Court declared Article 3 of Decision 2000/520/EC to be invalid in so far as it denied national supervisory authorities the powers which derive from Article 28 of Directive 95/46/EC, where a person puts forward matters that may call in question whether a Commission decision that has found that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (paragraphs 102-104)."; Judgment of 16 July 2020, Schrems II, C-311/18, EU:C:2020:559, with this ruling the CJEU has invalidated the European Commission's Privacy Shield Decision due to concerns over intrusive US surveillance programs. Additionally, the CJEU has imposed stricter requirements for the transfer of personal data based on standard contract clauses (SCCs). Data controllers or processors planning to transfer data using SCCs must ensure that the level of protection provided to the data subject is essentially equivalent to the safeguards guaranteed by the GDPR and the EU Charter of Fundamental Rights. If necessary, additional measures should be implemented to address any shortcomings in the protection offered by third-country legal systems. In cases where

EDPB,[632] it will be necessary to understand whether there is a need to rethink the concept of 'transfer' within public blockchains and whether this can really be applied within the context of the Blockchain or, as with the notion of 'erasure', the meaning can be adjusted on a case-by-case basis.

8. Blockchain: A Privacy-Enhancing Technology (PET)?

Researchers have directed their attention towards privacy preservation techniques to address the significant challenges of applying data protection regulations to Blockchain technology. These techniques aim to enhance privacy and anonymity within Blockchain systems.[633]

Building upon the previous discussion, which concluded that there is no absolute incompatibility between Blockchain and the GDPR and that privacy preservation can be achieved through mitigation measures, it is now essential to evaluate whether Blockchain can essentially be considered a Privacy-Enhancing Technology (PET).

First of all, what are PETs?

Upon examining the definition of Privacy-Enhancing Technologies (PETs), it becomes apparent that they carry significant implications. PETs are not novel technological trends; they have been a subject of academic research for nearly three decades. However, their practical applications are now being realized in various real-world scenarios.

equivalent protection cannot be ensured, operators must suspend the transfer of personal data outside the European Union (EU).

[632] EDPB, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, adopted on 14 February 2023; EDPB, *Guidelines 07/2022 on certification as a tool for transfers*, adopted on 14 February 2023.

[633] For an interesting example see I. T. Javed, F. Alharbi, T. Margaria, N. Crespi, K. N. Qureshi, *PETchain: A Blockchain-Based Privacy Enhancing Technology*, in *IEEE Access*, 2021, pp. 41129-41143.

To gain a deeper understanding of PETs, it is crucial to grasp their technical definition. PETs encompass a range of technologies that focus on ensuring data security. These technologies play a pivotal role in protecting and enhancing data privacy and security, particularly during activities such as searches or analytics. Although different types of PETs are tailored to specific use cases, they often share certain commonalities. By leveraging PETs, organizations and individuals can implement measures to uphold privacy and security standards in their data operations. These technologies enable the safe handling and processing of data, allowing individuals to have greater control over their personal information and organizations to mitigate the risks associated with data breaches and unauthorized access.

As PETs continue to evolve, their adoption is expected to become more widespread, leading to improve privacy and security practices across various domains and industries. When considering specific examples of privacy-enhancing technologies, nuances may arise depending on the use cases and applications involved since a particular technology's privacy protection and enhancement level is influenced by its inherent security capabilities.

Three key processes in PETs ensure significant benefits in privacy enhancement.[634] Firstly, PETs rely on establishing a trusted environment where sensitive data can be analyzed and processed securely. This ensures that the privacy of the data is maintained throughout the computation.

The second necessary phase involves executing processing and analytics tasks in a decentralized manner. By distributing the workload across multiple nodes or entities, PETs reduce the risk of data exposure and enhance privacy by minimizing the reliance on a single centralized entity.

[634] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, B. Joosen, *A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements*, in *Requir Eng,* 2010, pp. 3–32.

The third crucial task is encrypting data and algorithms before conducting analytics or processing tasks. By encrypting the data and algorithms, PETs provide additional privacy protection, ensuring that only authorized parties with the necessary decryption keys can access and interpret the information.[635]

These three processes collectively contribute to the privacy-enhancing capabilities of PETs, enabling the secure and confidential use of sensitive data while preserving individual privacy rights.

In this regard, various privacy-enhancing technologies have been proposed and discussed in the literature. Among the most widely adopted privacy techniques[636] are

[635] Among the commonly used privacy-enhancing techniques, K-anonymization, L-diversity, and T-closeness are prevalent. Each technique addresses different aspects of privacy preservation while considering trade-offs with data utility. K-anonymity is achieved through the application of suppression and generalization methods. These methods modify the dataset until each row becomes indistinguishable from at least k-1 other rows. By doing so, individual identities are protected, and privacy is enhanced. However, this process often leads to a reduction in the originality of the data.

L-diversity builds upon the concept of k-anonymity and aims to address homogeneity and background knowledge attacks. It ensures that sensitive attributes in a group of k-anonymous records exhibit a certain level of diversity, making it harder for attackers to infer specific information about individuals. While L-diversity provides an additional layer of privacy, it can further impact data utility and precision. T-closeness focuses on reducing attribute disclosure by decreasing the granularity of data. It aims to ensure that the distribution of sensitive attributes in a group of records is not significantly different from the overall distribution in the entire dataset. This technique helps protect sensitive information but also introduces a trade-off between privacy and data utility.

It is important to note that while these techniques enhance user privacy, they often come at the cost of reduced data accuracy, precision, and utility. Striking the right balance between privacy and data utility is crucial when implementing these anonymization techniques. Higher levels of anonymization may provide stronger privacy guarantees but can render the data less productive and less effective for certain applications. See L. Sweeney, *K-anonymity: A model for protecting privacy*, in *International Journal of Uncertainty Fuzziness Knowledge-Based System.*, 2002, pp. 557-570; A. Machanavajjhala, J. Gehrke, D. Kifer, M. Venkitasubramaniam, *L-diversity: Privacy beyond k-anonymity*, in *Proceeding 22nd International Conference of Data Engeneering (ICDE)*, 2006; N. Li, T. Li, S. Venkatasubramanian, *T-closeness: Privacy beyond k-anonymity and l-diversity*, in *Proceedings IEEE 23rd International Conference of Data Engeneering*, 2007, pp. 106-115; A.-E.-E.-A. Hussien, N. Hamza, H. A. Hefny, *Attacks on anonymization-based privacy-preserving: A survey for data mining and data publishing*, in *Journal of Information Secuity*, 2013, pp. 101-112.

[636] S.-C. Cha, T.-Y. Hsu, Y. Xiang, K.-H. Yeh, *Privacy enhancing technologies in the Internet of Things: Perspectives and challenges*, in *IEEE Internet Things Journal.*, 2019, pp. 2159-2187.

homomorphic encryption,[637] Zero-knowledge proofs ("ZKP"),[638] Secure Multi-Party Computation,[639] Ring signatures[640] and Differential Privacy techniques.[641]

Homomorphic encryption ("HE") is one of the most promising forms of encryption and plays a crucial role in various privacy-enhancing techniques as it can be combined with other cryptographic methods to achieve privacy objectives while allowing for computations to be performed on encrypted data without the need for decryption. Notwithstanding, its adoption has been limited due to the significant computational overhead it introduces, making it incompatible with many current client-server applications. A notable example is Google Search, which employs homomorphic encryption for privacy preservation.

The concept of homomorphic encryption was initially introduced by Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos in 1978 as a particular encryption function known as "privacy homomorphism".[642] Homomorphic encryption is particularly suitable for encrypting data in privacy preservation scenarios in cloud storage and computation.

In traditional encryption procedures, there are three main steps: key generation, encryption, and decryption. However, homomorphic encryption introduces an additional step: analysis or evaluation.

[637] H. Zhou, G. Wornell, *Efficient homomorphic encryption on integer vectors and its applications*, in *Proceedings Information Theory and Applications Workshop*, 2014, pp. 1-9.

[638] L. Sweeney, *K-anonymity: A model for protecting privacy*, in *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2002, pp. 557-570.

[639] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C. Z. Gao, H. Li, Y. Tan, *Secure Multi-Party Computation: Theory, practice and applications*, in *Information Sciences*, 2019, pp. 357–372; J. Zhou, Y. Feng, Z. Wang, D. Guo, *Using secure multi-party computation to protect privacy on a permissioned Blockchain*, in *Sensors*, 2021, pp. 1–17; S. Zapechnikov, Secure multi-party computations for privacy-preserving machine learning, in *Procedia Computer Science*, 2022, pp. 523–527.

[640] X. Li, Y. Mei, J. Gong, F. Xiang, Z. Sun, *A Blockchain privacy protection scheme based on ring signature*, in *IEEE Access*, 2020, pp. 76765–76772; X. Zhang, C. Ye, *A novel privacy protection of permissioned Blockchains with conditionally anonymous ring signature,* in *Cluster Computing*, 2022, pp. 1221–1235.

[641] M. Ul Hassan, M.H. Rehmani, J. Chen, *Differential privacy in Blockchain technology: A futuristic approach*, in *Journal of Parallel and Distributed Computing*, 2020, pp. 50–74.

[642] R. Rivest, L. Adleman, M. Dertouzos, *On data banks and privacy homomorphisms*, in *Foundations of secure computation,* 1978.

Using homomorphic encryption, sensitive data can be securely analyzed and processed without decryption, reducing the risk of data exposure and maintaining privacy. It offers a powerful tool for privacy preservation, especially in scenarios where data needs to be transmitted or analyzed without compromising confidentiality.

This technique enables computations to be performed directly on encrypted data, producing the same result as if the computations were performed on the plaintext data. This prevents unauthorized interception of information, preserves confidentiality, and allows a third party to perform operations on the ciphertext without revealing the original data values. Like other encryption schemes, HE utilizes an encryption key to encrypt plaintext and only permits access to the data with the corresponding decryption key, which can be symmetric or asymmetric. The key distinction lies in HE's ability to evaluate computations on the encrypted data without requiring access to the decryption key, while keeping the result encrypted.[643]

[643] HE enables the execution of a specific algebraic operation, denoted as fplain(), directly on the plaintext. This operation is equivalent to another algebraic operation, denoted as fcipher(), performed on the ciphertext. For instance, considering a ciphertext c0 = Enc(Ke, m0), where m0 represents the plaintext, HE allows obtaining the same result by applying any computational function f() directly on the ciphertext: fcipher(c0) = Enc(Ke, fplain(m0)). See. A. Acar, H., Aksu, A. S. Uluagac, M. Conti, *A survey on homomorphic encryption schemes: Theory and implementation*, in *International Journal of Computer Applications*, 2018, pp. 79.
Some previous studies have focused on combining Blockchain and HE technologies to guarantee high-security levels in aggregation processes. Ghadamyari and Samet (Cfr. M. Ghadamyari, S. Samet, *Privacy-preserving statistical analysis of health data using paillier homomorphic encryption and permissioned Blockchain*, in IEEE *International conference on Big Data*, 2019) present a privacy-preserving method for statistical analysis of health data leveraging Blockchain technology and Paillier encryption algorithm to increase the accuracy of data analysis while preserving the privacy of patients. It was a high step compared to previous works as it enjoys the benefits of a distributed solution in terms of higher availability while enhancing data security. The proposed scheme guarantees privacy between the different participants (patients) as they only share encrypted data. However, it does not provide patients privacy with the statistics recipient (for example, a researcher), as patients' data is always encrypted with the recipient's public key, limiting the statistics to him. Although this study really increases privacy, it still shows some privacy holes that can be improved with algorithms like the one presented in this work. Similar approaches have been presented in Yu et al. and Park, Chao, Jeong & Park for voting purposes (cfr. B. Yu, J. Liu, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, M.H. Au, *Platform-independent secure Blockchain-based voting system*, in *International conference on information security*, 2018; D.-S Park, H.-C. Chao, Y.-S Jeong, J.J. Park, *Decentralized E-voting systems based on the*

Zero-knowledge Proof[644] is a cryptographic protocol that allows one party, known as the prover, to demonstrate the validity or truth of a statement to another party, known as the verifier, without revealing any sensitive or personal data related to that statement. In a Zero Knowledge Proof, the prover aims to convince the verifier that they possess certain knowledge or information without explicitly revealing what that knowledge is. The prover achieves this by interacting with the verifier through a series of messages or computations based on a specific protocol.

These protocols enhance privacy in Blockchain transactions by validating them without disclosing internal details, such as the transaction's sender, recipient, and content (including personal data). The entire Blockchain network can reach a consensus on the transaction's validity without accessing the transaction's content: the

Blockchain technology, in *Advances in computer science and ubiquitous computing: CSA & CUTE 17*, Springer, 2018, pp. 305-309).

Finally, Wang et al. present a framework combining HE and a hierarchical Blockchain network for data aggregation in smart grids. Although it increases the data aggregation decentralization, the proposal highly depends on special nodes called "gateways" which centralize the link between the different Blockchain levels. If those nodes were attacked, the complete system would go down. On the contrary, the protocol proposed in this research, which also combines HE with Blockchain, solves this limitation by presenting a totally decentralized solution while maintaining the required privacy (see, Y. Wang, F. Luo, Z. Dong, Z. Tong, Y. Qiao, *Distributed meter data aggregation framework based on Blockchain and homomorphic encryption*, in *IET Cyber- Physical Systems: Theory & Applications,* 2019, pp. 30–37.

[644] In Blockchain, zero-knowledge protocols utilize zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) to eliminate the need for multiple interactions between the verifier and prover during transaction validation. zk-SNARKs only require a shared string of characters known by both parties to authenticate a statement. By using the prover's digital signature as this shared string, a transaction can be easily proven with minimal computational effort. The personal data within transactions remains decentralized, and no personal data is stored directly on the Blockchain. The absence of actual data on the Blockchain prevents participants from processing the data, ensuring data privacy and complying with GDPR's right to restriction of processing. See, S. Goldwasser, S. Micali, C. Rackoff, *The knowledge complexity of interactive proof systems*, in *SIAM Journal on computing*, 1989, pp. 186–208; N. Bitansky, R. Canetti, A. Chiesa, E. Tromer, *From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again*, in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 2012, pp. 326–349; D. Rahul et al., *Blockchain vs GDPR in Collaborative Data Governance,* in *Cooperative Design, Visualization, and Engineering*, 2020; V. Buterin, J. Illum, M. Nadler, F. Schar, A. Soleimani, *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium,* 2023, available at https://ssrn.com/abstract=4563364; M. Quiniou, *Blockchain: the Advent of Disintermediation,* in *ISTE Ltd*, 2019.

prover sends data, such as a secret embedded in a function, to the verifier. The verifier then performs various operations on the received data to verify its accuracy or truthfulness. Notwithstanding, the verifier does not gain any knowledge about the specific secret embedded in the function or any other sensitive information.

By utilizing Zero Knowledge Proofs, parties can establish trust and verify claims without disclosing private data, lowering the risk of liability for GDPR violations. Thus, this technique should be considered from the very beginning of the development cycle, i.e., it is recommended as a privacy-by-design solution.[645]

Zero Knowledge Proofs have applications in various domains, including Blockchain, authentication protocols, and secure communication systems. Despite being a prominent solution used in many applications, its main drawback was reported as the high computational workload.[646]

In Secure Multi-Party Computation ("SMPC") two or more parties, each owning private data, collaborate to perform a joint computation without revealing their individual inputs to each other. Essentially, the parties agree on a specific joint function that they want to compute. However, instead of sharing their private data directly, they use a cryptographic protocol that allows them to collectively compute the desired function while keeping their inputs private. The result of the computation, which is the output of the joint function, is revealed to the parties.

The underlying cryptographic techniques used in SMPC ensure that the private inputs of each party remain confidential throughout the computation. The parties share intermediate computations and messages while keeping their individual inputs

[645] L. Moerel (2018); R. Mannan, R. Sethuram, L. Younge, *Practitioner's corner • GDPR and Blockchain: a compliance approach*, in *European Data Protection Law Review*, 2019, pp. 421-426; A. Giannopoulou, *Putting data protection by design on the Blockchain*, in *European Data Protection Law Review*, 2021, pp. 388-399.

[646] S. Schwerin, *Blockchain and privacy protection in the case of the European general data protection regulation (GDPR): a Delphi study*, in *The Journal of the British Blockchain Association*, 2018.

encrypted or masked. This enables them to collectively compute the desired function without exposing any sensitive information. The security properties of SMPC ensure that no party can learn any information about the inputs of other parties, except for what can be inferred from the output of the joint computation. Additionally, the correctness property guarantees that the result of the computation is accurate and consistent with the agreed-upon joint function.[647]

Another technique used for privacy enhancement is the utilization of ring signatures. A ring signature is a form of digital signature that involves a collective endorsement of a message by a group of multiple participants using a shared key. In a ring signature scheme, any group member can affix their signature to the message, making it challenging to ascertain the precise identity of the signer. This imparts a degree of anonymity and privacy to the signing process.

The fundamental process behind this technique entails the creation of a signature through the utilization of the keys belonging to the members of the ring. Each member individually signs the message using their private key, and the resultant signature is then validated using the shared public keys of the group. [648] This mechanism makes it difficult to attribute the signature to a specific individual within the group.[649]

[647] In March 2020, a Blockchain-based framework utilizing the Homomorphic Encryption Technique was introduced. This framework addresses issues such as single-point failure, data integrity, and collusion attacks (in the semi-honest model). It offers a potential solution for the consensus and smart contract challenges in Blockchain technology. This framework is being applied in Decentralized Finance (DeFi) applications, such as Wanchain, which utilizes Secure Multi-Party Computation (SMPC) for privacy protection. Wanchain also facilitates interoperability with other Blockchains, including Ethereum in Wanchain 2.0 and Bitcoin in Wanchain 3.0. See Y. Yang, L. Wei, J. Wu, C. Long, *Block-SMPC: a Blockchain-based secure multi-party computation for privacy-protected data sharing*, in *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology,* 2020, pp. 46–51; T. Louie, *Welcome to Wanchain,* https://medium.com/wanchain-foundation/an-introduction-to-wanchain-a2936e25df91.

[648] R. Tso, *A new way to generate a ring: Universal ring signature*, in *Computer & Mathematics with Applications*, 2013, pp. 1350–1359.

[649] It is important to note that ring signatures exhibit some differences when compared to group signatures. In a ring signature scheme, a specific set of users can form the signing set without necessitating any additional setup or specific permissions. All members of the ring must possess

Due to the lack of inherent privacy and anonymity in Blockchain technology, various algorithms have been proposed to leverage the concept of ring signatures to enhance privacy and anonymity in Blockchain transactions. These algorithms aim to provide stronger privacy guarantees by incorporating the properties of ring signatures into the Blockchain system.

Even so, it is essential to note that ring signatures still need to be subject to standardization processes by either the developer communities or formal standardization bodies. In addition, it also remains to be seen if they reach the GDPR-required anonymization threshold.[650]

Another privacy-enhancing technology is differential privacy, which allows for collecting and sharing aggregate information about users while maintaining the privacy of individual users.[651] This is achieved by adding statistical noise to each user's data before it is shared with others. Introducing this noise makes it difficult to derive specific information about any individual from the aggregate data.

Three major strategies are commonly used in differential privacy: Laplace, Exponential, and Gaussian.[652] Laplace and Gaussian mechanisms are typically applied to numerical datasets, while exponential mechanisms are used for non-numerical datasets. These strategies help ensure that the privacy of individuals is preserved while allowing for the extraction of useful aggregate information.

However, it's important to note that the application of differential privacy comes with a trade-off between privacy and data accuracy. The amount of noise added to the data significantly impacts the precision and accuracy of the resulting aggregate

knowledge of each other's public keys, but they do not require any additional support or qualifications to participate in the ring.

[650] A. Giannopoulou (2021).

[651] C. Dwork, A. Roth, *The algorithmic foundations of differential privacy*, in *Foundations and Trends in Theoretical Computer Science*, 2014, pp. 211-407.

[652] M. U. Hassan, M. H. Rehmani, J. Chen, *Differential privacy in Blockchain technology: A futuristic approach*, in *Journal of Parallel and Distributed Computing*, 2019, pp. 50-74.

information. The trade-off is controlled by a parameter called epsilon.[653] Higher values of epsilon increase privacy by concealing sensitive information, but they may also reduce the usefulness or accuracy of the information.

Differential privacy is most effective when applied to scenarios where aggregate information is valuable and personalized data is not required. It is not suitable for personalized services where individual-level information is necessary.

Ultimately, in addition to the previously mentioned solutions, other technical approaches are proposed to enhance privacy and anonymity in Blockchain transactions. These include the use of one-time keys and adding noise to data.[654] The inclusion of salt in the hash function has also been recommended to reduce the likelihood of obtaining the original input value.[655] Another suggested technique is using third-party mixing services for public Blockchain transactions, which helps users mitigate the risk of re-identification by preventing "linkage attacks" that aim to uncover connections between transaction inputs and outputs.[656]

In addition, another solution to enhance anonymity is to avoid reusing public keys. Using a unique public key for each transaction makes it more challenging to de-anonymize a data subject.[657] This recommendation also applies to the context of smart contracts.[658]

The above illustration was meant to shed light on some interesting techniques that can protect user privacy by reducing the identifiability of data. They also introduce a

[653] E. ElSalamouny, S. Gambs, *Differential privacy models for location-based services*, in *Transaction on Data Privacy*, 2016, pp. 15-48.

[654] M. Al-Abdullah et al (2020).

[655] F. Molina et al (2021).

[656] N. Walters, *Privacy law issues in Blockchains: an analysis of PIPEDA, the GDPR, and proposals for compliance,* in *Canadian Journal of Law and Technology*, 2019, pp. 276-305.

[657] A. Shahaab, R. Maude, C. Hewage, I. Khan, *Managing gender change information on immutable Blockchain in context of GDPR,* in *Journal of British Blockchain Association*, 2020, pp. 23-28.

[658] C. Wirth, M. Kolain (2018).

trade-off by reducing the originality and utility of the data, limiting the service providers' ability to derive value from user data.

The application of Blockchain technology for privacy preservation is an active area of research, and various approaches and frameworks are being developed to maximize its potential in this regard. Further investigation is indeed necessary to comprehensively assess the strengths and weaknesses of different PETs, develop novel PETs or improve the effectiveness of existing ones, and address the challenges associated with deploying PETs in the online marketplace. It is crucial to educate individuals about the significance of these techniques, enabling them to make informed decisions regarding the adoption of suitable techniques to safeguard their information on the internet and maximize the benefits derived from these methods. Overcoming the issues of high computational requirements and limited usability remains a significant concern, as these factors contribute to the overall costliness of implementing PETs.

Furthermore, it is important to link the topic of privacy-enhancing technologies to privacy-by-design solutions. These concepts are closely related as they both aim to prioritize privacy considerations in the design and operation of systems. However, while PETs refer to specific technologies or techniques that enhance privacy, privacy by design is a broader framework that encompasses the integration of privacy principles throughout the entire lifecycle of a system or product.

This research claims that, to be a determinative approach, privacy by design should incorporate privacy-enhancing techniques as part of its implementation strategy.

In light of the above, Chapter IV will be dedicated to depicting the concept of Self-Sovereign Identity, which is, in our opinion, one of the most promising privacy-enhanced architecture for Blockchain applications[659] in order to demonstrate whether the aim of empowering individuals to maintain control over their digital identities across various applications can be practically achieved.

9. Conclusion

At first glance, some GDPR provisions seem ontologically incompatible with the main Blockchain characteristics. Hence, manifold points of tension have been identified.

This chapter focused on some overarching questions generally considered the most challenging, (i) Does data stored on Blockchain fall within the scope of the GDPR? (ii) Can the right to erasure apply despite Blockchain's immutability? (iii) Who is the data controller in blockchains?

In this regard, possible solutions based on living technologies have been outlined following the assumption that the technology and the Regulation aim to strengthen data subjects' control over their personal data.

It is worth noting that the starting point for any of the above considerations and, specifically, the thesis developed in this work is that the interplay between blockchains and GDPR can only be assessed by adopting a case-by-case analysis since tailored legal solutions are necessary for each case, as the outcomes depend on how the technology is designed.

Therefore, when assessing Blockchain compliance with the Regulation, it is crucial to consider that Blockchain technology is neither GDPR-compliant nor non-compliant per se; how it is used makes it compliant. This means that, instead of transposing to

[659] A. Tobin, D. Reed, *The inevitable rise of self-sovereign identity*, Provo: The Sovrin Foundation, 2016; M. Ma, C. Rumore, D. Gisolfi, W. Kussmaul, D. Greening, *SSI: A roadmap for adoption*, 2018, https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/a-roadmap-for-ssi.pdf; K. Wagner, B. Nemethi, E. Renieris, P. Lang, E. Brunet, E. Holst, *Self-sovereing identity. A position paper on Blockchain enabled identity and the road ahead*, Berlin: Blockchain Bundesverband, 2018.

decentralized environment concepts and rules specifically designed for a centralized framework, the intimate nature of this new technology should be understood to ensure the effective implementation of the data protection principles.

Understanding the characteristics of a Blockchain protocol (public or private, permissioned or permissionless) is crucial in defining the roles of different actors within the infrastructure. Consequently, analyzing data protection law from a micro-perspective and focusing on single individual transactions is more relevant than a macro-perspective.

From the research, it emerged that the purpose of processing in the Blockchain context refers to recording specific transactions onto the ledger, while the means pertain to the choice of the Blockchain platform.

Moreover, the work argued that blockchains (especially public and permissionless) might fall under the scope of the law if they have a presence in the European Union, such as having nodes within the EU, or if they target or monitor data subjects located within the Union.

Another element discussed was the identification of personal data within blockchains. According to the previous analysis, public keys are personal data under the GDPR since they serve as identifiers. One-time public keys can be used to minimize the risk of re-identification through techniques like singling out, linkability, or inference with additional data.

Notwithstanding, it is important to note that any additional data in the Blockchain can also be regarded as personal data if it directly or indirectly identifies an individual.

Private and permissioned Blockchain configurations may help comply with EU law regarding identifying controllers and processors. However, the identification of controllers in public and permissionless blockchains is contentious.

The key consideration is whether nodes and miners actively or passively process personal data on behalf of users. Even if they are passive in facilitating transactions, they should still be deemed processors akin to cloud providers. Users may be considered controllers, except when benefiting from the purely domestic exception. Nonetheless, the narrow interpretation of this exemption by the CJEU undermines data protection since users may not know if they interact with GDPR-compliant blockchains and personal transaction data gets replicated across different users' hardware.

As investigated, certification mechanisms and codes of conduct[660] may represent an instrument to determine GDPR compliance in Blockchain applications. However, due to most users' lack of *de facto* control, individual data protection rights might not be effectively enforced. Encouraging developers to build privacy-by-design Blockchain applications is advisable. Nevertheless, ruling on specific privacy-by-design guidance for industry stakeholders might hinder innovation and progress. In some instances, such as e-voting, privacy considerations should not be solely left to users, and a privacy-by-design perspective from the organization running the protocol should be expected.[661]

As widely argued, ensuring data subjects' rights on a Blockchain poses challenges. Interpreting the right to erasure contextually could include making data inaccessible, following the rationale of the Google case. Notwithstanding, a copy stored on a node might remain accessible outside European jurisdiction, and compliance with legal obligations under another law may exempt the right to erasure as per GDPR.

Implementing privacy solutions such as storing data off-chain, encryption, hash functions, noise adding, ring signatures, an editable Blockchain, and non-interactive zero-knowledge proofs can help address privacy concerns. Also, a fork in the

[660] For more details, see Chapter II.

[661] L. Moerel (2019), p. 851.

Blockchain protocol could allow for the modification of personal data. Nonetheless, these recommendations entail trade-offs that should be carefully considered for each use case.

Furthermore, whereas some have called for a revision of the regulation,[662] claiming it is already outdated,[663] this thesis argued that the technologically neutral structure of the GDPR allows for a different interpretation of some of its requirements and provisions. Regulatory flexibility may be the key to addressing those issues. The most illustrative example is the right to be forgotten, which can be interpreted in many different ways as there are different definitions of 'erasure'. Thus, an initiative by the regulators or interpretative guidance by DPAs[664] is necessary to shed light on those (arguable) problems.

What has been ultimately found is the need for further analysis and development of solutions that can reconcile the GDPR principles with Blockchain technology's unique features. It may be necessary to consider alternative technical approaches, such as some of the illustrated privacy-enhancing techniques to data subject rights in Blockchain networks. Additionally, clear guidelines and regulations may be needed to ensure that roles and responsibilities are attributed to actors in the DLT ecosystem.

[662] Recently, a *Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679*, COM(2023) 348 final, has been published. This proposal focuses on streamlining cooperation between data protection authorities when enforcing the GDPR in cross-border cases.

[663] A. Voss, *Fixing the GDPR: Towards Version 2.0*, 2021, https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf.

[664] The much-awaited Guidelines on Blockchain by the EDPB could likely clear the situation. These Guidelines were already mentioned in the 'EDPB Work Programme 2021/2022' (https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf) and they are included in the 'EDPB Work Porgramme 2023-2024' (https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf).

Chapter IV

Disentangling Nodes: Addressing GDPR in Blockchain-Based Digital Identity Systems

> *"Digital identities are the stories we tell about ourselves*
> *in bits and bytes; control your narrative."*
>
> *Aza Raskin*

1. Introduction

The previous chapter showed many (arguably) controversial issues regarding the relationship between European Data Protection law and Blockchain technology. For some of these, we have already tried to identify hypothetical solutions or mitigating factors;[665] for others, we have instead highlighted either the need for regulatory and case law guidance or modification from a technical point of view.[666]

[665] One of the mitigating solutions may be to identify certification mechanisms to narrow down architectural decisions for identifying data protection roles in the Blockchain context. For this controversial point, see section 4.1. of the previous chapter.

[666] For instance, to ensure the compatibility of the right to erasure with the Blockchain's immutability nature. See section 4.2.3. of the previous chapter.

In any case, we are aware that the proposed solutions will have to be re-evaluated in light of further technological advancement and legislation.[667]

In view of that, this chapter examines whether Blockchain technology can be leveraged to safeguard personal data by creating a digital identity management system (IDMS)[668] respectful of the principles of the GDPR. The objective is to evaluate the proposal's conformity with the established data protection principles outlined in the Regulation and covered in detail in the previous chapter.[669]

We chose to focus on the digital identity management system because, in this domain, users/data subjects are the central focus and operate as active agents of the data governance architecture. This, therefore, represents the most interesting use case to verify whether a decentralized system such as a Blockchain can be structured to support advanced techniques that implement privacy-enhancing solutions for decentralized data management. Proving that from a technical and legal point of view would achieve an important milestone: allowing data subjects to gain stricter control over their personal data while meeting both the requirements imposed by the GDPR and the main Regulation’s objectives, that is, giving natural persons control of their own personal data.[670] In this regard, several further initiatives have been launched,[671]

[667] For further details, refer to Chapter II of this thesis.

[668] Identity Management platforms can be described as systems that are utilized to facilitate the administration of digital identities or data related to digital identity.
Identity management serves the following purposes:
(i) Ensuring the reliability of identity information, including identifiers, credentials, and attributes.
(ii) Verifying the identity of various entities, such as users, subscribers, groups, user devices, organizations, networks and service providers, network elements and objects, and virtual objects.
(iii) Enabling the functioning of business and security applications.

[669] See paragraph 2.2. of Chapter III.

[670] See Recital 7 of the GDPR.

[671] Against this background, technology-driven tools have been developed to help data subjects and controllers exercise and comply with the GDPR. Some tools include:
(i) DataStreams.io: It serves as a consent manager for data controllers and a data stream manager for data processors, https://www.datastreams.io/.
(ii) The Data Transfer Project: This open-source platform enables direct user data portability between cloud services by converting proprietary APIs into standardized data formats. It was founded by Facebook, Google, Microsoft, and Twitter, https://dtinit.org/.

both from the private and public spheres, to argue for a human-centric approach to personal information.[672]

It follows that the GDPR and the Blockchain share a common ideological ground, which claims the need to change personal data management. While GDPR takes care of the policy side by setting up a standard, the Blockchain helps enable the implementation aspect by providing a unique framework.

Ultimately, the increasing integration of digital identity across online services has led to a growing reliance on Identity Management (IDM) Systems responsible for establishing, verifying, and managing these identities. However, the current practice of storing digital identities in centralized repositories controlled by a single authority represents a significant vulnerability, as this makes them attractive targets for attackers seeking to exploit security weaknesses and perpetrate identity theft or disseminate sensitive information. Hence, entities with privileged access to these repositories could collect and misuse users' data without their awareness or consent.

(iii) Fair&Smart: Designed to assist French data subjects, this application helps them claim GDPR rights, regain privacy control, and make informed decisions about trusted entities managing their personal data. It also offers GDPR compliance and management services for data controllers, https://www.fairandsmart.com/.
(iv) My Data Done Right: This project aids Dutch data subjects in exercising their Rights of Access (RoA) and Right to Data Portability (RtDP), https://mydatadoneright.eu/.
(v) DoNotPay: A legal services chatbot that offers various services, including seeking claims from Equifax for its security breach, https://donotpay.com/.
(vi) Jumbo Privacy: This application enables data subjects to back up and remove their data from platforms while allowing local access to that data, https://blog.withjumbo.com/.

[672] For instance, in 2014 the Finnish government published a study on the concept of *MyData.*
MyData promotes the notion that users should have enhanced visibility into the storage and utilization of their data and the ability to modify these aspects. It adopts a human-centric approach towards individuals' data, to return control of personal data to the users. In a separate context, Blockchain technology has garnered substantial research interest and industry focus in recent years, largely driven by the excitement and accomplishments associated with cryptocurrencies. See A. Poikola, K. Kuikkaniemi, H. Honko, *Mydata a Nordic model for human-centred personal data management and processing*, *Finnish Ministry of Transport and Communications*, 2015.

Moreover, another relevant issue caused by the majority of the IDM systems is that an identity owner never had control of their identity and its associated data.[673]

Within the scenario described, a decentralized identity system, precisely the Self-sovereign Identity (SSI),[674] may offer a solution for allowing users to take ownership of their identities and gain transparency into their data usage. Blockchain technology has undoubtedly played a pivotal role in conceptualizing SSI[675] as a decentralized and distributed environment where individuals have ultimate control over who can access and utilize their identity.

When defining the current regulatory scheme applying to Blockchain-based digital identity systems, we cannot identify a specific, widely recognized, or universally accepted legislative framework exclusively designed for addressing SSI. Notwithstanding, given that SSI typically concerns decentralized and user-controlled digital identities, it essentially involves the existing Data protection regulation, the GDPR, and the Digital Identity legislation, the eIDAS Regulation.[676] GDPR holds significant relevance in the realm of digital identity, considering that, by definition, identity information is personal data, while certain provisions of eIDAS can have

[673] N. Naik P. Jenkins, *An analysis of open standard identity protocols in cloud computing security paradigm*, in *14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016)*, IEEE, 2016; N. Naik, P. Jenkins, D. Newell, *Choice of suitable identity and access management standards for mobile computing and communication*, in *2017 24th International Conference on Telecommunications (ICT)*, 2017, pp. 1–6.

[674] Cfr. F. Wang, P. De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, in *Frontiers in Blockchain*, 2020.

[675] Kurihara expands the concept of SSI and describes the possibilities and problems when applying it to self-content management using the concept of Self-Content Management (SCM). In particular, in this paper, the author explores the possibility of self-sovereign management of digital content and discusses DRM using Blockchain technology as a means. See Y. Kurihara, *Self-Sovereign Identity and Blockchain-Based Content Management*, in D. Kreps, T. Komukai, T.V. Gopal, K. Ishii (eds), *Human-Centric Computing in a Data-Driven Society*, 2020, pp. 130-140.

[676] Regulation (EU) n. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

relevance to Blockchain technology at various levels, especially in the context of electronic signatures and trust services.

However, eIDAS does not encompass SSI, mainly focusing on government eIDs not integrating the new SSI paradigm. That is one of the reasons why this Regulation is under revision. The June 2021 Proposal to review the eIDAS Regulation (hereinafter "eIDAS 2.0")[677] has generated high expectations for a significant transformation in traditional identity models. The proposed user-centric identity model aims to establish European Digital Identity Wallets, granting citizens control over their data in identification and authentication processes, free from controlling entities providing identification services. Additionally, the proposed legal rules seek to provide legal certainty for electronic ledgers and blockchains, opening up possibilities for decentralization, particularly in the provision and management of user attributes. However, the implementation of qualified trust services for attestations or electronic ledgers imposes limitations on decentralization by requiring the involvement of a trusted third party.

The success of eIDAS 2.0 heavily relies on the development of common solutions. Standardization will be crucial in ensuring interoperability at the European Union level,[678] as we have already pointed out for Blockchain.

[677] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.
As the previous Regulation, also eIDAS 2.0 aims to support the Union's transformation towards a Digital Single Market. Hence, article 114 TFEU is the legal basis identified.

[678] The European standardization efforts concerning eIDAS 2.0 are distributed between two key organizations: ETSI and CEN. ETSI primarily concentrates on trust services, specifically focusing on establishing, authenticating, and safeguarding electronic signatures, seals, timestamps (known as ETSI ESI), and distributed ledger technology (referred to as ETSI PDL). On the other hand, CEN places its emphasis on areas such as the development of secure signature creation devices, decentralized identity management (including the fundamental aspects of Self-Sovereign Identity or SSI), wallet technologies (managed under CEN-CLC/JTC 19), as well as archiving solutions (overseen by CEN TC 468).
Establishing a coherent and easily understandable European standardization framework becomes increasingly crucial, given that these standards are slated to be cited in the predominantly obligatory implementing acts according to the eIDAS 2.0 proposal. Consequently, the referenced technical standards will effectively become legal obligations required for compliance with the regulation itself.

As a final remark to this premise, we deem it significant to specify that, although we are aware that SSI is a technological paradigm built on several principles, meaning that it is a technology-neutral concept which does not necessarily need Blockchain to be implemented, we use it interchangeably with the term 'Blockchain-based identity management systems'.

Based on the above, this chapter, along with assessing the challenges and opportunities of eIDAS 2.0, focuses on the compliance issues that Self-Sovereign Identity Solutions[679] face within the territorial and material scope of the GDPR and the resulting obligations. We explore the shared vision of Blockchain technologies, SSI, and key compliance mechanisms that decentralized solutions must address to fulfil their promises. Although similar inquiries have already been tackled in the previous chapter, albeit in general terms and in the context of (mostly public) blockchains, the unique technological framework crafted for decentralized identities offers a new breeding ground for evaluating GDPR compliance.

In light of this context, standardization efforts should concentrate on areas such as identification schemes, the EU Digital Wallet, and qualified attestation services, including the prerequisites for relying parties. These are evidently the central components of eIDAS 2.0. From a technical perspective, there should be a specific focus on ensuring the interoperability of Self-Sovereign Identity (SSI), particularly when it is built upon W3C specifications. Additionally, attention should be given to enhancing security and privacy requirements and optimizing the user experience. See S. Schwalm, I. Alamillo-Domingo, *Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0*, in *European Review of Digital Administration & Law*, 2021, pp. 89-108.

[679] Personal identity is typically established through Social Security numbers, driver's licenses, or passports. However, an equivalent robust approach to safeguarding online identities still needs to be improved. Blockchain technology offers the ability to create and utilize a digital identity as a reliable means for online transactions. Due to its immutability, Blockchain significantly reduces the risks of online fraud. Cfr. A.A. Monrat, O. Schelén, K. Andersson, *A survey of Blockchain from the perspectives of applications, challenges, and opportunities*, in *IEEE Access*, 2019, pp. 117134–117151.

2. Is the GDPR Truly Neutral Towards Technology?

Throughout the previous pages, we have often claimed that the GDPR adopts a technology-neutral approach,[680] almost apodictically. Therefore, it is at this point essential to validate this assertion's accuracy, as many subsequent discussions rely on this premise.

When we analyzed the relationship between technology and law,[681] we also mentioned the theory of Hilderbrandt and Tielmans, who defined when an act can be considered technology-neutral. Interestingly, they clearly distinguish between "technology-neutral law" and "technologically neutral law."[682] The former refers to the understanding that the legal effect should not depend on the specific technology that those subject to the law use. On the other hand, the term "technologically neutral law" implies that the law is independent of any technology.

These authors argue that the concept of a technologically neutral law is a misconception. They maintain that law inherently depends on a specific technological infrastructure and can never be entirely technologically neutral. Thus, applying this concept to the GDPR, the assessment should focus on whether the Regulation can be considered a technology-neutral law, meaning that it does not favor or discriminate against specific technologies in determining its legal effect. To do so, it is crucial to grasp the underlying purpose of the GDPR from the outset.

[680] Technology neutral differs from technology independent: "Technology-independent regulation ought to abstract completely away from technology, whereas technology-neutral regulation might be closely related to or intertwined with technology, as long as it does not favor one specific technology over another." B. J. Koops, *Should ICT Regulation be Technology-Neutral? Starting Points For Ict Regulation. Deconstructing Prevalent Policy One-Liners*, in B.J. Koops, M. Lips, C. Prins, M. Schellekens (eds), in *IT & Law Series*, 2006, pp. 77-108.

[681] See paragraph 2 of Chapter II.

[682] M. Hilderbrandt, L. Tielmans (2013).

In data protection, the traditional externality finds expression as an imbalance of power between the State and individuals, with the State having greater control over data collection, use, and retention. However, as the economic value of data has increased and technological advancements have made data accumulation and processing easier, the GDPR was adopted as a response to the technological externalities arising from developments in high-speed networking and data storage. The social costs imposed by these externalities were recognized in the Article 29 Data Protection Working Party Report,[683] highlighting the lack of control and information asymmetry risks. Information asymmetry refers to the significant disparity between the knowledge held by the data controller and the data subject regarding handling the latter's personal data.[684] Given that the GDPR is a response to technological externalities that threaten privacy and data protection, it is essential to analyze this Regulation by recalling the three interpretations of technology-neutral legislation put forward by Hilderbrandt and Tielmans, which, as already mentioned, are as follows:

(i) To maintain neutrality, the law may need to include technology-specific provisions to preserve the essence of the legal rights they support. The objective is to achieve equivalent outcomes in both online and offline environments.

(ii) Legislation should avoid discriminating between technologies with similar functionalities, as such discrimination could hinder innovation and lead to unfair competition.

(iii) There is a fundamental need for legislation to be adaptable to the future context. Since legislative acts often take a considerable time to come into effect, focusing on a specific technology may render the legislation outdated and ineffective sooner than anticipated.

[683] Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, WP 223, 2014, p. 6.

[684] P. J. Van de Waerdt, *Information asymmetries: recognizing the limits of the GDPR on the data-driven market,* in *Computer Law and Security Review*, 2020.

By examining the GDPR through these three lenses, we can assess its adherence to the principles of technology neutrality and its effectiveness in addressing the challenges posed by technological advancements.[685]

The GDPR, with its commitment to technology neutrality, emphasizes data protection by design and default as a fundamental characteristic. Article 25 of the Regulation specifically mandates implementing technical and organizational measures, including pseudonymization, to uphold data protection principles. The specific nature of the provision recognizes that technology can, on its own, establish equivalent protection. Thus, as embodied in Article 25, technological specificity is essential for achieving technology-neutral legislation.[686] Furthermore, recognizing the ever-evolving technological landscape, the legislator formulated GDPR provisions to ensure that the Regulation remains effective in protecting data privacy over time.

Based on these considerations, the GDPR possesses the necessary features to be regarded as a technology-neutral law. However, the true assessment of this claim can only be made when confronted with practical applications. Using the Blockchain model for digital identity management presents an opportunity to evaluate the Regulation's technology-neutral credentials in practice.

Against this backdrop, we argue that the GDPR's openness to innovative technologies like Blockchain hinges on how it is classified as a regulatory instrument.[687]

[685] M. Hilderbrandt, L. Tielmans (2013), p. 510.

[686] In addition to data protection by design, the GDPR grants data subjects the right to data portability, which is closely linked to interoperability, a prerequisite for dynamic efficiency. This empowers individuals to request data transfer from one data controller to another, potentially utilizing different technologies to ensure privacy-friendly defaults. This approach avoids discrimination against specific technologies, promoting a level playing field. For more on the right to data portability see R. Janal, *Data Portability - A Tale of Two Concepts*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, pp. 59-69.

[687] For an understanding of different regulatory instruments, see B. Morgan, K. Yeung, *An Introduction to Law and Regulation: Text and Materials,* Cambridge University Press, 2007, p. 79.

In Chapter II, we explored different regulatory instruments and categorized them into three groups: command-and-control, self-regulation, and co-regulation. If classified as a command-and-control regulatory instrument, the GDPR would be considered a traditional regulation implemented through rule-based enforcement.

Advocates argue that self-regulation within industries is particularly effective when overseeing activities that involve highly technical or specialized knowledge, such as collecting, storing, and processing personal data on a Blockchain.[688] They claim that industry self-regulation benefits from superior informational capacities compared to the State. The flexibility and adaptability of self-regulation to evolving technological demands are considered advantages over traditional command-and-control regulation. Nevertheless, self-regulation has its limitations. It needs formal government approval and may fall to achieve public goals due to a lack of enforceable measures. Some authors highlight that strict self-regulation may fail to attract sufficient industry involvement and address the need for international privacy standards.[689]

As a result, co-regulation emerges as a more desirable approach that strikes a balance between pure self-regulation and command-and-control regulation. Interestingly, if GDPR is seen as falling into the category of co-regulation, it would be more inclined to accommodate a Blockchain-based solution for digital identity management. Co-regulation can be achieved through measures like standardization. In this regard, it is worth considering that the European Commission requested[690] the

[688] Cfr. Section 4.4. of Chapter II.

[689] D. D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct,* in *Ohio State Law Journal*, 2013, p. 1043.

[690] Article 10 of Regulation 1025/2012 defines the process for requesting standardization from European Standardisation Organisations (ESOs). The European Commission prepares a request that outlines policy goals, relevant legislation, and the need for standardization in a specific field or topic. This request, known as the "mandate," also specifies the desired deliverables and objectives to be achieved. From a legal standpoint, the standardization request is a Commission Implementing Decision based on Regulation 182/2011 (OJ L 55, 28/2/2011). ESOs have one month to accept or reject the request upon receipt. The standardization request becomes a legally binding contract for both parties if accepted.

European Standardization Organizations (ESOs) to develop privacy and personal data[691] management standards. Based on Regulation 182/2011, this decision mandates the ESOs to establish these standards.[692] The standard-setting activity is overseen by the Commission, making it part of the realm of co-regulation.[693] Although the mandate pertains to the Data Protection Directive, we argued that, since the GDPR recognizes standardization and certification,[694] such standard-setting activities would have a

This regulatory approach involves the oversight of the Commission throughout various stages: as an observer in the Technical Committee meetings responsible for the standardization work and by approving the Workplan developed by the Technical Committee before commencing the deliverables' development. ESOs maintain their independence regarding the content of the deliverables and administration, aligning with the market-driven nature of co-regulation.

[691] It is worth highlighting that the use of the terms 'privacy' and 'personal data protection' in the standardization request appears inconsistent, as they are sometimes used interchangeably. However, it's important to note that the right to private life and the right to the protection of personal data are distinct rights outlined in articles 7 and 8, respectively, of the Charter of Fundamental Rights of the EU. In light of this observation, it should be clarified that 'data protection by design and by default' is not the same as 'privacy by design and by default.' These terms differ both in content, as they correspond to different rights, and in legal status, as 'data protection by design and by default' is a legal obligation established in Article 25 of the GDPR.

[692] Commission Implementing Decision of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy. This was the first standardisation request based on the fundamental right of protection of personal data as enshrined in Art. 8 of the Charter and art. 16 of the Treaty on the Functioning of the European Union (TFEU).

[693] Even though, in principle, standardization qualifies as collective self-regulation, there are exceptions to this argument. The aim of such requests is to establish 'an agreed way of meeting legal requirements on health, safety, environmental protection, civil security and interoperability' and to 'promote technical development' (European Commission, 2015). A standardization request may be issued in support of an EU policy or legislation. Therefore, the technical standards resulting from the standardization request can be considered a form of co-regulation since they involve regulatory involvement in the standardization process while allowing ESOs flexibility in determining the deliverables' type and content.

[694] Importantly, the GDPR emphasizes the importance of technical standards not only as a general best practice approach but also as a means to promote transparency in data controller practices and ensure compliance with the legislation. Standardization and certification are endorsed in relation to new modalities and tools introduced in the GDPR, such as data protection by design and by default (Article 25 of the GDPR). The provisions of the GDPR regarding standardization differ between the preparatory works and the final text. The final text explicitly mentions technical standards in Article 43 of the GDPR. In the European Parliament's First Reading version from 2014, standardization was included in provisions related to standardizing information policies, provision of information to data subjects,

mandate under the GDPR for co-regulation.[695] This may provide an opportunity, for instance for Blockchain-based digital identity management platforms, to align with the GDPR requirements, should them be able to demonstrate their qualifications during the standardization process conducted by the ESOs.[696] However, the standard-setting process must ensure the participating technology adheres to mandatory legal mandates.[697] Therefore, if a digital identity solution based on Blockchain technology can establish its adherence to GDPR legal requirements and successfully showcase its technological capabilities, it will potentially be adopted as a recognized technical standard for data protection by design. As noted by Falke et al.,[698] compliance with standards can possibly give rise to 'legitimate expectations,' leading individuals to perceive them as having official legal status. This could anchor the legal recognition of a Blockchain-based solution through a co-regulatory approach.

The analysis above illustrates that the GDPR, by itself, may not be sufficient to tackle emerging technology-related challenges effectively. Interpreting the GDPR as a

exercise of the right to object, and data security processing of personal data concerning health. The omission of direct references to technical standards in the final text is a legislative choice that allows for greater flexibility in the standardization activity in the field. This choice enables flexibility in terms of the subject matter of the standards to be developed, as it avoids specific references to Commission standardization. It also allows both the standardization bodies and the European Commission to initiate and carry out standardization activities.

[695] E. Lachaud, *The General Data Protection Regulation and the rise of certification as a regulatory instrument*, in *Computer Law and Security Review*, 2018, pp. 244–256. In addition, it is important to consider that the GDPR encourages the use of codes of conduct, data protection certification mechanisms, data protection impact assessments, and technical standards to promote transparency and compliance with the law.

[696] For instance, the EN 17529 'Data protection and privacy by design and by default' was developed in response to a request from the European Commission and it provides manufacturers and service providers with requirements before, or independently of, any specific application integration, https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:63633,2307986&cs=11F702120AA40D5CC2DD42848140B1806.

[697] I. Kamara, *Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate,* in *European Journal of Law and Technology*, 2017, pp. 1-24.

[698] J. Falke, H. Schepel (eds.), *Legal Aspects of Standardisation in the Member States of the EC and of EFTA*, vol 1, in H. S. A. Luxembourg: Office for Official Publications of the European Communities, 2000, p. 181.

regulatory tool that permits co-regulation may support the Regulation in fulfilling its objective of maintaining a technology-neutral stance.

In any case, it remains uncertain whether the digital identity management model constructed upon Blockchain technology can definitively establish its adherence to GDPR legal requirements. This challenge still needs to be surmounted.

In order to get a clear picture and understand the terms of the question, the following sections will delve further into this topic and discuss the opportunities brought about by (decentralized) identity management and the role of Blockchain technology in this regard.

3. Digital Identities in a Networked Society: Shaping Individuality in Virtual Realms

In the era of information,[699] the "privacy paradox"[700] lies at the heart of the ongoing struggle to protect data. This paradox represents the inherent trade-off between the value of personal data and the value individuals place on accessing online services,[701] which increased considerably during the COVID-19 pandemic.[702]

The abundance of personal data generated in today's data-intensive technological landscape has shaped our data-driven society and sparked a newfound concern for

[699] "Our lives have become increasingly digital and so has the vast amount of personal data traces that we leave behind. The current situation is that a few large multinational corporations make the majority of profits by offering services users pay for with their data. While data analytics can provide users with better services, the users' overview and control of their personal data has decreased.", see B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, R. Vatrapu, *BPDIMS: A Blockchain-based Personal Data and Identity Management System*, in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019, p. 6855.

[700] "The privacy paradox states that the information disclosure of Internet users is problematic; although many people are concerned about their privacy online, they still share plenty of personal information on the web.", T. Dienlin, P. K. Masur, S. Trepte, *A longitudinal analysis of the privacy paradox,* in *New Media & Society*, 2023, p. 1044.

[701] World Economic Forum (WEF), *Reimagining Digital ID*, 2023, https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf.

[702] J. Suh, E. Horvitz, R. W. White et al, *Disparate impacts on online information access during the Covid-19 pandemic,* in *Nature Communication*, 2022, pp. 1-15.

privacy and data protection online.[703] This has progressively led to the striving for a new and standardized ecosystem for digital identity, which has gained increasing attention from various entities and stakeholders. Consequently, numerous identity management solutions are emerging in different jurisdictions to create a unified, privacy-preserving identity that bridges offline and online realms.

The digital identity market is already substantial and diverse, addressing different needs such as financial inclusion, reputation management, and privacy-enhanced social media identities. Within this landscape, the concept of self-sovereign identity has resurfaced, although a clear, universally accepted definition is yet to be established. Self-sovereign identity can generally be described as an identity management system developed by private or public entities, guided by loosely defined principles and lacking a universally recognized standard.

Overall, it represents a technological solution that embodies the ideals of autonomy and individual control over digital data through decentralization and user-centric identity management systems.

As already mentioned, the development of self-sovereign identity projects has become closely intertwined with advancements in Blockchain technology and mainstream adoption efforts due to their shared objectives and features. The success of self-sovereign identity solutions holds significant importance for Blockchain proponents as it could represent a prominent implementation of this technology.

Within the legal context of digital identities, the eIDAS Regulation[704] plays a significant role by defining trust service levels and establishing a regulatory framework to develop identity systems that meet legal requirements. Moreover,

[703] M. K. Hamza, H. Abubakar, and Y. M. Danlami, *Identity and Access Management System: a Web- Based Approach for an Enterprise*, in *Path of Science*, vol. 4, no. 11, 2018, pp. 2001–2011; T. Rathee, P. Singh, *A systematic literature mapping on secure identity management using Blockchain technology*, in *Journal of King Saud University - Computer and Information Sciences*, 2021.

[704] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

compliance with the GDPR is mandatory for identity providers. However, aligning with these European regulations poses certain difficulties and decentralized technologies, which underlie contemporary identity solutions, introduce complexities in achieving privacy by design and complying with chosen technological methods and structures. Furthermore, the domain-dependent nature of many applicable legal norms, particularly in highly regulated areas like financial markets and institutions, adds to the (already intricated) framework. The coexistence of these diverse legal obligations often creates tensions between the applicable legal rules and the technology's objectives, making it challenging to reconcile them.

Before delving into the issue of whether developing an identity management tool on the Blockchain platform could offer a more efficient approach to safeguarding personal data, it is first necessary to introduce a set of principles and terminology.

3.1. Laying the Groundwork

Overall, there is no uniformity within the field of identity regarding key terms such as "identity," "identifier," "attributes," and "persona." These terms are often used interchangeably and ambiguously without clear definitions.

In this paragraph, we aim to provide a preliminary distinction between these.

The term "identity" has different meanings depending on the field of study.[705] Psychology typically encompasses all an individual's personality traits, including

[705] For this thesis, we use the term "identity" to describe all the attributes that uniquely define a person over their lifetime, providing a sense of sameness and continuity despite varying circumstances. It is important to consider that there exists a difference between "numerical identity," which refers to the exclusive relationship between a thing and itself, and "qualitative identity," which describes shared properties among different things. Only when there is complete qualitative identity between two entities they can be considered numerically identical. Cfr. B. Garrett, *Personal Identity and Self-Consciousness*. London, Routledge, 2002.

beliefs, and other personal attributes.[706] In sociology, it includes culture, history, religion, and traditions that an individual is a part of.[707]

From a legal perspective, identity can be associated with the concept of a "natural person" (an actual human being) or a "legal person" (such as a company, trust, partnership, or other collective entity recognized as a single entity under the law).

The attributes of an identity are not permanent and can change over time. Identity construction is indeed an ongoing, dynamic and multifaceted process where an individual develops and evolves through interactions with their environment. As a consequence of these peculiarities, any identity management system must be designed to be flexible and resilient enough to accommodate the variable and complex nature of human identity.

Nevertheless, no matter how sophisticated these systems become, they can only partially capture some aspect of a person's identity. Attempting to design a system that manages and categorizes various identities requires an understanding that such an arrangement will inevitably reduce the specific facets or use cases of each identity it encompasses.[708]

A "persona" refers to a specific aspect of an identity expressed in a particular social context. While an identity uniquely defines a person, individuals can embody

[706] N. Strohminger, J. Knobe, G. Newman, *The true self: a psychological concept distinct from the self*, in *Perspective on Psychological Sci*ence, 2017, pp. 551–560.

[707] J. E. Côté, *Sociological perspectives on identity formation: the culture–identity link and identity capital*, in *Journal of Adolescence*, 2016, pp. 417–428. Furthermore, from a social point of view, digital identity presents a series of specific properties, identified by the OECD, cfr. M. Rundle, B. Blakley, J. Broberg, A. Nadalin, D. Olds, M. Ruddy, P. Trevithick, *At a crossroads: "personhood" and digital identity in the information society*, STI Working Paper 2007/07, Organisation for Economic Co-operation and Development (OECD), 2007.

[708] P. J. Eakin, *How Our Lives Become Stories: Making Selves*, Cornell University Press, 1999.

multiple personas depending on their specific social context.[709] From a technical standpoint, personas can be seen as pseudonyms or practical identities[710] used for authentication purposes within an identity management system.[711]

An "attribute" describes an essential property of a person that qualifies them as a member of a particular set or class. Attributes are not unique to an individual and can include inherent elements like gender, height, weight, or capabilities and assigned elements like nationality or citizenship. These attributes are often used to identify or distinguish individuals into specific categories. It's important to note that these clusters are often abstract and can be arbitrarily defined, even when they refer to inherent properties.

In contrast, an "identifier" does not describe or qualify a person but refers to a real-world identity or a specific persona.[712] Identifiers are often assigned arbitrarily by a third party for a particular use case or domain. Examples of identifiers include legal names, social security numbers, or usernames. In some cases, identifiers can represent observable properties of an entity, such as fingerprints or biometric data.[713] It is important to understand that attributes and identifiers are technically data strings used for authentication. However, attributes classify individuals within specific

[709] J. R. Suler, *Identity management in cyberspace*, in *Journal of Applied Psychoanalytic Stud*ies, 2002, pp. 455–459.

[710] J. Christman, *Social practical identities and the strength of obligation*, in *Journal of Social Philosophy*, 2013, pp. 121–123.

[711] K. Toth, M. Subramanium, *The persona concept: a consumer-centered identity model*, in *3rd International Workshop on Emerging Applications for Wireless and Mobile Access,* 2003.

[712] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope, *Trust Requirements in Identity Management*, in P. Montague, & R. Safavi-Naini (Ed.), *Australasian Information Security Workshop 2005* (AISW 2005). Conferences in Research and Practice in Information Technology, pp. 99-108.

[713] A. Nagar, K. Nandakumar, A. K Jain, *Biometric template transformation: a security analysis*, in *Media Forensics and Security II,* 2010; A. Ross, A. K. Jain, *Multimodal biometrics: an overview*, in *2004 12th European Signal Processing Conference*, 2004, pp.1221–1224; N. Duta, *A survey of biometric technology based on hand shape*, in *Pattern Recognition*, 2009, pp. 2797–2806.

categories, while identifiers are intended to uniquely label individuals within a particular domain. While some identity management systems allow multiple individuals to share the same identifier or for one individual to have multiple identifiers (such as pseudonyms), it is desirable, for the purpose of identification and authentication, that an identifier ensures both uniqueness (no two people share the same identifier) and singularity (one person has only one identifier within the same domain). Most identifiers consist of random strings of unique characters within a specific domain. They are typically issued by centralized entities such as government agencies or administrative bodies (e.g., passport numbers or social security numbers) or companies or organizations (e.g., bank account numbers or email addresses).

In this context, centralization helps ensure the uniqueness of identifiers (e.g., avoiding assigning the same social security number to different individuals) and their singularity within an identity. Alternatively, individuals can generate identifiers, such as cryptographic keys for accessing cryptocurrency wallets. In this case, uniqueness is mathematically guaranteed with high probability, but singularity cannot be guaranteed (i.e., the same person can generate multiple identifiers).[714]

There are also decentralized identifiers - so-called DIDs that will be analyzed in the following - which utilize web addresses (URLs) as unique identifiers that link to publicly identified information about an identity subject. DIDs can be combined with Blockchain technology and public-private key pairs.

Understanding the distinctions between personas, attributes, and identifiers is crucial in designing effective identity management systems that revolve around digital identities nowadays. Considering that the Internet represents an integral part of our daily lives and poses a significant challenge for identifying the constantly

[714] P. Schartner, M. Schaffer, *Unique user-generated digital pseudonyms*, in *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, Springer, 2005, pp. 194–205.

expanding population of online users, the proliferation of digital identities has surged in tandem with the Internet's growth. In response to this situation, identity providers progressively emerged and assumed the role and responsibility of generating and overseeing users' (digital) identities, typically distinguished by specific attributes like email addresses and passwords.

Beyond its formal definition,[715] it is worth noticing that digital identities represent how we all identify ourselves during our online interactions, which now account for a large part of our daily communications. They have become increasingly important due to the spread of digital services,[716] as they enable digital representation of personal data. Although the notion can be applied to various entities, including hardware such as IoT devices and organizations,[717] this thesis primarily focuses on individual digital IDs, particularly the SSI model, which is much more individual-centered.

Since, to date, several prototypes of digital identity management have followed one another, it is very important to know them to understand how the Self-Sovereign Identity is a radical innovation in this field.

[715] The WEF Report states, "Digital ID provides a means of making claims about personal data through digital channels."

[716] The growing adoption of digital technology and the advancement in AI highlight the significance of establishing digital ID systems. According to the Financial Action Task Force (FATF), a global financial crime watchdog, digital transactions are increasing at an estimated annual rate of approximately 12.7%. As more transactions, whether online purchases or accessing in-person services rely on digital technologies, the development of effective digital ID solutions becomes increasingly essential. See Financial Action Task Force (FATF), *Guidance on Digital Identity*, 2020, pp. 1-105.

[717] S. Pal et al, *On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation*, in *IEEE Internet of Things Journal*, 2019, pp. pp. 2630-2639.

3.2. From Centralized to Decentralized: Evolving Digital Identity Models for the Digital Age

On a high level, we can distinguish two different models in identity management before decentralized identity: the centralized and the federated model.

In a centralized model,[718] also referred to as 'Silos model', the organization that offers a particular service retains a central position. To grasp the essence of a centralized digital identity model, one can envision scenarios where the establishment of an account with the organization operating a specific service is imperative, and the identity and all associated details are encompassed within the account itself. Users can formulate their digital identity within this framework, often as an 'account.' In this context, the service provider coincides with the identity provider, granting users access to services by requesting unique 'secrets' only the user should know, such as passwords or PINs.

All personal data belonging to users is stored within the organization's internal databases, referred to as 'Silos,' which aptly justifies the 'Silos Model' nomenclature.

In this completely centralized model, users entirely depend on the organizations retaining their data in centralized databases, where cybersecurity threats loom large in the event of breaches, which may lead to the exposure of sensitive user information.[719] Entrusting centralized authorities in the online realm with control over digital identities presents similar issues to those encountered with State authorities in the physical world. Users become reliant on a single authority that can deny or falsely confirm their identity. Centralization inherently grants power to these centralized entities rather than to the users themselves. Therefore, the current state of online

[718] M. Laurent, J. Denouël, C. Levallois-Barth, P. Waelbroeck, *Digital identity*, in M. Laurent, S. Bouzefrane (Eds.), *Digital Identity Management*, 2015, pp. 1-45.

[719] The numerous hacking incidents, including the recent one involving EasyJet, are examples. In 2020, EasyJet admitted that a "highly sophisticated cyber-attack" had affected approximately nine million customers, https://www.bbc.com/news/technology-52722626.

identity remains centralized or, at best, hierarchical. Digital identities are typically owned by certificate authorities, domain registrars, or individual websites, and users are merely granted temporary access or have their identities revoked at the discretion of these entities.

As the Internet expanded and power consolidated within hierarchies, a new problem arose: the 'multiple identity phenomenon.'[720] With the proliferation of websites, users found themselves juggling numerous identities across various platforms yet lacking control over any of them. In this context, a movement aimed at giving control of identities to individuals themselves, allowing them to have genuine ownership and control, has been gaining ground. Fundamentally, the centralized identity management model raises concerns regarding the user experience and the level of control individuals have over their online identities. This has then led towards the federated model, which seeks to tackle some of these issues.

In the federated model, the identity provider (IDP) is the custodian of the user's digital identity and associated data, acting as a bridge between the user and the accessed services. Under the federated model,[721] users utilize their digital identity through the IDP, enabling access to various services. An example of an IDP is Google which serves as a federated digital identity management platform, allowing users to access various services through their Google account, such as public Wi-Fi networks that require authentication via Google or Facebook accounts.

[720] O. Yu. Kurnykin, *The Phenomenon of "Multiple Identity" in Modern Kyrgyz Society*, in *Izvestiya of Altai State University*, 2021, pp. 73–78.

[721] D. Pöhn, P. Hillmann, *Reference Service Model for Federated Identity Management*, in *Lecture Notes in Business Information Processing*, 2021, pp. 196–211; R. Baldoni, *Federated Identity Management systems in e-government: The case of Italy*, in *Electronic Government*, 2012, pp. 64-68; D. W. Chadwick, *Federated identity management*, in *Lecture Notes in Computer Science*, 2009, pp. 96–120; D. Smith, *The challenge of federated identity management*, in *Network Security*, 2008, pp. 7–9; C. Satchell, G. Shanks, S. Howard, J. Murphy, *Identity crisis: User perspectives on multiplicity and control in federated identity management,* in *Behaviour and Information Technology*, 2011, pp. 51–62.

In this model, users are frequently compelled to establish a new association with an unfamiliar IDP, separate from the organization they intend to engage with. The IDP becomes a centralized personal information repository, storing credentials and other data for all its clients' employees and customers. Additionally, the IDP plays a pivotal role in defining the constraints of data structures and schema, and it must maintain direct connections with all network participants, limiting flexibility and scalability. Moreover, as exemplified by the Cambridge Analytica scandal, [722] the IDP establishes and enforces policies or chooses not to do so.

This model eliminates the need for users to maintain multiple identities by providing a Single Sign-On experience. Nonetheless, there are some similarities with the centralized model: the user does not have true ownership of their digital data, as it is held by a third party, i.e., the identity provider,[723] which has to be involved in every user's access to online services. This construction also raises privacy concerns for users, as the identity provider can potentially monitor the services accessed using the user's digital identity.

From this *excursus*, it emerges that user-centric designs have transformed centralized identities into federated identities with centralized control while maintaining a certain degree of user consent for sharing their identity information, including the choice of recipients.

This transition marked a significant advancement towards granting users more control over their identities, but it was merely a preliminary step. Advancing further necessitated empowering users with autonomy over their identities, which is the core of self-sovereign identity.

[722] See note 31 of this thesis.

[723] Cfr. S. Landau, H. Le Van Gong, R. Wilton, *Achieving privacy in a federated identity management system,* in *Lecture Notes in Computer Science*, pp. 51–70.

4. Blockchain-Based Digital Identity Systems: Is this a way forward?

Although there is no agreed-upon definition yet on what the terminology really means, for the scope of this research, self-sovereign identity[724] is defined as an independent,[725] long-lasting, and portable identity for individuals, organizations, or entities that enables the owner to access relevant digital services utilizing verifiable credentials linked to the identity in a privacy-preserving manner.[726]

In 1996, Carl Ellison explored the creation of digital identity in his paper "Establishing Identity without Certification Authority." He examined the use of Certificate Authorities and peer-to-peer systems like PGP as potential means of defining digital identity. He also proposed a method that involved verifying online identity by exchanging shared secrets over a secure channel. This interesting approach allowed users to control their identity without relying on a managing authority.

Ellison's involvement in the SPKI/SDSI project[727] showcased another step towards reimagining identity systems. The project aimed to establish a streamlined public infrastructure for identity certificates, intending to replace the complex X.509 system. While centralized authorities were considered as a possibility, they were not the sole focus.

Against this background, as significant as these developments were, a more revolutionary reimagining of identity was necessary in the 21st century to truly prioritize self-sovereignty and bring it to the forefront.

[724] Q. Stokkink, J. Pouwelse, *Deployment of a Blockchain-Based Self-Sovereign Identity*, in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1336-1342.

[725] " (…) each of us is owned by the state, which grants leeway (...) to govern and dispose of certain aspects of our bodies and lives"; see G. Trotter, *Autonomy as self-sovereignty*, in *HEC Forum*, 2014, p. 245.

[726] N. Naik, P. Jenkins, *Governing principles of self-sovereign identity applied to Blockchain-enabled privacy-preserving identity management systems*, in *IEEE International Symposium on Systems Engineering*, 2020, pp.1-6.

[727] C. M. Ellison, *SPKI/SDSI Certificates*, 2004, https://theworld.com/~cme/html/spki.html.

One of the earliest mentions of sovereign identity dates back to February 2012, when developer Devon Loffreto introduced the concept of "Sovereign Source Authority."[728] Loffreto argued that individuals possess an inherent "right to an 'identity'" but asserted that national registration undermines this sovereignty. Furthermore, in March 2012, Patrick Deegan initiated the development of Open Mustard Seed,[729] an open-source framework with the objective of empowering users to have control over their digital identities and data within decentralized systems. This initiative was part of a wave of "personal cloud" projects that emerged during that timeframe.

From a technical standpoint, self-sovereign identity is widely recognized as a novel approach to online identity management. In this paradigm, individuals and entities have the ability to oversee their identity-related information, such as identifiers, attributes, credentials, and other personal data. They can store this information either locally on their own devices or remotely on a distributed network. Additionally, they can selectively grant access to this information to authorized third parties without relying on any trusted authority or intermediary operator to provide or validate these claims.[730] This approach empowers individuals and entities with greater control over their personal identifying information and other pertinent data.

Since digital identifiers can take various formats, it is crucial to establish technical standards for ensuring interoperability in a global identity system. One of the most prominent standards in this regard is the Decentralized Identifier (DID), which we will discuss after analyzing the guiding principles of self-sovereign systems.

[728] D. Loffreto, *What is 'Sovereign Source Authority'?*, The Moxy Tongue, 2012, http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

[729] Open Mustard Seed, Open Mustard Seed (OMS) Framework, 2013, https://idcubed.org/open-platform/platform/.

[730] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, *A survey on essential components of a self-sovereign identity*, in *Computer Science Review*, 2018, pp. 80–86.

4.1. SSI Principles

Christopher Allen[731] introduced the concept of SSI as a framework based on principles to establish a decentralized system of user-centric, self-administered, and interoperable digital identities. Inspired by Kim Cameron's Laws of Identity,[732] this framework consists of ten foundational principles which summarize the main (desirable) elements of an ideal decentralized and self-sovereign identity.

SSI can be understood from two perspectives: the first is ideological, emphasizing the significance of individuals having control over their own online identity without the necessity for counteracting trust. The second perspective is technological, involving an analysis of the technologies and standards that can facilitate this objective.

The ten mentioned principles of SSI are specifically designed to outline the values and objectives that both the concept and technology should aim to achieve.
These principles are grouped into three main dimensions: controllability, portability and security.

The Controllability dimension consists of:

(i) *Existence* which underscores a user's need to possess an independent presence within the digital realm. This concept originates from the fundamental element of 'self' intrinsic to identity. In the contemporary context of increasing societal complexity, identity often merges with state-issued credentials such as driver's licenses and social security cards. This merger implies that a person's identity could be at risk if the state were to revoke these credentials. These credentials translate from the physical

[731] C. Allen, *The path to self-sovereign identity*, in *Life with Alacrity*, 2016, https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html#dfref-1212.

[732] K. Cameron, *The laws of identity*, in *Kim Cameron's Identity Weblog*, 2005, https://www.identityblog.com/?p=352.

world to the virtual sphere, creating a digital representation of the self. This principle asserts that a user should have the ability to exist in the digital world independently, without reliance on a third party.

(ii) *Control* which means that users should have full control over their identities. Recent incidents involving identity breaches, like the Cambridge Analytica scandal and significant Equifax-style data breaches,[733] have raised questions about data ownership. Sovereignty empowers users to determine how their identity is utilized without disrupting societal organization negatively. It's essential to clarify that control doesn't mean users can decide what data is associated with them, but the key difference is that once credentials are issued, users have control over it.

(iii) *Consent* which entails that the sharing of data can only happen when a user provides consent.

The Portability dimension:

(iv) *Access* entails that users must have unfettered access to their own data and related claims without the intervention of gatekeepers or intermediaries. This doesn't necessarily grant the user the authority to modify all aspects and claims associated with their identity. Still, it does ensure access to records reflecting any alterations linked to their identity. To safeguard the sovereignty of other users, an individual should only be granted access to their identity and not others.

[733] The Equifax data breach took place between May and July 2017, affecting the American credit bureau Equifax. This cyberattack exposed the personal records of 147.9 million Americans, 15.2 million British citizens, and approximately 19,000 Canadian citizens, marking it as one of the largest cybercrimes linked to identity theft. In response, Equifax reached a settlement with the United States Federal Trade Commission, offering affected individuals settlement funds and complimentary credit monitoring services. For further details: https://www.cbsnews.com/news/china-denies-responsibility-in-equifax-breach-after-doj-charges-four-military-members/; https://www.cnet.com/news/privacy/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-changed/.

(v) *Transparency* necessitates that algorithms and infrastructures operate openly. In tandem with the previous principle, transparency allows users to monitor any potential mismanagement of claims, credentials, or associations connected to their identity. In this context, transparency also integrates fairness and supports a balanced identity system, enhancing individual protection. Systems and algorithms should therefore operate transparently in an intelligible and easily accessible format, using clear and simple language.

(vi) *Portability* ensures that identity-related information and services are easily transferable. According to Allen, information and services must be effortlessly transferable and not exclusively controlled by a centralized third-party entity. Portability ensures that an individual's identity can be transferred and stored in multiple locations, as decided by the user's discretion.

(vii) *Interoperability* allows identities to be usable across various contexts and across international borders. This principle is linked to the principles of persistence and portability.

Security dimension:

(viii) *Persistence* means that identities should have a long-term lifespan determined by the user's discretion. Amidst the constant changes in data storage and private key rotation, persistence enables users to maintain their identities, even with multiple private keys. Persistence refers to individuals, institutions, organizations, and collective entities, allowing their identities to be determined by other entities' discretion. Identifiers within an SSI system should exclusively belong to the person or persons who created them.

(ix) *Minimization* emphasizes the meaning of safeguarding users' personal data when disclosing identity-related information. For instance, if a minimum age is required to access a particular service, users should not be compelled to provide their exact birth date. Instead, user disclosure should be minimized to meet the minimum age requirement. Through selective disclosure, range testing, and other zero-knowledge techniques, developers can facilitate minimization to enhance privacy in accordance with Allen's vision.

(x) *Protection* means that an independent censorship-resistant algorithm capable of authenticating user identities is essential. A self-sovereign identity system should strike a balance between transparency, fairness, and user support within the network while ensuring protection, as perfectly condensed in the GDPR.

Despite being applicable to the current SSI ecosystem, we know these principles may vary. Nonetheless, the overarching objective remains to enable individuals to be at the center of identity-related transactions. This entails managing multiple identifiers and personal information without relying on traditional centralized authorities,[734] but it does not mean that the entities responsible for issuing identity elements will lose their authority (privilege). Rather, individuals possessing multiple identifiers can present associated claims without relying on intermediaries.

4.2. SSI technical ecosystem

The SSI ecosystem presents three main roles: Issuer, Holder, and Verifier.

[734] E. Renieris, *SSI? What we really need is full data portability*, in *Women in Identity*, 2020, https://womeninidentity.org/2020/03/31/data-portability/.

The Issuer is a trusted entity, such as a government, bank, or educational institution, that creates and issues the Verifiable credentials. They also cryptographically sign the credential to guarantee its authenticity.

The Holder is the individual or organization that receives the Verifiable Credential from the issuer. Holders store their credentials in a secure digital wallet[735] and can share them with verifiers when needed to prove their identity or qualifications.

The Verifier is a person or organization that checks the authenticity and validity of a Verifiable Credential presented by the Holder.[736]

In this framework, the identity owner retains full control over their identity and its attributes and determines the type of identity data used to define them. It can therefore perform all operations related to their identity and personal data or delegate control to others. The identity owner can use their identity indefinitely and not be revoked or removed by anyone else.

SSI stands apart from previous identity models by employing new standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VC) based on Blockchain technology for creating cryptographically verifiable digital identities fully governed by their owners. Importantly, SSI differs from previous identity management technologies because it introduces DIDs, which are universally unique identifiers. The DID is a URL - a permanent, unique identifier with its own rules of syntax and

[735] These are general-purpose digital wallets that function much more like the real-world wallets we carry in our pockets or purses. Essentially, the wallet should have the capability to accept any standardized VC. The wallet should be installable on any of holder regularly used devices, similar to how holder can place your physical wallet in any chosen pocket or purse. However, unlike physical wallets, many holders would prefer their digital wallets to automatically synchronize across multiple devices, similar to how email and messaging apps keep messages in sync. Holder should be able to back up and transfer the contents of their wallet to other digital wallets as needed, even if they are from different vendors, just like how it is possible to move physical credentials from one physical wallet to another. Regardless of the specific wallet used, including different wallets from various vendors, holders should have a consistent and uniform experience. This consistency is crucial for ensuring the safe and secure usage of wallets. See A. Preukshat, D. Reed, *Self-Sovereign Identity*, 2021, p. 28.

[736] A. Mühle et al, *A survey on essential components of a self-sovereign identity*, 2018, available at https://arxiv.org/pdf/1807.06346.pdf.

processing– which relates a subject with a "decentralized identification document" (DID document). It completely differs from other ephemeral identifiers such as an IP address, a mobile number and a domain name. Public DIDs, along with selected public credentials, could be stored on the Blockchain (or off-chain) in the form of a DID document,[737] while private DIDs and confidential identity-related data are maintained in the identity owner's storage (e.g., digital wallet).

To understand what Verifiable Credentials are, it is first essential to define what a claim is. A claim represents an assertion related to any entity; a credential is a collection of claims used by entities to prove their identities. Verifiable Credentials (VCs) contains the DID of its subject (e.g., a bank customer), the attestation (e.g., KYC approval), and must be signed by the person or entity making the claim using the private key associated with the claim issuers DID.

Verifiable Credentials are like digital versions of the documents used by users every day, such as driver's licenses, passports, or school diplomas. It can be seen as a digital wallet containing user's important documents, which they can use to prove their identity or qualifications without carrying physical papers or cards.

Verifiable claims serve as mechanisms for trusted authorities, such as financial institutions, to issue certified credentials linked to specific DIDs securely. The control over DID claims remains in the hands of the DID subject, and these claims can be employed to verify a specific attribute of the DID subject independently, without relying on a certificate authority, identity provider, or centralized registry. Demonstrating that an individual or entity is indeed the subject of that particular DID (via a designated authentication method) grants them access privileges associated with these credentials.

[737] A DID document contains information about who the issuer is, the endpoints they use and the cryptographic keys they use (these documents are usually stored in a distributed ledger).

While DIDs are not inherently tied to Blockchain technology, they are intentionally designed to be compatible with any distributed ledger or Blockchain network. This compatibility arises from the fact that a DID can be associated with a specific private/public key pair used to validate identity claims. Consequently, linking this key pair (the one associated with the DID) with other key pairs utilized for signing financial transactions on a Blockchain becomes feasible.

As already emphasized, owing to the transparency and immutability inherent in Blockchain technology, personal information should never be directly stored on the Blockchain itself.[738] Nevertheless, a Blockchain can serve as a tool for monitoring permissions and access to personally identifiable data that is stored off-chain.

This approach establishes a traceable record of information access. Consequently, apart from the standardized DID methods, a Blockchain can also fulfil roles such as recording and potentially revoking claims or attestations, managing the granting and revocation of access to personal data repositories, and performing other functions that may be unique to a particular identity system. For instance, it can track claims submitted and resolved within a dispute resolution system dealing with false attestations.

With SSI, identity owners have control over their identity-related data, storing it in their own storage, which is typically a digital wallet. Credentials in the wallet are digitally signed and verifiable, allowing users to determine what information they share with other organizations. Users can share entire credentials, specific claims within a credential, or Zero-Knowledge Proofs (ZKPs) derived from a credential, which ensures encrypted and secure connections. Of course, the trust relationship between organizations and users is maintained through Blockchain technology since

[738] P. De Filippi, *The interplay between decentralization and privacy: the case of Blockchain technologies*, in *Journal of Peer Production*, 2016.

verifiers can verify the digital signatures on received credentials using the underlying Blockchain.

4.3. Assessing SSI compatibility with the Principles and Requirements of the GDPR

In our examination of the interplay between Blockchain and the European data protection framework in the previous chapter, we pointed out that the GDPR only applies when personal data is involved.

SSI is built upon Blockchain technology, which comes in various forms, differing in terms of technical design, governance structure, and complexity.

As a result, the compatibility between GDPR and Blockchain-based SSI can only be determined by assessing its underlying technical features. Therefore, our previous considerations regarding the challenges posed by some of the GDPR requirements still apply. For instance, one of the most significant issues revolves around the classification of data stored on a Blockchain, such as public keys and transactional data. This entails that it is not possible to draw a general conclusion on the compatibility or incompatibility of GDPR and SSI without considering the specific characteristics of a given SSI system. Nevertheless, both compatible and conflicting aspects of GDPR and SSI systems can be addressed. The intention is to highlight some peculiarities of the SSI in relation to the principles of the GDPR, so the general analysis in the previous chapter applies to anything not specified here.

Regarding the principle of lawfulness, it is important to consider that in an SSI system, the holder, typically the identity owner, possesses and exercises full control over their identity and its associated personal data. Consequently, any exchange or collection of personal data can only occur when the identity owner provides their consent, based on a lawful basis. When a holder has been granted (delegated) authority to manage another entity's or data subject's personal data, the authorized holder possesses the legal rights necessary to consent to the exchange or collection of personal data on behalf of the entity/data subject. This delegation ensures the protection of the entity's/data subject's interests and confidentiality.

The degree of fairness and transparency within this framework is contingent on the specific type of SSI system employed, which can enable users to oversee potential mishandling of personal data and stay informed about the entire processing process. Notwithstanding, these considerations should be challenged depending on the assumptions made regarding the classification of personal data in the Blockchain, as it is of pivotal importance in the SSI ecosystem.

In analyzing the compatibility of the principle of purpose with the characteristics of SSI systems, it should be recalled that Blockchain technology can be employed to monitor and manage consent interactions among the various roles within an SSI system. Yet, the precise articulation of the purpose relies on the type of SSI system in use and its accompanying data usage policy. Hence, it is essential that the data processing purpose is clearly defined, whether it is confined solely to transactions or encompasses all other related processing activities and potential new purposes. This aspect should not remain somewhat ambiguous, yet SSI systems should be fully aligned in this regard.

Going on with the principle of data minimization, it is important to consider that many SSI systems offer users the option to store their personal data off-chain, typically within their wallets, while conducting transactions through the Blockchain. Notwithstanding, we already emphasized two technical characteristics of Blockchain that do not comply with this principle: the Blockchain is engineered to ensure resilience through data replication across numerous locations and is an append-only ledger. However, we argue that SSI systems have the potential to substantially reduce the volume of personal data currently stored within organizational data silos. In an

SSI framework, personal data is ideally stored and controlled solely by the identity holder using wallet software. Organizations, such as companies, can make repeated requests for access to users' personal data and subsequently delete it after each use if necessary. In theory, this approach could minimize the personal data retained in organizations' databases to a minimal set of DIDs that would enable reidentification of users when required for subsequent interactions.

Regarding accountability, SSI systems that rely on permissioned blockchains and governance models may have the potential to enhance accountability. In such systems, competent authorities can implement necessary technical, procedural, and organizational measures to adhere to this principle. This approach could elevate the level of accountability and transparency in data and transaction management, providing audit trails and traceability features that assist organizations in demonstrating compliance with specific regulations.

As one can easily notice, there are conceptual similarities between the GDPR and SSI framework. Nonetheless, it's crucial to interpret this framework based on its practical implications and within the specific context of identity management systems.

5 The Regulatory Framework

5.1. The eIDAS Regulation

The eIDAS Regulation became fully effective[739] on 1st July 2016. It establishes a mandatory legal framework across Europe for digital identities and trust services and facilitates secure digital transactions between public administrations, companies, and citizens. The Regulation consists of two main components: digital identities and trust

[739] The Regulation entered into force on 17 September 2014 and applies from 1 July 2016 except for certain articles listed in Article 52.

services. Regarding identities, eIDAS primarily focuses on government-issued electronic identification schemes and identification means, setting requirements for the identity of natural and legal entities. Even though the Regulation allows for identification means issued by a notifying member state or independently recognized by that member state, member states issue the majority of identification means in practice.

5.1.1. The Notification Process

The eIDAS Regulation primarily addresses the notification of government identification schemes and core identity attributes such as name, surname, address, date of birth, and place of birth. Additional attributes like individual authorizations, rights of representation, diplomas, licenses, and others are not currently regulated or covered by the Regulation's technical standards. This lack of regulation limits their legal trustworthiness and interoperability, although these attributes can technically be added to digital identities.[740]

The notification process ensures mutual recognition, meaning that all European public administrations must accept any digital identity ("eID") that is notified. It also imposes reporting obligations for security breaches and places full liability on the notifying Member State, which fosters a high level of trust among private and business users, but this trust only applies to notified eIDs. Non-notified identification schemes and means are subject to national definitions of technical requirements, resulting in legal and technical interoperability limitations. It is important to note that the Member State is fully responsible and liable for its notified eID scheme and the associated

[740] J. Anke, T. Ehrlich, D. Richter, M. Meisel, *Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities*, pp. 247–270; U. Korte, S. Schwalm, T. Kusber, K. Shamburger, *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 2020, pp. 49-60; M. Kubach, C. Schunck, R. Sellung, H. Roßnagel, *Self-sovereign and decentralized identity as the future of identity management*, 2020, pp. 35-47.

means. The mentioned process includes a peer review of the proposed identification scheme by other Member States based on European standardization. Currently, the obligation to recognize notified eIDs only applies to public administrations when they require them for their public services, and it does not extend to private companies.

5.1.2. Not a Uniform Certification Process

Importantly, the eIDAS Regulation implicitly mentions private identification schemes or means, primarily in relation to the Level of Assurance (LoA) requirements.[741]

Although the Regulation includes the notification of government identification means under a specific Level of Assurance (LoA), it does not incorporate a formal European-wide certification process for identification means against defined LoA standards. The only certification mentioned in the Regulation is the module certification, as outlined in Article 24. This certification allows for auditing identification schemes against LoA substantial or higher. The process is however conducted at the national level, based on national norms and standards that align with the eIDAS Regulation, but it is also limited to qualified trust service providers issuing certificates without providing a general confirmation of LoA.

[741] Some Member States, such as Italy and Estonia, have notified private schemes; interestingly, these countries have the highest utilization of their notified eIDs. The levels of assurance, as defined in Article 8 of the eIDAS Regulation and 2015/1502 directive (Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) n. 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market), establishes specific security requirements for identity verification procedures. Digital service providers must recognize these levels of assurance to determine the necessary LoA for accessing their services. This assessment is typically based on risk management principles outlined in ISO 2700 (ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management), which involves evaluating potential threats, their impact, likelihood, and any relevant processes associated with the considered service. Therefore, the LoA determines which identification procedures can be utilized for a given digital service, and it is not exclusively dependent on notified eIDs but encompasses all identification procedures, including those that are not notified.

This situation creates varying certification requirements[742] across Member States.[743]As a result, there is competition among Member States regarding security and privacy requirements. Some Member States have established their own certification schemes to assess public or private identification schemes against LoA, even in cases where notification and Article 24 apply. These certification procedures are open to interested parties and may include confirmation processes.[744] Notwithstanding, the lack of a uniform certification process at the EU level creates a vulnerability within the eIDAS Regulation, limiting mutual recognition of such certifications and the interoperability of underlying identification procedures.

5.1.3. Qualified Trust Services

The eIDAS Regulation not only addresses digital identities but also defines (qualified) trust services, which include the following components:

(i) Creation of (qualified) certificates for (qualified) electronic signatures, seals, and/or timestamps.

(ii) Validation of (qualified) electronic signatures, seals, and/or timestamps.

(iii) (Qualified) Electronic registered delivery services.

[742] For instance, in Germany, the certification process for identification procedures, which is not based on the German eID card, such as video identification or self-identification, is significantly more challenging than in other Member States.

[743] This also seems hardly compatible with the nature of the instrument of regulation, which is to harmonize. The Explanatory Memorandum accompanying the Proposal for Regulation explained the reasons that are inherent to the peculiarities of the electronic identification mechanism within the framework of European competencies.: "It is therefore necessary for the EU to create an enabling framework to address cross-border interoperability and to improve the coordination of national supervision schemes. However, electronic identification cannot be addressed in the proposed Regulation in the same generic manner as the other trust electronic services because issuing means of identification is a national prerogative. The proposal therefore focuses strictly on cross-border aspects of electronic identification."

[744] These procedures enable the verification of LoA beyond notified eIDs and currently encompass various aspects such as mobile identities derived from a notified eID, automated identification, or BankID.

(iv) (Qualified) Preservation of (qualified) electronic signatures, seals, and/or timestamps.
(v) (Qualified) Website certificates.

Cryptographic electronic signatures or seals provide evidence of the authenticity and integrity of electronic records to third parties, while a (qualified) timestamp serves as valid proof of existence and evidence of the transaction's time. Successful validation and preservation are crucial in all cases. According to Article 27 of the eIDAS Regulation, any at least advanced signature, seal, or timestamp from a qualified trust service provider must be accepted and validated by any public administration.[745]

Article 24 of the eIDAS Regulation requires unique identification of individuals applying for a qualified certificate for qualified electronic signatures. The corresponding identification module must be certified by a conformity assessment body (CAB) before a qualified trust service provider can use it.

In this context, the possible identification procedures, aside from eID or qualified electronic signature, are defined nationally. This leads to significant differences between Member states and competition based on the lowest requirements.[746]

[745] A. Zaccaria, M. Schmidt-Kessel, R. Schulze, A. M Gambino (eds.), *EU eIDAS-Regulation: Article-by-Article Commentary*, London, Bloomsbury Publishing, 2020; U. Korte, S. Schwalm, T. Kusber, K. Shamburger (2020).

[746] As a practical consequence of this, in Germany, the requirements for alternative identification under Article 24(1)(b) are notably higher than in Austria or Nordic countries, resulting in a competitive disadvantage for German-qualified trust service providers.

Moreover, it is crucial to acknowledge that the eIDAS Regulation is supported[747] by mandatory Implementing Decisions.[748]

This overview highlighted that the current eIDAS Regulation operates on the premise of a centralized digital identity issued by or under the control of a Member State. It assumes the presence of a government trust anchor for each digital identity, necessitating a trustworthy third party to issue the eID. Therefore, digital identities without a government trust anchor are not covered by the eIDAS Regulation. However, this does not entail that Member States do not have control over every

[747] Regarding digital identities, it is important to mention the Implementing Decision 2015/1502, which defines the requirements for the Level of Assurance. In the context of trust services, the Implementing Decision 2015/1506 should not be forgotten, as it defines the mandatory signature formats for mutual recognition according to Article 27 of the eIDAS Regulation. See Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) n. 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for electronic transactions in the Internal Market.

[748] Implementing decisions find their legal basis in Article 291 of the Treaty on the Functioning of the European Union (TFEU). These legally binding acts of the European Union apply directly to all Member States of the EU. Implementing decisions can be specific to certain legal entities, binding them only to those entities. The EU employs two procedures for establishing Implementing Decisions. In both procedures, the Commission initiates and ultimately decides on Implementing Decisions. A committee composed of representatives from Member States either provides advice or must approve the implementing decisions. Implementing decisions have a limited scope and aim to ensure consistent implementation of European legislation and their purpose is solely to facilitate uniform implementation across Member States. Implementing decisions are directly applicable and do not require national legislation for transposition. This guarantees a similar implementation process in each Member State. In the event of a contradiction between national legislation and Implementing Decisions, the latter takes precedence. These acts are only issued when European legislation deems further measures necessary to ensure proper and often uniform implementation by Member States. The mandate of Implementing Decisions is restricted to what is necessary for implementation and does not encompass additional or complementary rules. They indeed focus on specific issues, often address technical details of legislation and frequently target particular legal entities. Legal entities directly affected by an Implementing decision have the right to challenge it in a court of law, both against a state and other legal entity. See P.J. Loewenthal, *Article 291 TFEU*, in M. Kellerbauer et al, *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, 2019, pp. 1925-1932.

transaction conducted by the owner of the eID. On the contrary, the notifying Member State is responsible for ensuring a government trust anchor.

Besides implementing acts, the eIDAS Regulation is supported by a standardized technical framework established by the European standardization organizations ETSI and CEN, mandated by the European Commission, which we have already mentioned in Chapter II. This framework promotes the interoperability of eID and trust services across Europe. For eID, it builds upon outcomes from the STORK project and relies on eIDAS nodes and the eIDAS minimal data set. Regarding trust services, it incorporates ETSI standards on qualified trust service providers (QTSPs) and their devices.[749]

In addition to the requirement for mutual recognition, the utilization of notified identification schemes and the corresponding identification means is determined by individual Member States. These established conditions ensure the identity provider's secure utilization of core identity data of natural entities, with a particular emphasis on restricting the data's use solely for identification within the specified service. This approach guarantees that no Identity Provider (IDP) has comprehensive knowledge of where users intend to use their eID.

eIDAS has established a trusted framework across the EU, built upon trust chains involving each entity acting as a reliable third party. This means, as demonstrated in the context of digital identities, that eIDAS consistently requires a trustworthy third party. Trust within eIDAS is established based on European law, overseen by European and national supervisory bodies, accredited conformity assessment bodies adhering to European standards, and trust service certification by Conformity Assessment Bodies (CABs) under the supervision of national supervisory bodies. This trust framework is verifiable through European-wide trusted lists, ensuring a

[749] U. Korte et al (2020).

democratic underpinning of the law, mutual oversight, certification, and transparent verifiability.[750]

It is important to note that this trust chain also encompasses the principle that any Qualified Trust Service Provider (QTSP) bears full liability for its actions.[751] Similarly, the CAB assumes liability for its conformity assessments, and the Accreditation body is responsible for accreditation, thus substantially limiting the liability risk for users of QTSPs.

5.2. Main Amendments in the Proposed eIDAS 2.0

Before delving into the proposed amendments of the eIDAS Regulation, a clarification of the terminology used is deemed necessary. A detailed analysis of all new changes would go beyond the scope of this thesis; hence, we will focus only on those most relevant for the implications to SSI systems.

When we defined the main technical characteristics of Blockchain technology, we maintained that therein set of data or transactions are bundled in sequential linked blocks to which this name is owned. The blocks also include the previous block's hash and build the mentioned hash protection and a so-called "timestamp".

The Blockchain-based "timestamp" and "signatures" need to be distinguished from the timestamps defined in eIDAS and related standards. This distinction arises due to several factors. Firstly, the lack of a trustworthy source of time in Blockchain-based timestamps. Secondly, the absence of a trust service provider's creation and validation of digital signatures. Lastly, the absence of a third party-generated Proof of Existence, with the Blockchain system itself being responsible for this function.[752]

[750] *Ibidem.*

[751] Cfr. Art. 13 of eIDAS Regulation.

[752] The integrity protection of each block in DLT is achieved through the use of Merkle trees. Cfr. U. Korte et al (2020).

The main legal changes in eIDAS 2.0 concern electronic identification. The proposal introduces certain obligations and requirements for Member States regarding identification schemes. According to Article 6a, each Member State must notify at least one identification scheme within 12 months of the Regulation's applicability. The European Commission is responsible for publishing mandatory implementing acts referencing European technical standardization within 6 months of the new regulation's publication.

Compared to eIDAS 1.0, the new regulation emphasizes the notification of at least one identity scheme from each Member state.[753] This notification is a prerequisite for the mutual recognition of identity and represents a significant step toward broader utilization of eID in Europe. Furthermore, any notified eID scheme must facilitate unique identification with the proposed EU Digital Wallet.[754]

In addition to government eID schemes, the new eIDAS proposal also introduces private identification schemes and allows for national certification based on different levels of assurance.[755]

In this regard, in our opinion, the most significant change in eIDAS 2.0 is the requirement for every Member State to offer an EU-Digital Wallet to its citizens. The EU-Digital Wallet can be published by, under the authority of, or recognized by the Member state. This opens up the possibility for private wallets under the recognition of a Member State. The EU-Digital Wallet will encompass the core identity information currently covered by government eIDs and additional attributes or verifiable credentials based on W3C standards.[756] This means that eIDAS 2.0 aligns closely with

[753] Article 10 and subsequent articles.

[754] Cfr. Article 11a.

[755] Cfr. Article 12a. The certification scheme is expected to comply with the EU Cybersecurity Act and be conducted by dedicated Conformity Assessment Bodies transparently listed by the European Commission. However, the current proposal does not specify an implementing act, which creates a risk of varying national interpretations and standards for the Cybersecurity Act. This could potentially lead to competition among member states and identity providers regarding certification requirements.

[756] "Web standards are the building blocks of the web. They are the blue prints of how to implement browsers, blogs, graphic editors, search engines, and many more software that power our experience

the Self-Sovereign Identity triangle. Each citizen becomes the holder of an EU-Digital Wallet and has control over releasing their identity information to the desired parties. The wallet consolidates the attributes, but it's important to note that core identities, such as the government eID, will typically be stored on secure hardware like a secure element or e-SIM. Only the attributes will be stored in the wallet as a software component. The EU Digital Wallet is meant to also support the creation of (qualified) electronic signatures. The EU-Digital Wallet's technical details and security requirements will be defined through ongoing European Standardization efforts at ETSI and CEN.

In line with the guidance on the SSI triangle, eIDAS 2.0 Regulation includes requirements for the verifier (relying party) in Article 6b. Verifiers are obligated to notify their operations and comply with European standards, which will be specified in mandatory implementing acts. Conformity assessment bodies will assess compliance with these standards. However, the proposal for eIDAS 2.0 stipulates that certification requirements, including strong authentication for verifiers, are defined at the national level. This approach carries the risk of potential competition based on the lowest standards, which could result in privacy risks for identity holders.

Similar to the dedicated requirements for the EU-Digital Wallet, qualified attestation services, and identification schemes, eIDAS 2.0 also imposes specific obligations for the acceptance of the wallet. It mandates that public services, entities in critical infrastructure sectors (such as finance, utilities, healthcare, etc.), and major internet companies are required to accept the EU-Digital Wallet.[757]

In conjunction with the EU-Digital Wallet, eIDAS 2.0 introduces qualified attestation services according to Articles 45a-e. Qualified attestation services assume the full risk of liability, as do all qualified trust service providers (QTSPs), according

on the web. They enable developers to build rich interactive experiences that can be available on any device.", https://www.w3.org/standards/about/.

[757] Article 12b.

to Article 13. This means that eIDAS significantly limits the risk for users, a principle that carries over to eIDAS 2.0. Only qualified trust service providers offering such attestation services will have access to the EU-Digital Wallet.

Therefore, recognizing the close relationship between qualified attestation services and the wallet, eIDAS 2.0 mandates implementing acts that refer to European Standards for both the wallet and attestation service. Thus, only qualified attestation service providers can issue credentials to the EU-Digital Wallet and, as a result, eIDAS 2.0 intertwines digital identity means and (qualified) trust services, as they mutually influence each other.

5.2.1. Is there Room for Blockchain?

For our analysis, the proposed Regulation is particularly interesting for the observations formulated regarding electronic ledgers, which align with the proposal presented in the SSI eIDAS Legal Report developed under EBSI[758] V2.0.[759] The memorandum accompanying the proposed eIDAS 2.0[760] acknowledges the necessity of establishing a legal framework for electronic ledgers. It highlights that electronic ledgers offer users proof and an unalterable audit trail for transaction sequencing and data records, thereby safeguarding data integrity. The memorandum also mentions various use cases for electronic ledgers, including their utility in data sharing from decentralized sources, self-sovereign identity solutions, and the attribution of ownership in digital assets.[761]

[758] For many details about what EBSI is and its mission, refer to para 5 of Chapter I.

[759] It is the report prepared in the context of the European Blockchain Services Infrastructure building block, https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf.

[760] Explanatory memorandum, 3 June 2021, COM(2021) 281 final, 2021/0136(COD), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN.

[761] Electronic ledgers provide users with proof and an immutable audit trail for the sequencing of transactions and data records, safeguarding data integrity. While this trust service was not part of the impact assessment, it builds upon existing trust services as it combines time stamping of data and their sequencing with certainty about the data originator, which is similar to e-signing. This trust service is

The proposal of eIDAS 2.0 recognizes the importance of establishing a unified pan-European framework to enable cross-border recognition of trust services that support the operation of electronic ledgers, particularly relevant when using Blockchain in order to prevent fragmentation and ensure interoperability.

Although there have been prior attempts in various countries[762] to regulate DLTs, which is worth recalling is the genus of which Blockchain is the species, the merit of the eIDAS 2.0 proposal is to present a comprehensive vision with a neutral approach encompassing both centralized and decentralized solutions.

The proposed eIDAS 2.0 Regulation aims to address the challenges hindering the deployment of SSI and Blockchain solutions, particularly regarding their recognition as legal evidence and the transfer of legal responsibility. Regulating these technologies as trust services and establishing corresponding legal presumptions may facilitate their adoption. Article 45h of the Proposal[763] affirms the legal effects of electronic ledgers, stating that an electronic ledger should not be denied legal effect or admissibility as evidence in court solely because it is in electronic form or does not

necessary to prevent fragmentation of the internal market, by defining a single pan-European framework that enables the cross-border recognition of trust services supporting the operation of qualified electronic ledgers. Data integrity, in turn, is very important for the pooling of data from decentralized sources, for self-sovereign identity solutions, for attributing ownership to digital assets, for recording business processes to audit compliance with sustainability criteria and for various use cases in capital markets.

[762] For example, Italy's Decree-Law 135/2018 (validated by Law 12/2019). Article 8-ter provided a definition for smart contracts and DLT but did not specify any other particular implications or effects. Instead, it tasked the Agency for Digital Italy (AgID) with the responsibility to formulate a regulation that would implement this definition, establish the specific standards that DLTs must adhere to in order to function as electronic timestamps, and outline the identification process that smart contracts should follow to be covered by Article 8-ter of Law Decree No. 135. As of the present moment, AgID has not yet issued such a regulation.

[763] "Article 45h, Legal effects of electronic ledgers:

1. An electronic ledger shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.

2. A qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger."

meet the requirements of qualified electronic ledgers (the so-called non-discrimination principle). In this regard, a qualified electronic ledger enjoys the presumption of uniqueness and authenticity of the data, accuracy of its date and time, and sequential chronological order within the ledger. Regardless of its nature, any electronic ledger will benefit from this.

As mentioned, eIDAS 2.0 adopts a technology-neutral approach. It does not require a specific infrastructure for (qualified) attestations, identification schemes, or identification methods. At the same time, we already clarified at the beginning of this chapter that the implementation of SSI does not necessarily mandate the use of Blockchain or DLT. SSI primarily focuses on identity and access management, where individuals control which parts of their identity information they share. They can selectively disclose only the necessary information or use Zero Knowledge Proofs to prove specific identity statements (e.g., age verification, valid driver's license) without revealing underlying data.

Technically, SSI can be achieved without DLT, as attestations can be created within a centralized Public Key Infrastructure (PKI). In such cases, a centralized authority, such as a qualified attestation service, issues attestations based on trusted sources typically provided by Member States. However, in our opinion, certain SSI proposals, such as the one involving DIDs and VCs, have the merit of leveraging Blockchain functionalities.

Many of the challenges[764] that Blockchain poses for the European Data Protection Framework also recur for SSI, therefore highlighting the need for further development and compliance with privacy and data protection regulations.

[764] For instance, Blockchain lacks a clear and legally compliant identification mechanism for network participants and a robust means of providing unique evidence for transaction authenticity and integrity. Moreover, the immutability of Blockchain, by design, contradicts privacy laws like the GDPR, which grants individuals rights such as the right to erasure and the right to correction. Additionally,

5.2.2. Criticism and Open Questions

Although eIDAS 2.0 has yet to be approved,[765] we are aware that this Regulation will considerably impact the digital identity industry and the adoption of related technologies, including Blockchain.

The proposed Regulation introducing tamper-proof electronic ledgers for immutable audit trails based on decentralized databases has raised several criticisms from different actors. On the contrary, we welcome this innovation since we believe that Blockchain, and thus to use eIDAS terminology, electronic ledgers are cutting-edge solutions for Self-sovereign identity that can effectively support and transform public services by contributing to data integrity and providing citizens access to previously shared, technically immutable data. The Commission motivates this novelty as: "data integrity, in turn, is crucial for the pooling of data from decentralized sources, for self-sovereign identity solutions, for attributing ownership to digital assets, for recording business processes to audit compliance with sustainability criteria, and for various use cases in capital markets." Furthermore, another of the primary objectives of integrating electronic ledgers into the identity ecosystem is to prevent fragmentation in the internal market, as this allows for more decentralized governance through multi-party cooperation. This combination of data timestamping, sequencing, and knowledge of data originators enables various benefits, such as flexible electricity markets, protection of intellectual property rights, and reliable audit trails for the provenance of commodities in cross-border trade.

The Proposal also addresses the dominance of large web platforms like Google and Meta by promoting the inclusion of small and medium-sized businesses in identity

the lack of standards for interoperable data exchange of on-chain data limits the right to data portability as outlined in the GDPR.

[765] The Parliament's position in 1st reading is still awaiting; however, the Proposal is included in the list of the legislative priorities within the Joint Declaration 2023-24, https://oeil.secure.europarl.europa.eu/oeil/popups/thematicnote.do?id=41380&l=en (update at October 2023).

management. This inclusion probably represents a response to the significant centralization of digital means.

The above is not shared by the European Data Protection Supervisor (EDPS),[766] which released formal comments on the eIDAS 2.0 plan in July 2021. The EDPS highlighted that although Blockchain technology in the Proposal is intended as one of the implementing technologies for the newly introduced trust services, the European Digital Identity Wallet does not require it to offer consumers enhanced transparency regarding which data to share, with whom, and for what purposes. In addition, the EDPS recalled that the use of Blockchain technology raises several GDPR-related concerns, such as the inability to delete or update records on a Blockchain.

While we agree that, generally speaking, the relationship between Blockchain and GDPR raises compliance issues, we believe that what the EDPS points out supports our thesis of the need to assess the applicability of the GDPR on a case-by-case basis. "(…) [T]he use of Blockchain technology may not be appropriate for all possible use cases and may require additional safeguards."[767] As our research tried to show, Blockchain is not GDPR-compliant per se but depends on the specific use case. Therefore, we do not entirely understand why such statements led to such harsh reactions,[768] as will be explained below.

The Council of Bars and Law Societies of Europe disagreed with the eIDAS trust services strategy, suggesting that it creates unnecessary conflict between the planned pan-European sectoral approach and the market-driven, globally available electronic ledger alternatives. Additionally, it cautioned against delegating everything to the

[766] https://edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf.

[767] *Ibidem*, p. 3.

[768] It is interesting to note that in the speech entitled "European Standardisation in support of the EU cybersecurity legislation" that EDPS gave at the Cybersecurity Standardisation Conference 2023 no mention was made of electronic ledgers and Blockchain, 7 February 2023, https://edps.europa.eu/system/files/2023-02/23-02-07_ww-enisa_en_2.pdf.

Commission's implementing acts[769] and ETSI/CEN, as this might disproportionately benefit a small number of established service providers in standardization organizations without clear knowledge of the intended impacts.[770]

In response to these comments, the ITRE Committee of the Parliament approved a revised version of the eIDAS 2.0 proposal on February 9th, 2023, excluding Section 11 on Electronic Ledgers as a Regulated Trust Service.[771]

This adjustment was likely made to realign the Proposal with the necessary technological neutrality, which, in our view, was not threatened by the previous wording, as rightly maintained by INATBA and numerous Blockchain foundations and companies which recently jointly published an open letter[772] advocating for the retention of the electronic ledger provisions in eIDAS 2.0. The letter argues that electronic ledgers are sometimes misconceived as a technology that relies on a specific energy-intensive consumption. In contrast, as defined in Section 11, electronic ledgers represent a technology-agnostic definition of a new type of trust service that offers a

[769] The Proposal provides for 28 Implementing Acts, which may cause too much freedom in their implementation.

[770] “The definition of electronic ledger is very wide, and thus, it is important to restrict to what the e-ID proposal is trying to address. Electronic ledgers can be both permissioned and permissionless, and any regulator can designate (permissioned) "special electronic ledgers" with special power entrusted on them by the EU institutions. The e-ID proposal tries to do this for unclear reasons in Article 45h-45i, and gives a presumption of "uniqueness and authenticity of data" such special ledgers will contain. These ledgers may be created only by qualified trust service providers specifically entitled to do so (special nodes of the special ledger).”; “In this regard, the CCBE considers that the eIDAS trust services approach is not an appropriate approach, and creates unnecessary tension between currently existing, market based, bottom-up, global electronic ledger solutions and the foreseen pan-EU-sectoral approach. The volatile market of global electronic ledgers may see such a regulatory approach as another attempt to isolate certain parts of a technically global infrastructure by way of regulation.
If there is indeed a clear need for such a regulation, it should be adopted at the sectoral level for a specific purpose or use case, explaining why only "special nodes" can operate that particular ledger and decentralised application, or why that particular regulation is necessary (such as for issuing crypto-assets to the public). However, none of the documents underlying the e-ID proposal and the Report explains in any way that such a generic regulation of electronic ledgers nodes is necessary.” https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20220401_CCBE-position-paper-on-the-e-ID-proposal.pdf.

[771] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf.

[772] https://inatba.org/news/savesection11-eidas2-trusted-electronic-ledgers-open-letter/.

series of digital data records while ensuring the accuracy and integrity of their chronological order. However, the letter also highlighted that if electronic ledgers are excluded from the eIDAS 2.0 proposal, they will remain unregulated because they differ from electronic signatures, seals, or timestamps trust services. Ultimately, the letter emphasizes that electronic ledgers play a crucial role in establishing resilient digital infrastructures that can withstand cyberattacks, benefiting European businesses and consumers. They are also important in relation to multiple initiatives, such as the prototypical implementation of diploma use case by EBSI.[773]

6. (Intermediate) Conclusive Remarks

This chapter intended to present one of the most interesting use cases of Blockchain, the Self-sovereign identity, which is the one created and managed by each person individually, without the intervention of third parties. SSI represents a significant shift in the realm of identity management, going beyond merely placing users at the center of the identity process. As explained by Allen, "rather than just advocating that user be at the center of the identity process, self-sovereign identity requires that users be the rulers of their own identity". [774]

SSI is grounded in the principle that individuals possess the inherent right to an identity that stands independently, free from reliance on third-party identity providers like governmental entities or centralized authorities.

Research on Blockchain-based identity has been evolving in recent years but remains in its early stages of development.[775] Some authors discussed how specific privacy-preserving techniques, such as the ones presented in the previous chapter,

[773] https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home.

[774] C. Allen (2016).

[775] Y. Liu, D. He, M.S. Obaidat, N. Kumar, M.K. Khan, K.K.R. Choo, *Blockchain-based identity management systems: a review*, in *Journal of Network and Computer Applications*, 2020, pp. 1-11.

could be integrated into SSI models for Blockchain-based applications.[776] Other authors[777] reviewed Blockchain-based identity management systems, assessing them from three perspectives: compliance and liability, end-user experience, and technological implementation, integration, and operational criteria. The evaluation revealed that most current Blockchain-based identity management systems lack standard-compliant interfaces.

We believe that to make SSI a reality, it necessitates the development of technical standards and adjustments in socio-political landscapes, often requiring legal modifications. SSI is realized as identity management systems closely related to Blockchain technology yet not entirely dependent on it. Therefore, the SSI ecosystem also suffers from the uncertainties and regulatory gap that characterize the current discussion around Blockchain in general. This means that the existing lack of clear guidance on which data components of the SSI constitute personal data, how the GDPR applies, and who is considered a controller creates a burden on the use of this privacy-enhancing technology. With further clarifications, SSI can provide a high standard of privacy protection as it can technically protect the privacy of data subjects being at the same time compliant with GDPR.

SSI is not a buzzword, but it represents a new paradigm for digital identities. This does not mean that there is *just one way* to create digital identities, it means that it is possible to build new ways based on existing tools, as the previous analysis showed. Technology alone cannot create a new paradigm since the establishment depends on

[776] J.B. Bernabe, J.L. Canovas, J.L. Hernandez-Ramos, R.T. Moreno, A. Skarmeta, *Privacy-preserving solutions for Blockchain: review and challenges*, in *IEEE Access*, 2019, pp. 164908-164940.

[777] M. Kuperberg, *Blockchain-based identity management: a survey from the enterprise and ecosystem perspective*, in *IEEE Transaction on Engineering Management*, 2020, pp. 1008-1027.

the user's acceptance, which at the same time requires awareness fostered by legal and technical certainty.

Undoubtedly, future solutions in this domain will need to consider a dual perspective, encompassing both normative and technological aspects. To establish legal certainty, it is pivotal to consider data protection authorities' interpretations and official stances regarding the technological tools and methods employed in decentralized identities.

Furthermore, a critical element in risk assessment and management is the collaboration between technology experts and legal professionals right from the inception of such projects. This techno-legal cooperation should be recognized as playing a significant role in shaping the future of decentralized identity systems and creating an effective and practical framework.

Conclusions

"Technology without the wisdom of law and ethics can be a dangerous tool; however, law without the sophistication of technology can be an ineffectual one."

Amit Ray

1.The Research Key Findings – **1.1.** *Can* Blockchain be subject to legal oversight? If yes, *should* it? – **1.2.** Should conventional legal systems be modified to accommodate the new paradigm of Blockchain technology, or should a technical legal framework be established to address its unique characteristics? – **1.3.** What are the key characteristics and technical foundations of Blockchain technology that impact personal data protection, and how can they be addressed effectively? – **1.4.** What role can privacy-enhancing protocols play in mitigating privacy concerns within Blockchain ecosystems? – **1.5.** Can Blockchain be considered a tool to achieve GDPR's objectives? – **1.6.** Can Blockchain-based self-sovereign identity (SSI) enhance data protection rights? – **2.** Research contributions – *a) Regulatory Guidance and Interpretative Frameworks – b) Emphasis on Privacy-by-Design - c) Enforcement of User Control – d) Contextual Compliance* – e) *Establishment of a Techno-Legal Framework*

1. The Research Key Findings

The European Union has positioned itself as a leader in emerging technologies, bringing about technological, economic and normative challenges addressing more than just the issue of developing appropriate technology, business models, and use cases, which also involves the respect of public policy objectives.

The term "Blockchain" has become synonymous with broader technological change and innovation and is accompanied by a narrative that captures the collective imagination regarding the profound impact of technological change on humankind. The immaturity of the technology, combined with a seemingly infinite array of potential use cases, opens up numerous future scenarios for utilising blockchains, as the previous pages showed.

Against this background, the analysis embarked on a comprehensive journey to establish a techno-legal framework for Blockchain technology in relation to EU data protection law.

The research navigated through the intricate Blockchain landscape, with its transformative potential and inherent challenges, and scrutinized European data protection laws, chiefly anchored by the GDPR.

This study sought to unravel the compatibility between Blockchain and the Regulation, highlighting these two domains' mutual influence and interdependence through rigorous analysis and examination, shedding light on areas of contention, potential conflict, and novel approaches and exploring their dynamic relationships, the impact of technological advancements on legal principles and frameworks, and the role of law in shaping and governing technology.

The analysis of the technical feature of Blockchain technology led to emphasizing its decentralized nature, cryptographic security, immutability, and potential to disrupt various sectors.[778]

The overarching questions that fuelled this research were whether the GDPR provides a suitable framework for Blockchain-based solutions and whether the Blockchain can be seen as a Privacy Enhancing Technology.

As presented in the Introduction, a set of specific questions guided the discussion and will, therefore, be reviewed individually in this concluding chapter.

[778] Chapter I has been entirely dedicated to presenting Blockchain from the informatics perspective.

1.1. *Can* Blockchain Be Subject to Legal Oversight? If Yes, *Should* It?[779]

Regulating Blockchain involves various demands and scenarios, both online and offline, making it challenging to include them within a single all-encompassing definition. The questions of whether Blockchain can be subject to legal oversight and, if yes, whether it should it, stem from the assertions that blockchains could be immune to regulation due to their decentralized and distributed structure and the essential role of encryption in its functioning.

Like the Internet, Blockchain evokes utopian and dystopian visions, as its emergence has sparked new ways of thinking about technology and its impact on our lives. In this regard, this thesis refused the idea of *'alegality'* of Blockchain and the cyberlibertarian narrative surrounding this topic. To counter these, parallels were drawn to early debates on Internet regulation, emphasizing the existence of centralized access points that enable regulatory intervention within the decentralized network.

1.2. Should Conventional Legal Systems Be Modified to Accommodate the New Paradigm of Blockchain Technology, or Should a Technical Legal Framework Be Established to Address its Unique Characteristics?[780]

After ruling out that Blockchain technology is immune to the law, the discussion turned to whether conventional legal systems should apply to the new Blockchain paradigm or whether a technical legal framework should be established to address the technology's unique characteristics.

By reflecting on the intricate interaction between law, technology, and innovation, this research emphasized the need for appropriate regulation and argued that, as the

[779] Paragraphs 1-3 of chapter II focused on this theme.

[780] Chapter II, paragraphs 4-6 addressed this issue, please refer to them for more details.

technology evolves, so should the law. This led to the claim that regulating Blockchain should be addressed according to the multistakeholder approach, aiming to reconcile the established benefits of public policy protection with the regulatory opportunities presented by technology.

Retracing the debates regarding the governance of these technological innovations designed to replace trust in human beings cast light on the importance of Blockchain governance and the connections between internal and external regulatory processes.[781] According to this vision, these elements can collectively contribute to delineating a techno-legal framework that includes requirements incorporating appropriate standards - the character of which ought to be determined collectively by all stakeholders - and tackling the societal and economic dimensions of regulation while ensuring the protection of fundamental rights.

In this context, the interoperability and standardization of distributed ledgers still remain ongoing challenges. The establishment of shared protocols and frameworks holds the potential to facilitate seamless integration and cooperation among diverse systems, ultimately enabling cross-border transactions and promoting the scalability and adoption of Blockchain technology. In other words, standardization could play a significant role in ensuring security and privacy in Blockchain systems. These standards encompass various aspects, including cryptographic algorithms, key management, and identity verification, all contributing to the establishment of robust security practices within Blockchain networks. Similarly, privacy standards address data protection, anonymity, and confidentiality concerns within the Blockchain ecosystem, striving to strike a delicate balance between the transparency and immutability of Blockchain and the imperative of safeguarding sensitive information.

[781] Chapter II also explored Blockchain technology's legal and governance aspects, thus revealing several tensions. In particular, by examining the technology's essential technical components and characteristics, the thesis demonstrated that while Blockchain possesses significant innovative potential, its practical effectiveness depends on both endogenous and exogenous rules and principles.

Efforts in standardization extend their scope beyond technical aspects and encompass legal, regulatory, and governance dimensions. Legal and regulatory standards are crucial in addressing compliance prerequisites, delineating liability frameworks, and setting forth guidelines for Blockchain-based transactions and contracts. These standards serve to ensure that Blockchain technology operates harmoniously within the borders of existing legal frameworks, thereby bestowing clarity and legal assurance upon all participants involved. Additionally, governance standards are oriented towards instituting transparent decision-making processes and consensus mechanisms within Blockchain communities' network governance structures. These standards are pivotal in facilitating the efficient administration and coordination of decentralized networks, ultimately nurturing trust and collaboration among participants. By establishing common frameworks and protocols, standardization efforts promote collaboration, trust, and innovation while effectively addressing challenges and ensuring Blockchain technology's responsible and seamless implementation.

Dispelled doubts about the possibility - at least theoretical - of regulating Blockchain, the thesis argued that Blockchain could act as a regulatory agent capable of governing humans and machines. This recognition positions the technology as part of the broader trend towards increased automation of law, uncovering associated promises and drawbacks. Blockchain can indeed be employed to incorporate and enforce legal provisions within the code, regardless of the existence of underlying legal rules. However, Blockchain technology cannot function as a standalone regulatory system disconnected from the relevant legal frameworks of a jurisdiction. Instead, decentralized systems should align and adhere to the existing laws and regulations governing their jurisdiction.

As claimed in the specific section,[782] in this context, fundamental rights might serve as both a limitation to the adoption of Blockchain technology and a driver for their protection through the technology itself. The discussion around this topic must involve the interrelationship between technological advancements and the protection of fundamental rights. Engaging in interdisciplinary research and fostering multi-stakeholder dialogues is crucial to ensure that these future configurations align with and promote legal and public policy objectives rather than undermining them.

1.3. What Are the Blockchain Technology's Key Characteristics and Technical Foundations That Impact Personal Data Protection, and How Can They Be Addressed Effectively?[783]

Gaining insight into the regulatory challenges posed by Blockchain technology served as a foundational step to delve into the core of this research: (i) untangling the intricate relationship between blockchains and the European data protection framework, of which the GDPR serves as the flagship legislative act and (ii) scrutinizing what key characteristics and technical foundations of Blockchain technology could impact personal data protection and how they can be addressed effectively.

Starting from the assertion that, at first glance, some provisions of the GDPR appear ontologically incompatible with the core characteristics of Blockchain technology and that Blockchain's immutability and decentralized nature raised issues in identifying data controllers and in ensuring data subjects' rights, this thesis showed that margins of mutual adaptation exist, thus reconciling (some of) the (arguable) contradictions arising from the application of this technology.

[782] See Chapter III, para 5.

[783] Chapter III has been entirely dedicated to answering to those questions.

To achieve that conclusion, the research built its arguments on the concept that the Regulation is technologically neutral and that to avoid being hindered by the "law lag",[784] the GDPR provisions should not be narrowly interpreted; on the contrary, regulatory flexibility becomes crucial to depict the law in a way that accommodates new technologies and supports data protection adequately.

Moreover, another theme endorsing this thesis is that, in evaluating Blockchain's compliance with the Regulation, it is imperative to acknowledge that this technology cannot be inherently categorized as GDPR-compliant or non-compliant. Instead, its compliance hinges on the specific use of the technology that is made. This implies that rather than directly applying concepts and rules designed for centralized systems to decentralized environments, it is crucial to grasp the unique characteristics of this novel technology to ensure the practical application of data protection principles.

This thesis concluded that achieving compliance between Blockchain technology and the GDPR necessitates a nuanced, case-by-case assessment since tailored legal remedies are required for each situation. The research posited that Blockchain could be leveraged to enhance data protection by ensuring transparency, integrity, and security, effectively serving as a privacy-enhancing technology.

An example addressed in the thesis and considered paradigmatic is that of the right to be forgotten, which can be subject to varied interpretations due to differing definitions of "erasure." Therefore, this would entail regulators or Data Protection Authorities (DPAs) taking the initiative and providing interpretative guidance to address these potentially debatable issues. Such supervision would help clarify and consistently apply GDPR rights and principles in Blockchain contexts. However, it is reported that there is a real lack of guidance on the topic, for instance, from the EDPB, whose guidelines on Blockchain have been awaited in vain for years.[785]

[784] This term describes the inadequacy of existing legal provisions to address social, cultural, or commercial contexts created by rapid information and communication technology advancements.
[785] See Chapter III, para 4.3.

In any case, only an oriented interpretation of the provisions of the GDPR cannot be decisive if technology continues to move in the opposite direction and if the data protection principles, 'privacy by design' above all, are not embedded in Blockchain use cases.

The topic of the interplay between Blockchain and the GDPR is associated with considerable trade-offs. Indeed, while the research revealed that Blockchain technology could significantly challenge existing legal frameworks and their underlying technical and economic assumptions, such as with the GDPR, it also highlighted that this technology could represent a technical solution in areas where the law currently falls short in achieving desired normative objectives. For example, in supply chain management, distributed ledgers can enable end-to-end traceability, ensuring the authenticity and provenance of goods.[786] This can help combat issues like counterfeit products and unethical practices. Additionally, distributed ledgers can provide secure and tamper-proof records in land registries, reducing the risk of fraud and disputes.

1.4. What Role Can Privacy-Enhancing Protocols Play in Mitigating Privacy Concerns within Blockchain Ecosystems?[787]

A substantial section of this thesis has been dedicated to illustrating some of the most interesting and widely recognized privacy-enhancing techniques that aim at protecting user privacy by reducing the identifiability of data. In examining these

[786] Distributed ledgers can facilitate the implementation of smart contracts, which can streamline processes, reduce transaction costs, and minimize the need for intermediaries. They can increase efficiency and trust in financial transactions, intellectual property rights management, and decentralized autonomous organizations.

[787] Paragraph 6 of chapter III entirely focused on describing some privacy-enhancing techniques with the aim of applying them to the Blockchain environment. The methods described are homomorphic encryption, zero-knowledge proof, secure multi-party computation, ring signatures, differential privacy and other technical approaches, like one-time keys and adding noise to data.

techniques within the Blockchain context, we described their implementation and feasibility, also emphasizing that they present possible drawbacks, such as decreased data utility and increased processing overhead. In other words, these techniques can reduce the uniqueness and usefulness of the data and impact their utility and quality for analysis, research, or business purposes. Moreover, they can be resource-intensive, increasing computation time, storage requirements, and network overhead and thus undermining the effectiveness of the entire network.

Regardless of the techniques implemented, it is essential to consider them from the beginning of the development cycle, i.e., they are recommended as privacy-by-design solutions that should be embedded into the design and development process.

Although the study considered the possibility to encounter practical difficulties, it argued that this should be the path for creating an effective techno-legal framework that can enhance the potential of Blockchain technology while ensuring compliance with regulations.

1.5.Can Blockchain Be Considered a Tool to Achieve GDPR's Objectives?[788]

The discourse around privacy-enhancing techniques helps address another essential element in the design of a techno-legal framework for Blockchain. Exploring these techniques has indeed outlined that the value of the right to data protection lies in promoting informational self-determination and individual personality rights and that Blockchain can potentially contribute to respecting some of the requirements of the GDPR and achieving its objective, that is, giving back control to data subjects.

[788] This question is not answered in a specific chapter or paragraph of the thesis but is the *leitmotiv* of the entire research project because it is from the affirmative answer to this question that the considerations relating to the possibility of creating a techno-legal framework for Blockchain and GDPR derive.

While Blockchain alone may not provide a complete solution to meet all GDPR requirements, as specified above, the suitability of Blockchain as a tool to achieve GDPR's objectives depends on the context and specific use case. Notwithstanding, privacy-enhancing techniques offer a compelling argument in this regard. By guaranteeing the ability to verify data without disclosing sensitive information, these techniques align with the GDPR's data principles and safeguard individual privacy.

Furthermore, it is possible to identify – though not exhaustively - other areas where Blockchain can align with GDPR objectives, such as the principle of transparency, accountability, minimization, data integrity and security and consent management.

Blockchain technology offers numerous opportunities to enhance security due to its characteristics of resilience and cryptography (in particular, hashes, digital signatures, and consensus algorithms), which ensure data integrity and protection prevent unauthorized parties from tampering with, deleting, or stealing data. As a consequence, Blockchain-based systems are regarded as preferable for creating a GDPR-compliant environment with respect to implementing the security principle, as they can help organizations meet GDPR requirements for data protection and safeguarding individuals' rights.

Additionally, smart contracts can represent a solution for handling data subject consent thanks to their ability to translate privacy preferences into automated rules. These contracts can subsequently validate data access requests from third parties and enable individuals to verify which entities can access specific portions of their personal data.

From the above discussion, it emerged that the question posed at the beginning of this paragraph finds a positive answer. In this regard, in order for the argument to be consistent with the whole thesis, we deemed it necessary for it to be supported by a practical example, given that it has been stated here and in several other parts of the thesis that context and a specific use case can never be disregarded.

In light of this, the last question which guided our research regarded the possibility of leveraging Blockchain to safeguard personal data by creating a digital identity management system respectful of the principles of the GDPR.

1.6.Can Blockchain-Based Self-Sovereign Identity (SSI) Enhance Data Protection Rights?

Through assessing the self-sovereign identity use case, this thesis argued that a decentralized system, such as a Blockchain, can be structured to support advanced techniques that implement privacy-enhancing solutions for decentralized data management. However, as presented in the previous pages, this does not mean that it is possible to conclude, in general, on the compatibility of GDPR and SSI, as some considerations can be formulated only in relation to the specific characteristics of a given SSI system.

Nevertheless, confronting the SSI principles with the principles of the GDPR showed possible grounds for mutual adaptability.

The research claimed that a real (and practical) implementation of a Blockchain-based digital identity system would require the development of technical standards and adjustments in the current regulatory framework, which suffers uncertainties and gaps related not only to the Blockchain domain but also to digital identity.

Analysing the use case of the SSI helped prove not only that all the uncertainties encountered for Blockchain are also reproduced in this specific use case - in our opinion, the most paradigmatic for discussing the issue of data protection - but also that each use case is affected by the regulatory, social and political context in which it is set.

In this respect, the current process of revising the eIDAS regulation, which included provisions in the draft regulation to legitimize Blockchain as the underlying technology for self-sovereign identities, is characterized by a number of discordant opinions regarding whether or not this provision should be retained.[789]

The current debate signals relevant differences of opinion among the various stakeholders involved. In this regard, what is noteworthy and surprising is that, instead of promoting a constructive dialogue to find common ground among different perspectives and interests, some actors load with prejudices the Blockchain, which, although is still in its developmental stages, requires some guidance.

Undoubtedly, progresses in the discourse around Blockchain-based digital identities can only occur if, first and foremost, the involved stakeholders actively endorse a shift in governance and contribute to the construction of a new digital identity ecosystem; otherwise, the idea that SSI could provide a high standard of privacy protection while remaining compliant with GDPR would remain unaccomplished.

2. Research Contributions

This thesis served as an attempt to address numerous questions that revolve around two primary aspects: the compatibility of the existing data protection framework with Blockchain technology and the feasibility of implementing a Blockchain-based digital identity management solution.

Although this research may not have provided definitive answers to all inquiries, it has certainly begun to chart the course towards a more comprehensive understanding of the intricate relationship between Blockchain and the legal and data protection landscape. The following recommendations and implications, drawn from the research findings, may offer valuable insights into formulating a nuanced techno-

[789] Refer to paragraph 5.2.2. for further details.

legal framework tailored to the unique challenges and opportunities presented by the technology within the EU Data Protection law context.

a) Regulatory Guidance and Interpretative Frameworks

It is imperative to develop regulatory guidance and interpretative frameworks tailored to the distinctive challenges presented by Blockchain technology.

These frameworks should offer clear directives regarding the application of data protection principles, considering the unique attributes of Blockchain systems. Collaboration between regulatory bodies and industry stakeholders should be encouraged to establish best practices and standards that strike a harmonious balance between fostering innovation and safeguarding privacy.

b) Emphasis on Privacy-by-Design

A pivotal aspect of Blockchain application development should involve a resolute commitment to privacy-by-design principles. Developers should proactively integrate privacy-enhancing technologies and mechanisms to strictly adhere to data protection requirements. Privacy-enhancing techniques should be harnessed to effectively mitigate the inherent privacy risks associated with Blockchain technology.

c) Enforcement of User Control

Blockchain systems should explore innovative mechanisms that empower users to exercise control over their personal data while capitalizing on the advantages offered by the technology. Implementing features like smart contracts and self-sovereign identity frameworks can give individuals the means to assert authority over their personal information, ensuring that their consent and preferences are respected within the system.

d) Contextual Compliance

It is crucial to emphasize that Blockchain technology cannot be unequivocally categorized as GDPR-compliant or non-compliant in a blanket manner. The degree of compliance is intrinsically linked to the context and intricacies of the specific Blockchain implementation. Thus, a case-by-case assessment is crucial to ascertain the technology's alignment with data protection regulations.

e) Establishment of a Techno-Legal Framework

The research aimed to develop a foundational cornerstone for a comprehensive techno-legal framework. This framework should be meticulously crafted to harmonize the revolutionary potential of Blockchain with the fundamental tenets of data protection. Therefore, the distinctive attributes of Blockchain should not be denied, but, at the same time, the effective application of data protection principles should be ensured.

In conclusion, these recommendations underscore the true meaning of adapting and evolving regulatory approaches to accommodate the transformative influence of Blockchain technology. The goal is to foster an ecosystem where innovation and data protection coexist harmoniously, safeguarding individual rights while encouraging technological advancement.

This journey, which appears at the initial stages, necessitates collaborative efforts from all stakeholders, including policymakers, technologists, and legal experts, to navigate the complex intersection of Blockchain and data protection effectively. This common approach towards proving some (in a broad sense, regulatory) guidance would serve a dual purpose. Firstly, it would offer greater assurance to stakeholders operating in the Blockchain industry, addressing their concerns about the challenges of creating compliant Blockchain applications due to the existing ambiguity in legal requirements. Secondly, offering guidance on GDPR's application to blockchains and clarifying aspects of the Regulation that have generated uncertainty would contribute to greater clarity and transparency in the broader data economy.

The recent proposal by the European Commission to reform the GDPR[790] emphasizes that the Regulation is not static but rather a framework that requires ongoing attention and development. This analogy likens the GDPR to a "very young child"[791] needing nurturing and guidance to mature effectively. However, it is important to note that the proposed reform primarily focuses on addressing disputes and harmonizing cross-border requirements rather than specifically adapting the Regulation to Blockchain technology.

This research often affirmed that the question of regulating Blockchain and reforming the GDPR is not that easy, given that it could entail re-designing the whole data protection framework and inevitably reopening contentious debates. [792]

Although the current situation does not seem so favourable to Blockchain and, at the same time, the GDPR is progressively revealing (some of) its inefficiency, this research still affirms that implementing a European law specifically addressing Blockchain technology could bring several advantages and address key areas of concern.

[790] Cfr. note 663.

[791] https://www.euronews.com/my-europe/2023/07/04/brussels-pitches-gdpr-reform-but-without-opening-pandoras-box.

[792] As Reynders said, it would inevitably reopen the 'Pandora box', https://www.euronews.com/my-europe/2023/07/04/brussels-pitches-gdpr-reform-but-without-opening-pandoras-box.

Firstly, such a law would provide regulatory clarity, reducing uncertainty and facilitating innovation within the Blockchain ecosystem. This clarity would enable businesses and individuals to operate confidently, knowing the legal boundaries and requirements.

Secondly, a European law on Blockchain could promote the establishment of standards encompassing interoperability, security, and governance. These standards would ensure that Blockchain systems across different sectors and industries within the European Union are compatible and can collaborate effectively. This harmonization would drive widespread adoption and streamline operations in various fields.

Moreover, as often noted in this thesis, such a law could specifically address the unique challenges related to data protection and privacy in Blockchain networks. As Blockchain often involves processing personal data, a European law would provide guidelines on ensuring compliance with existing data protection frameworks, such as the GDPR. Tailored provisions would clarify data handling practices, enhancing privacy rights and safeguarding individuals' personal information within Blockchain systems.

In other words, an EU regulatory scheme would provide a more cohesive, coordinated, and influential approach to addressing the challenges posed by Blockchain technology, which has no space or time borders. Given the significant influence exerted by EU regulations and standards on global markets and industries, an EU solution would also effectively shape global norms and practices, influencing businesses, governments, and regulators worldwide[793] (i.e., towards non-member States).

[793] We refer to the so-called "Brussels effect", see Chapter III, para 3.4.

We find ourselves at the threshold of a profound debate, and the journey has only just commenced. It's akin to the unfolding of a captivating story, where some contend that the legal framework laid out by the GDPR is in its embryonic stage,[794] and the Blockchain, like a never-ending novel, continues to write its chapters of development and innovation.

[794] Opinion of Advocate General Bobek, C-645/19, Facebook V. Belgium DPA (2021) ECLI:EU:C:2021:5, para. 12.

References

Literature

Abramowicz M., *Cryptocurrency-Based Law*, in *Arizona Law Review*, 2016, p. 359-420.

Adinolfi A., *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in Dorigo S. (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Editore, 2020, pp. 1-16.

Alessi M., Camillò A., Giangreco E., Matera M., Pino S., Storelli D., *A decentralized personal data store based on Ethereum: towards GDPR compliance*, in *Journal of Communication Software and System*, 2019, pp. 79-88.

Allen C., *The path to self-sovereign identity*, in *Life with Alacrity*, 2016, https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html#dfref-1212.

Almeida Teixeira G., Mira da Silva M., Pereira R., *The critical success factors of GDPR implementation: A systematic literature review*, in *Digital Policy, Regulation Governance*, vol. 21, no. 4, 2019, pp. 402–418.

Amelin R., Channov S., Lipatov E., *Lex Informatica: Information Technology as a Legal Tool*, in *Communications in Computer and Information Science*, Springer Science and Business Media Deutschland GmbH, 2022, pp. 177–189.

Andrew J., Baker M., *The General Data Protection Regulation in the Age of Surveillance Capitalism*, in *Journal of Business Ethics*, 2021, pp. 565–578.

Anke J., Ehrlich T., Richter D., Meisel M., *Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities*, pp. 247–270.

Ateniese G., Magri B., Venturi D., Andrade E., *Redactable Blockchain – or – Rewriting history in Bitcoin and friends*, in *2017 IEEE European Symposium on Security and Privacy*, 2017, pp. 111–126.

Atzori M., *Blockchain technology and decentralized governance: is the state still necessary?*, 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713.

Atzori M., *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 2015.

Bacon J. et al, *Blockchain Demystified*, Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017, p.4, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218.

Bag A., Aamir Ali S.M., Ghose A., Mishra P., Singh B. P., Datta S., *The Role of Blockchain Technology on Human Rights Management and Business Ethics—Utopia or Dystopia*, in: Yadav S., Haleem A., Arora P.K., Kumar H. (eds), *Proceedings of Second International Conference in Mechanical and Energy Technology. Smart Innovation, Systems and Technologies*, Springer, 2023, pp. 359-365.

Balboni P., Barata M.T., Botsi A., Francis K., *Accountability and Enforcement Aspects of the EU General Data Protection Regulation: Methodology for the Creation of an Effective Compliance Framework and a Review of Recent Case Law*, in *The Maastricht Law and Tech Lab*, 2019, pp. 103-254.

Balboni P., Barata M.T., *Legal aspects of Blockchain technology,* in *Essentials of Blockchain Technology,* Chapman and Hall, 2019, pp. 293-348.

Baldoni R., *Federated Identity Management systems in e-government: The case of Italy*, in *Electronic Government*, 2012, pp. 64-68.

Baldwin R., Cave M., Lodge M., *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2013, pp. 1-568.

Baran P., *On distributed communications: I. Introduction to distributed communication networks*, Santa Monica, 1964, pp.1-37.

Bardhan A., *Recent Developments in Blockchain,* in *Journal of University of Shanghai for Science and Technology*, 2021, pp. 1487–1498.

Baxter L. G, *Understanding Regulatory Capture: An Academic Perspective from the United States,* in *Making good financial regulation: towards a policy response to regulatory capture,* (Stefano Cagliari ed., 2012), p. 31-39.

Beck R., Muller-Bloch C., King J., *Governance in the Blockchain Economy: A Framework and Research Agenda*, 2018, https://www.researchgate.net/publication/323689461_Governance_in_the_Blockchain_Economy_A_Framework_and_Research_Agenda.

Belli L., Francisco P. A., Zingales N., *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police*, in Belli L., Zingales N. (eds), *Platform Regulations: How Platforms Are Regulated and How They Regulate Us*, FGV Direito Rio, 2017.

Bello B., *Tackling online hate speech from a European perspective: Potentials and challenges of inter-legality*, in *Oñati Socio-Legal Series*, 13(4), 2023, pp. 1376–1411.

Benkler Y., *The Wealth of Networks How Social Production Transforms Markets and Freedom*, Yale University Press, 2006.

Berberich M., Steiner M., *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, 2016, pp. 422-426.

Bernabe J.B. , Canovas J.L. , Hernandez-Ramos J.L., Moreno R.T., Skarmeta A., *Privacy-preserving solutions for Blockchain: review and challenges*, in *IEEE Access*, 2019, pp. 164908-164940.

Bitansky N., Canetti R., Chiesa A., Tromer E., *From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again*, in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, 2012, pp. 326–34.

Black J., *Critical reflections on regulation,* in *Australian Journal of Legal Philosophy*, 2002, pp. 1-37.

Blume P., Svanberg C. W., *The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/Public Sector Divide and the Bureaucratic Apparatus*, in *Cambridge Yearbook of European Legal Studies*, 2013.

Bodó B., Brekke J.K., Hoepman J.H. , *Decentralisation in the Blockchain space* in *Internet Policy Review*, 10(2), 2021, pp. 1-12.

Bogner A., Chanson M., Meeuw A., *A decentralised sharing app running a smart contract on the Ethereum Blockchain*, in *ACM International Conference Proceeding Series,* 2016, pp. 177–178.

Bollen R., *The Legal Status of online currencies: are bitcoins the Future?*, in *Journal of Banking and Finance Law and Practice,* 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285247.

Botsman R., *Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart*, 2017, London: Portfolio Penguin.

Boyle J., *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors, University of Cincinnati Law Review*, 1997, pp. 177-205.

Bradford A., *The Brussels Effect*, in *Northwestern University Law Review,* 2012, pp. 1-68.

Brakeville S., *Blockchain basics: Introduction to distributed ledgers*, 2018, available at https://developer.ibm.com/tutorials/cl-Blockchain-basics-intro-bluemix-trs/.

Brekhov G. S., *Crypto-Anarchism: The Ideology of Blockchain Technologies*, in *RUDN Journal of Political Science*, 2022, pp. 393–407.

Brescia R., *Regulating the Sharing Economy: New and Old Insights into an Oversight Regime for the Peer-to-Peer Economy,* in *Nebraska Law Review 87*, 2016, p. 88-145.

Brescia R.H., *What We Know and Need to Know about Disruptive Innovation*, in *South Carolina Law Review*, 2016.

Brevini B., Pasquale F., *Revisiting the Black Box Society by rethinking the political economy of big data* in *Big Data and Society*, SAGE Publications Ltd, 2020.

Brown J., Marsden C.T., *Regulating Code: good governance and better regulation in the Information Age,* Cambridge: MIT Press, 2013.

Brownsword R., Goodwin M., *Law and the Technologies of the Twenty-First Century. Texts and Materials*, Cambridge University Press, 2012.

Brownsword R., *Law, Technology and Society: Reimagining the Regulatory Environment*, Oxford: Routledge, 2019.

Brownsword R., *Rights, Regulation, and the Technological revolution,* Oxford University Press, 2008, p. 559-564.

Buocz T., Ehrke-Rabel T., Hödl E., Eisenberger I., *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, in *Computer Law Security Review*, 2019, pp. 182–198.

Burton C., De Boel L., Kuner C., Pateraki A., Cadiot S., Hoffman S. G., *The Final European Union General Data Protection Regulation,* in *Bloomberg Law: Privacy & Data Security,* 12 February 2016.

Buterin V., Illum J., Nadler M., Schar F., Soleimani A, *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium,* 2023, available at https://ssrn.com/abstract=4563364.

Byhoff M., Ford B., *This State is Becoming America's Crypto Capital*, Bloomberg, 2022.
Caccia L., *The Extraterritorial Reach of the General Data Protection Regulation: A Critique of the Establishment Criterion*, in *Common Market Law Review*, 2019, pp. 63-100.

Cai W., Wang Z., Ernst J.B., Hong Z., Feng C., Leung V. C. M., *Decentralized Applications: The Blockchain-Empowered Software System,* in *IEEE Access*, 2018, pp. 53019–53033.

Callon M., Lasoumes P., Bathe Y., *Acting in an Uncertain World: Essay on Technical Democracy* (Inside Technology), MIT Press, 2011.

Cameron K., *The laws of identity,* in *Kim Cameron's Identity Weblog,* 2005, https://www.identityblog.com/?p=352.

Campanile L., Iacono M., Levis A.H., Marulli F., Mastroianni M., *Privacy regulations, smart roads, Blockchain, and liability insurance: putting technologies to work,* in *IEEE Security and Privacy,* 2020, pp. 34-43.

Cannon J. C., *The EU General Data Protection Regulation: A Primer and Future Implications*, in *Journal of Information Privacy and Security*, 2017, pp. 61-76.

Cappiello B., *Where is justice taking place? Blockchain technology as a tool to fill a gap*, in *Rivista di diritto internazionale privato e processuale 3/2019*, pp. 652-680.

Cavoukian A., *Evolving FIPPs: proactive approaches to privacy, not privacy paternalism*, in Gutwirth S., Leenes R., de Hert P. (eds), *Reforming European data protection law*, Springer, 2015.

Chadwick D. W., *Federated identity management*, in *Lecture Notes in Computer Science*, 2009, pp. 96–120.

Chaum D., *Blind signatures for untraceable payments,* 1998, http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

Chen Y., Bellavitis C., *Blockchain disruption and decentralized finance: The rise of decentralized business models*, in *Journal of Business Venturing Insights*, 2020, pp.1-23.

Chiu I.H.Y., *Regulating the Crypto Economy: Business Transformations and Financialisation*, Hart Publishing, 2021.

Chowdhuri N., *Inside Blockchain, Bitcoin, and cryptocurrencies,* CRC Press, 2020, pp. 1-390.

Christensen C.M. et al, *Disruptive Innovation: An Intellectual History and directions for further research,* in *Journal of Management Studies,* 2018, p. 1043.

Christensen C.M., *Disruptive Class: How disruptive innovation will change the way the world learns,* McGraw-Hill, 2008.

Christman J., *Social practical identities and the strength of obligation*, in *Journal of Social Philosophy*, 2013, pp. 121–123.

Clark C., *The answer to the machine is the machine* in *The future of copyright in a digital environment: Proceeding of the Royal Academy Colloquium,* The Hague Kluwer Law International, 1996, pp. 139-145.

Cockfield A.J., Pridmore J., *A Synthetic Theory of Law and Technology*, in *Minnesota Journal of Law, Science & Technology*, 2007, pp. 475-513;

Cockfield A.J., *Towards a law and technology theory*, in *Manitoba Law Journal*, 2004, pp. 383-415.

Cohen J. E., *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, in *Connecticut Law Review,* 1996, p. 981-1039.

Cohen J. E., *Between Truth and Power - The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019.

Cohen J. E., *Examined Lives: Informational Privacy and the Subject as Object*, in *Stanford Law Review*, 2000, pp. 1373-1438.

Cong L.C., He Z., *Blockchain disruption and smart contracts*, in *Nber Working paper series*, 2018.

Connor-Green D., *Blockchain in Healthcare Data*, in *Intellectual Property & Technology Law Journal*, 2017.

Contaldi G., *Il regolamento 2022/1925 e la tutela della privacy online*, in *QUADERNO AISDUE, SERIE SPECIALE Atti del Convegno "Ambiente, digitale, economia: l'Unione europea verso il 2030" Bari 3-4 novembre 2022,* Serie speciale, Editoriale scientifica, pp. 119 – 140.

Contaldi G., *Il DMA (Digital Markets Act) può contribuire alla protezione dei dati degli utenti online?,* in *Diritti umani e diritto internazionale*, Il Mulino, 2023, pp. 77 – 93.

Corballis T., Soar M., *Utopia of abstraction: Digital organizations and the promise of sovereignty,* in *Big Data and Society*, 2022.

Côté J.E., *Sociological perspectives on identity formation: the culture–identity link and identity capital,* in *Journal of Adolescence*, 2016, pp. 417–428.

Crumpler W., *The Human Rights Risks and Opportunities in Blockchain,* Center for Strategic and International Studies, 2021, pp. 1-90.

Cryer R., Hervey T., Sokhi-Bulley B., Bohm A., *Research methodologies in EU and International Law*, Hart Publishing, 2011.

Dahlberg L., *Cyber-Libertarianism 2.0: A discourse theory/critical political economy examination,* in *Cultural Politics an International Journal,* 2010, pp. 331-356

Dahlberg L., *Cyberlibertarianism,* in *Oxford Research Encyclopedia of Communication*, 2017.

Daoui S., Fleinert-Jensen T., Lemperiere M., *GDPR, Blockchain and the French data protection authority: many answers but some remaining questions*, in *Stanford Journal Blockchain Law & Policy*, 2019, pp. 240-251.

Daudén-Esmel C., Castellà-Roca J., Viejo A., Domingo-Ferrer J., *Lightweight Blockchain-based platform for GDPR-compliant personal data management*, in *Proceedings of the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy*, 2021, pp. 68-73.

De Filippi P., Hassan S., *Blockchain technology as a regulatory technology: From code is law to law is code*, in *First Monday,* volume 21, number 12, 5 December 2016.

De Filippi P., Mannan M., Reijers W., *The alegality of Blockchain technology*, in *Policy and Society*, 2022, pp. 1–15.

De Filippi P., *The interplay between decentralization and privacy: the case of Blockchain technologies,* in *Journal of Peer Production, Issue n.7: Alternative Internets*, 2016.

De Filippi P., Wright A., *Blockchain and the Law -The rule of code*, Harvard University Press, 2018, pp.1-300.

De Hert P., Papakonstantinou V., *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*, in *Computer Law & Security Review*, 2016, pp. 179-194.

De Pasquale P., *Crypto art e NFT nell'Unione europea: aporie sistemiche e ragioni di una (dis)attesa disciplina,* in *Il diritto dell'Unione europea,* 2022, pp. 1-26.

De Sousa H.R., Pinto A., *Blockchain based informed consent with reputation support*, in *Blockchain and Applications: International Congress*, Springer, 2019, pp. 54-61.

De Sousa H.R., Pinto A., *On the feasibility of Blockchain for online surveys with reputation and informed consent support Ambient Intelligence – Software and Applications*, in *9th International Symposium on Ambient Intelligence,* 2018, pp. 314-322.

Deffains B., Fenoglio P., *Economics and legal order of cyberspace*, in *Revue Economique*, *52*(7), 2001, pp. 331–347.

Deng M., Wuyts K., Scandariato R., Preneel B., Joosen B., *A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements*, in *Requir Eng*, 2010, pp. 3–32.

Dhillon V., Metcalf D., Hooper M., *Blockchain-enabled application*, Springer, 2017.

Dienlin T., Masur P. K., Trepte S., *A longitudinal analysis of the privacy paradox,* in *New Media & Society*, 2023, pp. 1043 – 1064.

Duarte D. G., *An Introduction to Blockchain Technology from a Legal Perspective and its Tensions with the GDPR*, in *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law*, 2019.

Dulong de Rosnay M., *Peer-to-Peer as a Design Principle for Law: Distribute the Law,* in *Journal of Peer Production,* 2015.

Duta N., *A survey of biometric technology based on hand shape*, in *Pattern Recognition*, 2009, pp. 2797–2806.

Dwork C., Roth A., *The algorithmic foundations of differential privacy*, in *Foundations and Trends in Theoretical Computer Science*, 2014, pp. 211-407.

Eakin P. J., *How Our Lives Become Stories: Making Selves*, Cornell University Press, 1999.
Eberhardt J., Tai S., *On or off the Blockchain? Insights on off-chaining computation and data*, in De Paoli F., Schulte S., Broch Johnsen E. (Eds.), *Service-oriented and cloud computing*, Springer International Publishing (Lecture Notes in Computer Science), pp. 3–15.

Edwards L., *Law, Policy and the Internet,* Oxford: Hart Publishing, 2018.

Eichler N., Jongerius S., McMullen G., Naegele O., Steininger L., Wagner K., *Blockchain, Data Protection, and the GDPR*, Technical Report VR 36105 B 27/661/52176, German Blockchain Association (Bundesblock), 2018.

Eichner K., *The Territorial Scope of the General Data Protection Regulation*, in *Journal of Data Protection & Privacy*, 2017, pp. 122-140.

El Emam K., C. Álvarez, *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, in *International Data Privacy Law*, 2015.

El Khoury A., *Dynamic IP Addresses Can Be Personal Data, Sometimes. A Story of Binary Relations and Schrodinger's Cat*, in *European Journal of Risk Regulation* (EJRR), 2017, pp. 191-197.

El-Gazzar R., Stendal K., *Examining how GDPR challenges emerging technologies*, in *Journal of Information Policy*, Penn State University Press, 2021, pp. 238-275.

Ellison C. M., *SPKI/SDSI Certificates*, 2004, https://theworld.com/~cme/html/spki.html.
ElSalamouny E., Gambs S., *Differential privacy models for location-based services*, in *Transaction on Data Privacy*, 2016, pp. 15-48.

Engels C., Westermeier M., *Blockchain and the GDPR: Conflict or Concordance*?, in *Computer Law & Security Review 34,* no. 6, 2018, pp. 1345-1357.

Erbguth J., *Five ways to GDPR-compliant use of Blockchains,* in *European Data Protection Law Review*, 2019, pp. 427-433.

Esposito C., De Santis A., Tortora G., Chang H., Choo K.K. R., *Blockchain: A Panacea for healthcare cloud-based data security and privacy?* in *IEEE Cloud Computing*, pp. 31–37.

Ezzat S. K., Saleh Y. N.M., Abdel-Hamid A. A., *Blockchain Oracles: State-of-the-art and research directions,* in *IEEE Access,* 2022 pp. 1-19.

Faber B., Michelet G., Weidmann N., Mukkamala R. R., Vatrapu R., *BPDIMS: A Blockchain-based Personal Data and Identity Management System*, in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019, pp. 6855-6864.

Fairfield J., *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, in *Indiana Law Journal,* 2022, Available at: https://www.repository.law.indiana.edu/ilj/vol97/iss4/4;

Falke J., Schepel H. (eds.), *Legal Aspects of Standardisation in the Member States of the EC and of EFTA,* vol 1, in H. S. A. Luxembourg: Office for Official Publications of the European Communities, 2000, p. 181.

Farzanehfar A., Houssiau F., de Montjoye Y.A., *The risk of re-identification remains high even in country-scale location datasets*, in *Patterns (NY)*, 2021.

Fenwick M.,. Kaal W.A, Vermeulen E.P.M., *Regulation tomorrow: what happens when technology is faster than the law?,* in *American University Law Review*, 2017, pp. 561-594.

Ferrari V., Quintais J.P., Giannopoulou A., Bodo B., *EU Blockchain Observatory and Forum Workshop on GDPR,* in *Data Policy and Compliance,* Research Nodes 2018/1, Blockchain & Society Policy Research Lab, Institute for Information Law, University of Amsterdam, 2018.

Finck M., *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?,* 2019.

Finck M., *Blockchain, Regulation and Governance in Europe,* Cambridge University Press, 2018.

Finck M., *Blockchains and data protection in the European Union,* in *Max Planck Institute for Innovation and Competition Research Paper (MPI Paper),* 2017.

Finck M., *Blockchains and Data Protection in the European Union,* in *European Data Protection Law Review*, 2018.

Finck M., *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy,* in *European Law Review*, 2018.

Finck M., *Smart contracts as a form of solely automated processing under the GDPR,* in *International Data Privacy Law*, 2019, pp. 78-94.

Fischer A., Valiente M.C., *Blockchain governance,* in *Internet Policy Review*, 2021, pp. 1-10.

Fisse B., Braithwaite J., *Corporations, crime and accountability,* Cambridge University Press, 1993.

Frydman B., Hennebel L., Lewkowicz G., *Co-regulation and the rule of law,* in Brosseau E., Marzouki M., Méadel C., *Governance, Regulation and Powers on the Internet,* Cambridge University Press, 2012, pp. 133-150.

Frydman B., Hennebel L., Lewkowicz G., *Public strategies for Internet Co-Regulation in the United States, Europe and China,* in Brosseau E., Marzouki M., Méadel C., *Governance, Regulations and Powers on the Internet, Cambridge, Cambridge University Press*, 2008.

Gal M., Aviv O., *The Competitive Effects of the GDPR,* in *Journal of Competition Law and Economics*, 2020, pp. 1-37.

Gallagher J. R., *A Framework for Internet Case Study Methodology in Writing Studies*, in *Computers and Composition*, 2019,

Garcia Mexia P., Morales Barroso J., *Cryptoregulation in a nutshell*, Wolters Kluwer, 2020, pp. 1-164.

Giannopoulou A., *Data protection compliance challenges for self-sovereign identity*, in *Blockchain and Applications: 2nd International Congress, Springer*, 2020, pp. 91-100.

Giannopoulou A., Ferrari V., *Distributed data protection and liability on Blockchains*, in *Internet Science (Lecture Notes in Computer Science),* Springer, 2019, pp. 203–211.

Giannopoulou A., *Putting data protection by design on the Blockchain*, in *European Data Protection Law Review*, 2021, pp. 388-399.

Gil González E., de Hert P., *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, in *ERA Forum*, 19(4), 2019, pp. 597–621.

Giordanengo A., *Possible usages of smart contracts (Blockchain) in healthcare and why No one is using them*, in *MEDINFO 2019: Health and Wellbeing E-Networks for All*, IOS Press, 2019, pp. 596-600.

Giordano M.T. , *Blockchain and the GDPR: new challenges for privacy and security*, in Cappiello B., Carullo G. (eds), *Blockchain, Law and Governance, Springer*, 2021, pp. 275-286.

Gola C., Sedlmeir v, *Addressing the Sustainability of Distributed Ledger Technology*, Bank of Italy Occasional Paper No. 670, 2022, available at SSRN: https://ssrn.com/abstract=4032837.

Goldsmith J., *Against Cyberanarchy*, in *University of Chicago Law Review* 65, 1998.

Goldsmith J., Wu T., *Who controls the Internet? Illusions of a borderless world,* Oxford University Press, 2006.

Goldwasser S., Micali S., Rackoff C., *The knowledge complexity of interactive proof systems*, in *SIAM Journal on computing*, 1989, pp. 186–208.

Grimmelmann J., *Death of a data haven: cypherpunks, WikiLeaks, and the world's smallest nation*, 28 March 2012, https://arstechnica.com/tech-policy/2012/03/sealand-and-havenco/.

Guihot M., *Coherence in Technology Law*, in *Law and Technology* 11(2), 2019, pp. 6-7.

Gurstein M., *The Multistakeholder Model, Neo-liberalism and Global (Internet) Governance,* in *Gurstein's Community Informatics,* 26 March 2014.

Hacker P., Lianos I., Dimitropoulos G., Eich S. (eds), *Regulating Blockchain. Techno-Social and Legal Challenges,* Oxford University Press, 2019.

Hallinan D., Zuiderveen Borgesius F., *Opinions can be incorrect! In our opinion: on data protection law's accuracy principle,* in *International Data Privacy Law*, 2020.

Hamza M. K., Abubakar H., Danlami Y. M., *Identity and Access Management System: a Web- Based Approach for an Enterprise*, in *Path of Science*, vol. 4, no. 11, 2018, pp. 2001–2011.

Hassan S., De Filippi P., *Decentralized autonomous organization*, in *Internet Policy Review*, *10*(2), 2021, pp. 1–10.

Hassan U., Rehmani M. H., Chen J., *Differential privacy in Blockchain technology: A futuristic approach*, in *Journal of Parallel and Distributed Computing*, 2019, pp. 50-74.

Heiss J., Ulbricht M.-R., Eberhardt J., *Put Your money where Your mouth is – towards Blockchain-based consent violation detection*, in *Proceedings of the 2020 International Conference on Blockchain and Cryptocurrency, IEEE*, 2020.

Hemenway F., Hammer S., *A Comprehensive Approach to Crypto Regulation*, in *The University of Pennsylvania Journal of Business Law*, Available at SSRN: https://ssrn.com/abstract=4245285.

Herian R., *Blockchain, GDPR, and Fantasies of Data Sovereignty*, 2019, available at https://oro.open.ac.uk/69445/9/69445.pdf.

Herian R., *Regulating Blockchain – Critical perspectives in law and technology*, Routledge, 2019.

Herian R., *Regulating disruption: Blockchain, GDPR, and questions of data sovereignty*, in *Journal of Internet Law*, 2018.

Hildebrandt M., Tielmans L., *Data Protection by Design and Technology Neutral Law*, in *Computer Law and Security Review*, 2013, pp. 509-521.

Hintze M., El Emam K., *Comparing the benefits of pseudonymisation and anonymisation under the GDPR*, in *Journal of Data Protection and Privacy*, 2018, pp. 145–158.

Hirsch D. D., *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, in *Ohio State Law Journal*, 2013, p. 1030-1069.

Hjerppe K., Ruohonen J., Leppanen V., *The general data protection regulation: Requirements, architectures, and constraints*, in *Proc. IEEE 27th Int. Requirements Eng. Conf. (RE*), 2019, pp. 265–275.

Hoffman M. R., Ibáñez L. D., Simperl E., *Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework* in *Frontiers in Blockchain*, 2020, pp. 1-18.

Hofman D., Lemieux V.L., Joo A., Batista D.A., *The margin between the edge of the world and infinite possibility": Blockchain, GDPR and information governance,* in *Record Management Journal*, 2019, pp. 240-257.

Hoofnagle C. J., van der Sloot B., Borgesius F. Z., *The European Union general data protection regulation: What it is and what it means*, in *Information and Communications Technology Law*, 2019, pp. 65–98.

Hsieh Y.Y., Vergne J.P., Anderson P., Lakhani K., Reitzig M., *Bitcoin and the rise of decentralized autonomous organizations*, in *Journal of Organization Design*, 7(1), 2018.

Hutter B., *Risk, regulation and management*, in Taylor-Gooby P., Zinn J. (eds), *Risk in social science*, OUP, Oxford, pp 202–227.

Iansiti M., Lakhani K., *The truth about Blockchain,* in *Harvard Business Review,* 2017, https://hbr.org/2017/01/the-truth-about-Blockchain.

Ibanez Jiménez J. W., *Blockchain: Primeras cuestiones en el ordenamiento español*, Dikinson, pp.1-192.

Ibáñez L. D., O'Hara K., Simperl E.<, *On Blockchains and the General Data Protection Regulation,* available online at *https://eprints.soton.ac.uk/422879/1/Blockchains_GDPR_4.pdf*.

Imteaj A., Amini M. H., Pardalos P.M., *Foundation of Blockchain – Theory and Applications*, Springer, 2021.

Irti C., *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in Senigaglia R., Irti C., Bernes A., (eds) *Privacy and Data Protection in Software Services. Services and Business Process Reengineering*, Springer, 2022.

Jamshed A., Bhardwaj M., Pandey M., Kant Agrawal K., *Securing through pseudorandom number generator and hashing in cryptography,* in *Journal of emerging technologies and innovative research,* 2019, pp. 203-206.

Janal R., *Data Portability - A Tale of Two Concepts*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 2017, pp. 59-69.

Jarvis C., *Cypherpunk ideology: objectives, profiles, and influences (1992–1998),* in *Internet HistorIes,* 2022, pp. 315–342

Jasserand v, *Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation,* in *European Data Protection Law Review,* 4(2), 2018, pp. 152–167.

Javed I. T., Alharbi F., Margaria T., Crespi N., Qureshi K. N., *PETchain: A Blockchain-Based Privacy Enhancing Technology,* in *IEEE Access,* 2021, pp. 41129-41143.

Jimènz G., Briseida S., *Risks of Blockchain for data protection: A European approach,* in *Santa Clara High Technology Law Journal,* 2020, pp. 281-343.

Johnson D., Post D., *Law and Borders: The Rise of Law in Cyberspace,* in *Stanford Law Review,* 1996, pp. 1367-1402

Johnson D.R., Post D.G., *Law and Borders: The rise of Law in Cyberspace,* in *Stanford Law Review,* 1996, p. 1367.

Jøsang A., Fabre J., Hay B., Dalziel J., Pope S., *Trust Requirements in Identity Management,* in P. Montague, & R. Safavi-Naini (Ed.), *Australasian Information Security Workshop 2005.*

Juhasz P. L., Steger J., Kondor D., Vattay G., *A bayesian approach to identify bitcoin users,* in *PLoS ONE,* 2018, pp.1-21.

Jussila J. P., *Reconciling the conflict between the 'immutability' of public and permissionless Blockchain technology and the right to erasure under Article 17 of the General Data Protection Regulation,* 2017,

Kakarlapudi P. V., Mahmoud Q. H., *Design and development of a Blockchain-based system for private data management,* in *Electronics,* 2021, pp. 1-22.

Kamara I., *Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate,* in *European Journal of Law and Technology,* 2017, pp. 1-24.

Katyal N., *Disruptive Technologies and the Law,* in *Georgetown Law Journal,* 2014.

Kaushal M., *Cryptography: A Brief Review. International Journal for Research,* in *Applied Science and Engineering Technology.*

Kelly K., *Out of Control,* Basic Books 1994.

Kianieff M., *Blockchain technology and the Law – Opportunities and Risks,* Routledge, 2019.

Kohl U., *Blockchain utopia and its governance shortfalls*, in Pollicino O., De Gregorio G., *Blockchain and Public Law*, cit., 2022, pp.39-40.

Kokott J., Sobotta C., *The distinction between Privacy and Data Protection in the Jurisprudence of the CjEU and ECtHR,* in *International Data Privacy Law,* 2013.

Kolan A., Tjoa S., Kieseberg P., *Medical Blockchains and privacy in Austria - technical and legal aspects*, in *Proceedings of the 2020 International Conference on Software Security and Assurance*, 2020.

Koops B. J., *Should ICT Regulation be Technology-Neutral? Starting Points For Ict Regulation. Deconstructing Prevalent Policy One-Liners*, in Koops B.J., Lips M., Prins C., Schellekens M. (eds), in *IT & Law Series*, 2006, pp. 77-108.

Koops B.J., *Ten Dimensions of Technology Regulation - Finding Your Bearings in the Research Space of an Emerging Discipline*, in Goodwin M., Koops B.J., Leenes R. (eds), *Dimensions of Technology Regulation*, Wolf Legal Publishers, 2010, pp. 309- 324.

Koppell J.G.S., *Pathologies of Accountability: ICANN and the Challenge of Multiple Accountabilities Disorder*, in *Public Administration Review,* 2005.

Korhonen O., Rantala J., *Blockchain governance challenges: Beyond libertarianism*, in *AJIL Unbound, 2021,* pp. 408–412.

Korte U., Schwalm S., Kusber T., Shamburger K., *Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation*, 2020, pp. 49-60.

Koscina M., Lombard-Platet M., Negri-Ribalta C., *A Blockchain-based marketplace platform for circular economy*, in *Proceedings of the 36th Annual ACM Symposium on Applied Computing, ACM*, 2021, pp. 1746-1749.

Kubach M., Schunck C., Sellung R., Roßnagel H., *Self-sovereign and decentralized identity as the future of identity management*, 2020, pp. 35-47.

Kuner C., *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges",* in Hess B., Mariottini C. M. (eds.), *Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55,* in *LSE Law, Society and Economy Working Papers 3/2015,* pp. 19-55.

Kuner C., *The Extraterritorial Application of the EU Data Protection Regulation*, in *International Data Privacy Law*, 2016, pp. 83-96.

Kuperberg M., *Blockchain-based identity management: a survey from the enterprise and ecosystem perspective*, in *IEEE Transaction on Engineering Management*, 2020, pp. 1008-1027.

Kurihara Y., *Self-Sovereign Identity and Blockchain-Based Content Management*, in Kreps D., Komukai T., Gopal T.V., Ishii K. (eds), *Human-Centric Computing in a Data-Driven Society*, 2020, pp. 130-140.

Lachaud E., *The General Data Protection Regulation and the rise of certification as a regulatory instrument*, in *Computer Law and Security Review*, 2018, pp. 244–256.

Lambrinoudakis C., *The general Data Protection Regulation (GDPR) era: Ten steps for compliance of data processors and data controllers*, in *Proceedings of the International Conference on Trust Privacy and Digital Business*, Springer, 2018, pp. 3–8.

Lamport L., *Time, Clocks, and the Ordering of Events in a Distributed System,* in *Massachusetts Computer Associates, Inc.*, pp. 588-565, https://lamport.azurewebsites.net/pubs/time-clocks.pdf.

Landau S., Le Van Gong H., Wilton R., *Achieving privacy in a federated identity management system,* in *Lecture Notes in Computer Science*, pp. 51–70.

Laurent M., Denouël J., Levallois-Barth C., Waelbroeck P., *Digital identity*, in Laurent M., Bouzefrane S. (Eds.), *Digital Identity Management*, 2015, pp. 1-45.

Lee J., Lee B., Jung J., Shim H., Kim H., *DQ: Two approaches to measure the degree of decentralization of Blockchain*, in *ICT Express*, 2021, pp. 278–282.

Lehdonvirta V., *The Blockchain Paradox: why distributed ledger technologies may do a little to transform the economy,* Oxford Internet Institute, 2016, https://www.oii.ox.ac.uk/news-events/news/the-Blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/

Leonard D., Treiblmaier H., *Can cryptocurrencies help to pave the way to a more sustainable economy? Questioning the economic growth paradigm*, in Treiblmaier H., Beck R. (Eds.), *Business transformation through Blockchain*—Volume I, Cham, Switzerland: Palgrave Macmillan, 2019.

Lessig L., *Code,* Basic Book, 2006.

Lessig L., *Code: And Other Laws of Cyberspace 2.0,* 2006, http://codev2.cc/.

Lessig L., *Remix: Making Art and Commerce Thrive in the Hybrid Economy*, Bloomsbury Publishing, 2008.

Lessig L., *The law of the Horse: what cyberlaw might teach,* in *Harvard Law Review*, p. 1999.

Lessig L., *The Laws of Cyberspace*, 1998.

Lessig L., *The New Chicago School*, in *The Journal of Legal Studies*, 1998, pp. 661–691.

Lifante-Vidal I., *Is Legal Certainty a Formal Value?*, in *Jurisprudence, 2020, p.* 456-467.

Lima C., *Blockchain GDPR privacy by design: how decentralized Blockchain Internet will comply with GDPR data privacy*, 2018, https://Blockchain.ieee.org/images/files/pdf/Blockchain-gdpr-privacy-by-design.pdf.

Liu Y., He D., Obaidat M.S. , Kumar N., Khan M.K., Choo K.K.R., *Blockchain-based identity management systems: a review,* in *Journal of Network and Computer Applications*, 2020, pp. 1-11.

Lo S. et al, *Reliability analysis for Blockchain oracles,* in *Computers and Electrical Engineering*, in 2020, pp. 1-6.

Loewenthal P.J., *Article 291 TFEU*, in M. Kellerbauer et al, *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, 2019, pp. 1925-1932.

Loffreto D., *What is 'Sovereign Source Authority'?*, The Moxy Tongue, 2012, http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

Lopez Rodriguez A. M., *Blockchain and its Impact on Human Rights,* in *Legal Challenges in the New Digital Age*, 2021, pp. 231–252.

Louie T., *Welcome to Wanchain*, https://medium.com/wanchain-foundation/an-introduction-to-wanchain-a2936e25df91.

Luo B., Yang C., *AeRChain: An Anonymous and Efficient Redactable Blockchain Scheme Based on Proof-of-Work*, in *Entropy*, 2023, pp. 270 e ss.

Lyons T., Courcelas L., Timsit, K. *Blockchain and the GDPR: a Thematic Report Prepared by the European Union Blockchain Observatory and Forum*, Thematic Report European Union Blockchain Observatory and Forum, 2018,

Ma J., Xu S., Ning J., Huang X., Deng R. H., *Redactable Blockchain in Decentralized Setting*, in *IEEE Transactions on Information Forensics and Security*, 2022, pp. 1227–1242.

Ma M., Rumore C., Gisolfi D., Kussmaul W., Greening D., *SSI: A roadmap for adoption*, 2018.

Mahieu R. et al, *Responsibility for Data Protection in a Networked World. On the question of the controller, "effective and complete protection" and its application of data access rights in Europe*, in *Journal of Intellectual Property, Information Technology and E-commerce Law*, 2019, https://www.jipitec.eu/issues/jipitec-10-1-2019/4879.

Mainelli M., *Blockchain could help us reclaim control over our personal data*, in *Harvard Business Review*, 2017.

Mainelli M., *Blockchain Will Help Us Prove Our Identities in a Digital World*, in *Harvard Business Review*, 2017.

Malgieri G., *The concept of Fairness in the GDPR: A linguistic and contextual interpretation*, in *FAT* 2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, pp. 154–166.

Mangano R., *Blockchain securities, insolvency law and the sandbox approach*, in *European Business Organization Law Review*, 19(4), 2018, pp. 715–735.

Mannan R., Sethuram R., Younge L., *Practitioner's corner • GDPR and Blockchain: a compliance approach*, in *European Data Protection Law Review*, 2019, pp. 421-426.

Manolopoulos A., *Raising Cyberborders: The Interaction Between Law and Technology*, in *International Journal of Law and Technology*, 2003.

Markey-Tower B., *Anarchy, Blockchain and Utopia: A Theory of Political-Socioeconomic Systems Organised using Blockchain,* in *The Journal of British Blockchain Association,* 2018, pp. 1-14.

Martin A., Sharma G., Peter de Souza S., Taylor L., van Eerd B., McDonald S. M., Dijstelbloem H., *Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions*, in *Geopolitics,* 2022.

Maslin M., Watt M., Yong C., *Research methodologies to support the development of Blockchain standards*, in *Journal of ICT Standardization*, 2019, pp. 249–268.

Mazières D., Sirer E. G., *A decentralized model for data privacy*, in *Communications of the ACM* 62, no. 6, 2019, pp. 58-66.

Mc Nealy J., Flowers A., *Privacy Law and Regulation: Technologies, Implications and Solutions,* in *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*, 2015, pp. 189-205.

McCrudden C., *Legal Research and the Social Sciences* in *Law Quarterly Review* 122, 2006, pp. 632–650.

Meyer D., *Blockchain technology is on collision course with EU privacy law*, IAPP, 2018.

Mirchandani A., *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, *29*(4), 2019, p. 1201.

Moerel L., *Blockchain & Data Protection ... and Why They Are Not on a Collision Course*, in *European Review of Private Law*, 2019, pp. 825–852.

Moerel L., *The long arm reach of EU data protection law: does the Data protection Directive apply to processing of personal data of EU citizens by websites worldwide?,* in *International Data Privacy Law*, 2011, pp. 40-45.

Mohsin K., *Cryptocurrency & Its Impact on Environment*, in *International Journal of Cryptocurrency Research*, 2021, pp. 1-4.

Molina F., Betarte G., Luna C., *Design principles for constructing GDPR-compliant Blockchain solutions*, in *Proceedings of the 2021 4th IEEE/ACM International Workshop on Emerging Trends in Software Engineering for Blockchain*, IEEE, 2021.

Monrat A., Schelén O., Andersson K., *A survey of Blockchain from the perspectives of applications, challenges, and opportunities*, in *IEEE Access,* 2019, pp. 117134–117151.

Morgan B., Yeung K., *An Introduction to Law and Regulation: Text and Materials,* Cambridge University Press, 2007.

Mourby M., Mackey E., Elliot M., Gowans H., Wallace S. E, Bell J., Smith H., Aidinlis S., Kaye J., *Are 'pseudonymised'data always personal data? Implications of the GDPR for administrative data research in the UK*, in *Computer Law Security Review*, vol. 34, no. 2, 2018, pp. 222–233.

Mouzakitis A., *Modernity and the Idea of Progress, in Frontiers in Sociology*, 2017.

Mühle A. et al, *A survey on essential components of a self-sovereign identity*, 2018, available at https://arxiv.org/pdf/1807.06346.pdf

Mühle A. et al, *A survey on essential components of a self-sovereign identity*, in *Computer Science Review*, 2018, pp. 80–86.

Mulford Q. S., *Utopian Thought and Technology,* in *American Journal of Political Science,* 1971, pp. 1921-1989.

Nagar A., Nandakumar K., Jain A. K, *Biometric template transformation: a security analysis*, in *Media Forensics and Security II,* 2010.

Naik N., Jenkins P., An *analysis of open standard identity protocols in cloud computing security paradigm,* in *14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016)*, IEEE, 2016.

Naik N., Jenkins P., *Governing principles of self-sovereign identity applied to Blockchain-enabled privacy-preserving identity management systems*, in *IEEE International Symposium on Systems Engineering*, 2020, pp.1-6.

Naik N., Jenkins P., Newell D., *Choice of suitable identity and access management standards for mobile computing and communication*, in *2017 24th International Conference on Telecommunications (ICT)*, 2017, pp. 1–6.

Nakamoto S., *Bitcoin a Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf

Narayanan A., Bonneau J., Felten E., Miller A., Godfeder S., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* Princeton University Press, 2016.

Narayanan A., Clark J., *Bitcoin's Academic Pedigree*, in *Communications of the ACM*, 2017, pp.20-49.

Neisse R., Steri G., Nai-Fovino I., *A Blockchain-based approach for data accountability and provenance tracking*, in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017.

Newell S., Marabelli M., *Strategic Opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term social effects of 'datafication'*, in *Journal of Strategic Information Systems,* 2015, p. 3.

Nikhil Panday S., Saini A., Gupta N., *Instigating Decentralized Apps with Smart Contracts,* in *Proceedings - IEEE International Conference on Advances in Computing, Communication and Applied Informatics,* 2022.

Nofer M., Gomber P., Hinz O., Schiereck D., *Blockchain,* in *Business and Information Systems Engineering*, 2017, pp. 183-187.

Pagallo U., Bassi E., Crepaldi M., Durante M., *Chronicle of a clash foretold: Blockchains and the GDPR's right to erasure*, in *Legal Knowledge and Information Systems*, 2018, pp. 81-90.

Park D.-S, Chao H.-C., Jeong Y.-S, Park J.J., *Decentralized E-voting systems based on the Blockchain technology*, in *Advances in computer science and ubiquitous computing: CSA & CUTE 17*, Springer, 2018, pp. 305-309.

Pasquale F., *The Blackbox Society*, Cambridge, MA: Harvard University Press, 2015.

Patel A., Jain S., *Present and future of semantic web technologies: a research statement,* in *International Journal of Computers and Applications*, 2021, pp. 413-422.

Pei X., Li X, Wu X., Sun L. , Cao Y,. *UDPP: Blockchain based open platform as a privacy enabler*, in *Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference,* 2020, pp. 500-505.

Pejic I., *Blockchain babel – The Crypto Craze and the Challenge to Business*, Kogan Page, pp. 1-224.

Peters G., E. Panayi, A. Chapelle, *Trends in crypto-currencies and Blockchain technologies: A monetary theory and regulation perspective*, in *Journal of Financial Perspectives*, 2015, pp.1-25.

Petrick E. R., *Building the Black Box: Cyberneticians and Complex Systems* in *Science Technology and Human Values*, 2020, pp. 575–595.

Petrov A.V., Zyryanov A. V., *Formal-dogmatic approach in legal science in present conditions*, in *Journal of Siberian Federal University - Humanities and Social Sciences*, 2018, pp. 968–973.

Pfitzmann A., Hansen M., *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf.

Pinto-Gutiérrez C. et al, *The NFT Hype: What draws attention to Non-fungible tokens?*, in *Mathematics*, 2022, pp. 1-13.

Pisa M., Juden M., *Blockchain and Economic Development: Hype vs Reality*, in *Center for Global Development*, *CGD Policy* (107), 2017, pp. 1–49.

Pitt J., Diaconescu A., *The Algorithmic Governance of Common-Pool Resources*, in Clippinger J. H., Bollier D. (eds), *From Bitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society*, Off the Commons Books, 2014.

Poelman M., Iqbal S., *Investigating the Compliance of the GDPR: Processing Personal Data On A Blockchain*, in *2021 IEEE 5th International Conference on Cryptography, Security and Privacy* (CSP), 2021, pp. 38-44.

Pöhn D., Hillmann P., *Reference Service Model for Federated Identity Management*, in *Lecture Notes in Business Information Processing*, 2021, pp. 196–211.

Poikola A., Kuikkaniemi K., Honko H., *Mydata a Nordic model for human-centred personal data management and processing, Finnish Ministry of Transport and Communications*, 2015.

Politou E., Casino F., Alepis E., Patsakis C., *Blockchain mutability: challenges and proposed solutions*, in *IEEE Transactions on Emerging Topics in Computing*, 2021.

Pollicino O., De Gregorio G., *Blockchain and Public Law: An introduction*, in Pollicino O., De Gregorio G. (eds), *Blockchain and Public Law*, Edward Elgar, 2022, pp.1-256.

Posner R., *Antitrust in the New Economy,* in *Antitrust Law Journal* 68, 2001, pp. 925-943.

Poullet P. L., *The Principles of the General Data Protection Regulation and the Challenges They Raise*, in *Computer Law & Security Review*, 2017, pp. 267-273.

Preukshat A., Reed D., *Self-Sovereign Identity*, 2021.

Price M., Verhulst S., *In search of the self: charting the course of self-regulation on the Internet in a global environment,* in Marsden C. T., *Regulating the Global Information Society*, Routledge, 2000, pp. 57-78.

Puddu I., Dmitrienko A., Capkun S., *μchain: How to Forget without Hard Forks,* 2020, https://eprint.iacr.org/archive/2017/106/1591084586.pdf

Qiao L., Dang S., Shihada B., Alouini M.S., Nowak R., Lv Z., *Can Blockchain link the future?,* in *Digital Communications and Networks*, 2022, pp. 687-694.

Quiniou M., *Blockchain: the Advent of Disintermediation,* in *ISTE Ltd*, 2019.

Rahul D. et al., *Blockchain vs GDPR in Collaborative Data Governance,* in *Cooperative Design, Visualization, and Engineering*, 2020.

Ramadoss R., *Blockchain technology: An overview,* in *IEEE Potentials*, 2022, pp. 6–12.

Ramos L.F.M., Silva J.M.C. , *Privacy and data protection concerns regarding the use of Blockchains in smart cities,* in *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, ACM,* 2019, pp. 342-347.

Rampone F., *Data protection in the Blockchain environment: GDPR is not a hurdle to permissionless DLT solutions,* in *Ciberspazio e Diritto*, 2018, pp. 457-478.

Rantos K., Drosatos G., Demertzis K., Ilioudis C., Papanikolaou A., *Blockchain-based consents management for personal data processing in the IoT ecosystem,* in *Proceedings of the 15th International Joint Conference on E-Business and Telecommunications,* 2018, pp. 572-577.

Rathee T., Singh P., *A systematic literature mapping on secure identity management using Blockchain technology,* in *Journal of King Saud University - Computer and Information Sciences*, 2021.

Reidenberg J. R, *Technology and Internet Jurisdiction,* University of Pennsylvania Law Review, 2005

Reidenberg J. R., *Lex informatica: The formulation of information policy rules through technology,* Texas Law Review, volume 76, number 3, 1998, pp. 553-584.

Reijers W, Wuisman I., Mannan M., De Filippi P., Wray C., Rae-Looi V., Vélez A.C., Orgad L., *Now the code runs itself: On-chain and off-chain governance of Blockchain technologies*, Springer, 2018, pp. 1-22.

Renda A., *Beyond the Brussels effect – Leveraging digital regulation for strategic autonomy*, FEPS – Foundation for European Progressive Studies, 2022.

Renda A., *Single Market 2.0: The European Union as a Platform,* in *The Internal Market 2.0*, Garben S., Govaere I. (eds), Hart Publishing, 2020, pp. 187–212.

Renieris E., *SSI? What we really need is full data portability*, in *Women in Identity*, 2020, https://womeninidentity.org/2020/03/31/data-portability/.

Reno S., Haque M., *Solving Blockchain trilemma using off-chain storage protocol*, in *IET Information Security*, 2023, pp. 681-702.

Reyes C., *Emerging Technology's Language Wars: Smart Contracts*, in *Wisconsin Law Review*, 2022, pp. 85-113.

Reyes C., *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: an Initial Proposal* in *Villanova Law Review*, Vol. 61, No. 1, pp. 191–234.

Riva G. M., *What happens in Blockchain stays in Blockchain. A legal solution to conflicts between digital ledgers and privacy rights,* in *Frontiers in Blockchain*, 2020.

Robb L., Deane F., Tranter K., *The Blockchain conundrum: humans, community regulation and chains,* in *Law, Innovation and Technology*, 2021, pp. 1-22.

Rosenberg A., *Philosophy of Social Science*, Boulder: Westview Press, 2008.

Ross A., Jain A. K., *Multimodal biometrics: an overview*, in *2004 12th European Signal Processing Conference*, 2004, pp.1221–1224.

Rosseau J. J., *On the Social Contract, or Principles of Political Right* (original title Du contrat social: ou principes du droit politique), p. 1762.

Rossi Dal Pozzo F., *La giurisprudenza della Corte di Giustizia sul trattamento dei dati personali,* in *Annali AISDUE I*, 2020, pp. 63-86.

Rossi Dal Pozzo F., Zoboli L., *To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within the EU,* in *Eurojus,* 2021, pp. 315-330.

Rueckert C., *Cryptocurrencies and fundamental rights*, in *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, pp. 1-12.

Rundle M., Blakley B., Broberg J., Nadalin A., Olds D., Ruddy M., Trevithick P., *At a crossroads: "personhood" and digital identity in the information society*, STI Working Paper 2007/07, Organisation for Economic Co-operation and Development (OECD), 2007.

Samonte M., *Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law,* in *European Papers*, 2019, pp. 839-851

Sapkota N., Grobys K., *Blockchain Consensus Protocols, Energy Consumption and Cryptocurrency Prices,* in *Journal of Energy Markets,* 2021, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3778604.

Sartor G., *Human Rights and Information Technologies*, in R. Brownsword, E. Scotford,

Satchell C., Shanks G., Howard S., Murphy J., *Identity crisis: User perspectives on multiplicity and control in federated identity management,* in *Behaviour and Information Technology*, 2011, pp. 51–62.

Sater S., *Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows, Tulane University*, 2017.

Saurabh K., Rani N., Upadhyay P., *Towards Blockchain led decentralized autonomous organization (DAO) business model innovations*, in *Benchmarking*, 2022.

Schar F., Berentsen A., *Bitcoin, Blockchain and cryptoassets*, The MIT Press, 2020, p.1-288.

Schartner P., M. Schaffer, *Unique user-generated digital pseudonyms*, in *International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, Springer, 2005, pp. 194–205.

Schepisi C., *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *Quaderni AISDUE*, 2022, pp. 330-356.

Schmelz D., Fischer G., Niemeier P., Zhu L., Grechenig T., *Towards Using Public Blockchain in Information-Centric Networks: Challenges Imposed by the European Union's General Data Protection Regulation*, in *2018 1st IEEE International Conference on Hot Information-Centric Networking*, 2018, pp. 223-228.

Schonberger V., *The Shape of Governance: Analyzing the World of Internet Regulation,* in *Virginia Journal of International law*, 2003, pp. 606- 674.

Schradie J., *The Revolution that Wasn't*, Cambridge, MA: Harvard University Press, 2019.

Schrepel T., *Anarchy, State, and Blockchain Utopia: Rule of Law vs Lex Cryptographia,* in *General Principles and Digitalisation*, Hart Publishing, 2020.

Schrepel T., *Blockchain: from ideology to implementation*, in *Blockchain + Antitrust,* 2021, pp. 1-304.

Schwalm S., Alamillo-Domingo I., *Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0*, in *European Review of Digital Administration & Law*, 2021, pp. 89-108.

Schwerin S., *Blockchain and Privacy Protection in the Case of The European General Data Protection Regulation (GDPR): A Delphi Study*, in *The Journal of The British Blockchain Association*, 2018, pp. 1-75.

Schwerin S., *Blockchain and privacy protection in the case of the European general data protection regulation (GDPR): a Delphi study*, in *The Journal of the British Blockchain Association*, 2018.

Scott J., Trubek D., *Mind the Gap: Law and New Approaches to Governance in the European Union,* in *European Law Journal,* 2002, pp. 4–6

Sell F. G, Martin-Bariteau F., *The impact of Blockchains for Human Rights, Democracy and*
Senden L. A. J., *Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?,* in *Electronic Journal of Comparative Law,* 2005.

Sharma T. K., *Advantages and disadvantages of permissionless Blockchain,* Blockchain Council, Oct. 3, 2018.

Simmons G.J., *Symmetric and asymmetric encryption*, in *Secure Communications and Asymmetric Cryptosystems*, Taylor and Francis, 2019, pp. 241–298.

Singh M., Kim S., *Blockchain technology for decentralized autonomous organizations*, in *Advances in Computers*, 2019, pp. 115–140.

Singhal B., Dhameja G., Sekha Panda P., *Beginning Blockchain – a beginner's guide to building Blockchain solutions*, Springer, 2018.

Smith D., *The challenge of federated identity management*, in *Network Security*, 2008, pp. 7–9.

Smits J. M., *What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644088, 2015.

Sobkow B., *Forget me, forget me not—redefining the boundaries of the right to be forgotten to address current problems and areas of criticism*, in Schweichhofer E. et al (eds), *Privacy technologies and policy, 5th Annual Privacy Forum*, APF 2017, Vienna, Austria, 7–8 June 2017, Revised selected papers, Springer.

Spindler G., Schmechel P., *Personal Data and Encryption in the European General Data Protection Regulation*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2016.

Spindler G., Schmechel P., *Personal Data and Encryption in the European General Data Protection Reglation*, in *Journal of Intellectual Property, Info Tech, and e-commerce L. 163*, 2016.

Stalla-Bourdillon S., Knight A., *Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsis International Law Journal*, 2016, pp.285-322.

Stazi A., *Smart Contracts: Elements, Pathologies and Remedies*, in Loo J., Remolina Leon N. (eds), *Law and Change: An Asian Perspective*, SMU, 2022.

Steichen M., Beltran F., Norvill R., Shbair W., State R., *Blockchain-based, decentralized access control for IPFS*, in *IEEE International Conference on Blockchain*, 2018.

Stilinovic M., Hutchinson J., *The Internet regulation turn? Policy, Internet and technology*, in *Policy and Internet*, 2022, pp.6-12.

Stokkink Q., Pouwelse J., *Deployment of a Blockchain-Based Self-Sovereign Identity*, in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1336-1342.

Strohminger N., Knobe J., Newman G., *The true self: a psychological concept distinct from the self*, in *Perspective on Psychological Sci*ence, 2017, pp. 551–560.

Suh J., Horvitz E., White R. W. et al, *Disparate impacts on online information access during the Covid-19 pandemic,* in *Nature Communication*, 2022, pp. 1-15.

Suler J. R., *Identity management in cyberspace*, in *Journal of Applied Psychoanalytic Stud*ies, 2002, pp. 455–459.

Swand M., De Filippi P., *Toward a philosophy of Blockchain: A symposium, Introduction*, in

Szabo N., *Smart Contracts: Building blocks for digital markets*, 1996.

Szostek D., *Blockchain and the law*, Nomos, 2019, pp.1-160.

Taherdoost H., *Non-fungible tokens (NFT): A systematic review,* in *Information,* 2023, pp. 1-12, https://www.sciencedirect.com/science/article/pii/S8755461518300598

Tamburri D. A., *Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation*, in *Information Systems*, 2020, p. 91.

Tapscott D., Tapscott A., *Blockchain revolution*: *How the technology behind bitcoin is changing money, business, and the world,* New York: Penguin, 2016.

Tatar U., Gokce Y., Nussbaum B., *Law versus technology: Blockchain, GDPR, and tough tradeoffs*, in *Computer Law & Security Review*, 2020, pp. 1-11

Teichmann F. M. J., Boticiu S.R., Sergi B.S., *The EU MiCA Directive – chances and risks from a compliance perspective*, in *Journal of Money Laundering Control*, 2023.
the Rule of Law, Council of Europe, 2022.

Tian G., Wei J., Kutylowski M., Susilo W., Huang X., Chen X., *VRBC: A Verifiable Redactable Blockchain with Efficient Query and Integrity Auditing*, in *IEEE Transactions on Computers*, 2023, pp. 1928–1942.

Tobin A., Reed D., *The inevitable rise of self-sovereign identity*, Provo: The Sovrin Foundation, 2016.

Toth K., Subramanium M., *The persona concept: a consumer-centered identity model*, in *3rd International Workshop on Emerging Applications for Wireless and Mobile Access*, 2003.

Tranter K., *Disruptive technology disruptive law*, in *Law, Culture and the Humanities*, 2021, Vol. 17(2), pp. 158–170.

Treiblmaier H., Umlauff U., *Blockchain and the future of work: A self-determination theory approach*, in Swan M., Potts J., Takagi S., Tasca P., Witte F. (Eds.), *Blockchain economics: Implications of distributed ledger technology*, New Jersey, 2019, pp. 105-124.

Trotter G., *Autonomy as self-sovereignty*, in *HEC Forum*, 2014, pp. 237–255.

Tso R., *A new way to generate a ring: Universal ring signature*, in *Computer & Mathematics with Applications*, 2013, pp. 1350–1359.

Tyagi S. S., Bhathia S., *Blockchain for business: how it works and creates values*, Wilei, 2021, p. 1-400.

Van Alsenoy B., Heyman R., *The GDPR and the free flow of personal data outside the EU: Towards a human-centric approach to international data transfers*, in *Computer Law & Security Review*, 2019, pp. 35-51.

Van Blarkom G. V., Borking J.J., Olk J.G.E., *Handbook of Privacy and Privacy-Enhancing Technologies*, College bescherming persoonsgegevens, 2003.

Van de Waerdt P. J., *Information asymmetries: recognizing the limits of the GDPR on the data-driven market*, in *Computer Law and Security Review*, 2020.

Van der Jeught S., *Current practices with regard to the interpretation of multilingual EU Law: how to deal with diverging language versions?* in *European Journal of Legal Studies*, 2018, pp. 5-38.

Van der Laan J., *Understanding Blockchain*, in M. Aztzt, T. Richter (eds), *Handbook of Blockchain Law: a guide to understanding and resolving the legal challenges of the Blockchain technology*, Kluwer Law International, 2022, p. 29.

Van der Linden T., Shirazi T., *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, in *Financial Innovation*, 2023.

Van Eecke P., Haie A.-G., *Practitioner's corner • Blockchain and the GDPR: the EU Blockchain observatory report*, in *European Data Protection Law Review*, 2018, pp. 531-534.

Van Geelkerken F.W.J., Konings K., *Using Blockchain to strengthen the rights granted through the GDPR*, in *7th International youth science forum «Litteris et Artibus»*, Ukraine, 2017, pp. 458–461.

Van Hoecke M., *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?*, Oxford Hart Publishing, 2011.

Van Humbeeck A., *The Blockchain-GDPR paradox,* in *Journal of Data Protection and Privacy*, *2*(3), 2019, pp. 208–212.

Van Meerbeeck J., *The Principle of Legal Certainty in the Case Law of the European Court of Justice: From Certainty to Trust*, in *European Law Review*, 2016, p. 282

Vismann C., *Files: Law and Media Technology,* Stanford University Press, 2008.

Vogel H.L., *Disruptive Technologies and Disruptive Thinking,* in *Michigan State Law Review*, 2005.

Voigt P., von dem Bussche A., *The EU general data protection regulation (GDPR): a practical guide*, Springer, 2017.

Voss A., *Fixing the GDPR: Towards Version 2.0*, 2021, https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf.

Wacker M., *The EU General Data Protection Regulation (GDPR): Implications for international data flows and the global data protection regime,* in *International Data Privacy Law*, 2017, pp. 67-75.

Wagner J., *The transfer of personal data to third countries under the GDPR: When does a recipient country provide an adequate level of protection?*, in *International Data Privacy Law*, *8*(4), 2018, pp. 318–337.

Wagner K., Nemethi B., Renieris E., Lang P., Brunet E., Holst E., *Self-sovereing identity. A position paper on Blockchain enabled identity and the road ahead*, Berlin: Blockchain Bundesverband, 2018.

Walch A., *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains,* in

Walters N. , *Privacy law issues in Blockchains: an analysis of PIPEDA, the GDPR, and proposals for compliance*, in *Canadian Journal of Law and Technology*, 2019, pp. 276-305.

Wang F., De Filippi P., *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, in *Frontiers in Blockchain*, 2020.

Wang S., Ding W., Li J., Yuan Y., Ouyang L., Wang F.Y., *Decentralized Autonomous Organizations: Concept, Model, and Applications*, in *IEEE Transactions on Computational Social Systems*, 2019, pp. 870–878.

Ward S., *Blockchain to Clash with New EU Privacy Law*, 2018, www.bestvpn.com/privacy-news/Blockchain-clash-new- eu-privacy-law.

Weber R. H., "*Rose is a rose is a rose is a rose" – what about code and law?'*, in *Computer Law & Security Review*, 2018, p. 701-706.

Webster J., Watson R. T., *Analyzing the past to prepare for the future: Writing a literature review*, in *MIS quarterly*, 2002, xiii-xxiii.

Werbach K., Cornell N., *Contracts ex machina*, in *Duke Law Journal*, 2017, pp. 313-382

Werbach K., *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, in *Florida Law Review*, 2017.

Werbach K., *Trust, but verify*, in *Barkeley Technology Law Journal*, 2018, pp.487-550.

Werbach K., *Blockchain and the New Architecture of Trust*, MIT Press, 2019, pp.1-344.

Werth J., Berenjestanaki M., Barzegar H.et al, *A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma*, in *International Conference on Enterprise Information Systems, ICEIS – Proceedings*, 2023, pp. 146-155.

Winner L., *Whale and the Reactor*, University of Chicago Press, 1986.

Winnowicz K., Cam-Duc A., Stein D., *Crypto Regulation within the European Union*, 2021, available at SSRN: https://ssrn.com/abstract=4194771.

Wirth C., Kolain M., *Privacy by Blockchain design: a Blockchain-enabled GDPR-compliant approach for handling personal data*, in *Proceedings of 1st ERCIM Blockchain Workshop*, 2018.

Won Eschenbach W. J., *Transparency and the Black Box Problem: Why We Do Not Trust AI,* in *Philosophy and Technology*, *34*(4), 2021 pp. 1607–1622.

Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia,* 10 March 2015.

Wrigley S., *"When people just click": Addressing the difficulties of controller/processor agreements online,* in M. Corrales, M. Fenwick, H. Haapio, (eds), *Legal Tech, Smart Contracts and Blockchain,* 2019, pp. 221-252.

X Rheingold A., *The Virtual Community,* MIT Press, 1994.

Xu J., Xue K., Tian H., Hong J., Wei D.S.L., Hong P., *An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks*, in *IEEE Transactions on Vehicular Technology*, 2020, pp. 6688–6698.

Xu M., Chen X., Kou G., *A systematic review of Blockchain*, in *Financial Innovation*, 2019, pp. 1-14.

Xu X. et al., *Architecture for Blockchain Applications*, Springer Nature Switzerland, 2019, pp. 1-329.

Yang A. Y. P., *When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?,* in *Stanford Journal of Blockchain Law & Policy*, 2023, available at https://stanford-jblp.pubpub.org/pub/jurisdiction-rules-Blockchain/release/1.

Yang Y., Wei L., Wu J., Long C., *Block-SMPC: a Blockchain-based secure multi-party computation for privacy-protected data sharing,* in *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology,* 2020, pp. 46–51.

Yeung K. (eds), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press, 2017, pp. 424-450-

Yeung K., *Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of law and Code as Law,* in *Modern Law Review*, 2019, p. 207.

Young A., *The European Union as a global regulator? Context and comparison,* in *Journal of European Public Policy*, 2015, pp. 1233–1252.

Yu B., Liu J., Sakzad A., Nepal S., Steinfeld R., Rimba P., Au M.H., *Platform-independent secure Blockchain-based voting system*, in *International conference on information security*, 2018.

Yu. Kurnykin O., *The Phenomenon of "Multiple Identity" in Modern Kyrgyz Society*, in *Izvestiya of Altai State University*, 2021, pp. 73–78.

Yuming L., *Sovereignty Blockchain 1.0 – Orderly Internet and Community with a Shared Future for Humanity*, Springer, 2021, pp.1-252.

Zaccaria A., Schmidt-Kessel M., Schulze R., Gambino A. M (eds.), *EU eIDAS-Regulation: Article-by-Article Commentary*, London, Bloomsbury Publishing, 2020.

Zarsky T. Z., *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 2017.

Zeba S., Suman P., Tyagi K., *Types of Blockchain*, in *Distributed Computing to Blockchain: Architecture, Technology, and Applications*, pp. 55–68.

Zednik C., *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*, in *Philosophy and Technology*, 34(2), 2021, pp. 265–288.

Zemler F. , *Concepts for GDPR-compliant processing of personal data on Blockchain: a literature review*, in *Anwendungen und Konzepte der Wirtschaftsinformatik*, 2019, pp. 96-107.

Zemler F., Westner M., *Blockchain and GDPR: Application scenarios and compliance requirements*, in *Proc. Portland Int. Conf. Manage. Eng. Technol (PICMET)*, 2019, pp. 1–8.

Zetzsche A. D., Buckley P. R., Douglas W. A., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, in *University of Illinois Law Review* 2017, no. 5, 2017,

Zhao D., *Application and Development Trend of Blockchain in the Financial Field*, in *Advances in Intelligent Systems and Computing*, Springer, 2021, pp. 558–564

Zhao Y., Kang X., Li T., Chu C. K., Wang H., *Toward Trustworthy DeFi Oracles: Past, Present, and Future*, in *IEEE Access*, 2022, pp. 60914–60928.

Zheng Z. et al, *An overview on smart contracts: Challenges, advances and platforms*, in *Future Generation Computer Systems*, 2020, pp. 475-491.

Zheng X. et al, *Blockchain-based personal health data sharing system using cloud storage*, in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services*, 2018, pp. 1-6

Zheng Z., Xie S., Dai H., Chen X., Wang H., *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress,* 2017, pp. 557–564.

Zook M., Blankenship J., *New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance,* in *Geoforum*, 2018, p. 248-255.

Zou M., *Code: and other laws of Blockchain,* https://ora.ox.ac.uk/objects/uuid:7af6d923-07fa-4eb6-8340-e05205f7b4ee/download_file?file_format=pdf&safe_filename=Zou_2020_Code_laws_Blockchain.pdf&type_of_work=Journal+article

Zuiderveen B., *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation,* in *Computer Law & Security Review,* 2016.

Zwitter A., Hazenberg J., *Decentralized Network Governance: Blockchain Technology and the Future of Regulation*, in *Frontiers in Blockchain*, 2020, pp.1-12.

Table of Cases

European Union

Joined Cases 6/73 and 7/73, *Istituto Chemioterapico Italiano and Commercial Solvents* v *Commission*, EU:C:1974:18.

Case 30/77, *Regina v Pierre Bouchereau,* EU:C:1977:172.

Case 44/79, *Hauer*, EU:C:1979:290.

Case 283/81, Cilfit, EU:C:1982:335.

Case C-352/85, *Bond van Adverteerders and Others vs. The Netherlands State*, EU:C:1988:7.

Case C-41/90, *Höfner and Elser*, EU:C:1991:161.

Joined Cases C-159/91 and C-160/91, *Poucet and Pistre*, EU:C:1993:63.

Case C-109/92, *Wirth,* EU:C:1993:312.

Case C-218/00, *Cisal*, EU:C:2002:36.

Case C-101/01, *Bodil Lindqvist,* EU:C:2003:596.

Joined Cases C-465/00, C-138/01 and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann*, EU:C:2003:294.

Case C-110/03, *Belgium v Commission*, EU:C:2005:223.

Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission of the European Communitie,* EU:C:2006:346.

Case C-49/07, *MOTOE,* EU:C:2008:376.

Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,* EU:C:2008:727.

Case C-553/07, *Rijkeboer*, EU:C:2009:293.

Case C-28/08P, *European Commission v Bavarian Lager*, EU:C:2010:378.

Case C-201/08 *Plantanol GmbH & Co KG v Hauptzollamt Darmstadt*, EU:C:2009:539.

Case C-351/08, *Grimme,* EU:C:2009:697.

Joined Cases C-585/08 and C-144/09, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG (C-585/08) & Hotel Alpenhof GesmbH v. Oliver Heller,* EU:C:2010:273.

Joined Cases C-92/09 and 93/09, *Schecke,* EU:C:2010:662.

Case C-70/10, *Scarlet Extended,* EU:C:2011:771Case C-72/10 *Criminal proceedings against Costa*, EU:C:2012:80.

Case C-617/10, *Åkerberg Fransson*, EU:C:2013:105.

Case C-399/11, *Melloni*, EU:C:2013:107.

Case C-558/11, *Kurcums Metal,* EU:C:2012:721.

Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* EU:C:2014:31.

Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland,* EU:C:2014_238.

Case C-342/12, *Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT),* EU:C:2013:355.

Case C-74/13, *GSV,* EU:C:2014:243.

Case C-206/13, *Siragusa,* EU:C:2014:126.

Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, EU:C:2014:2428.

Case C-201/14, *Bara,* EU:C:2015:461.

Case C-230/14, *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság Weltimmo v NAIH,* EU:C:2015:426.

Joined cases C-443/14, *Ibrahim Alo* and C-444/14, *Amira Osso,* EU:C:2016:127.

Case C-362/14, *Schrems,* EU:C:2015:650.

Case C-191/15, *Verein fuř Konsumenteninformation v. Amazon EU Sàrl*, EU:C:2016:388.

Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for Home Department v Tom Watson and Others*, EU:C:2016:970.

Case 29/16, *Erich Stauder v City of Ulm, Sozialamt*, EU:C:1969:57.

Case C-48/16, Ergo Poist'ovňa EU:C:2017:377.

Case C-73/16, *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy*, EU:C:2017:725.

Case C-207/16, *Ministerio Fiscal*, EU:C:2018:788.

Case C-210/16, *Wirtschaftsakademie*, EU:C:2017:796.

Case C-404/16, *Lombard Ingatlan Lízing*, EU:C:2017:759.

Case C-434/16, *Nowak*, EU:C:2017:994.

Opinion of AG Kokott in Case C-434/16 *Peter Nowak*, EU:C:2017:582.

Case C-25/17, *Proceedings brought by Tietosuojavaltuutettu (Jehovan todistajat*, EU:C:2018:551.

Case C-40/17, *Fashion ID,* EU:C:2019:629.

Case C-136/17, *GC and Others (De-referencing of sensitive data)*, EU:C:2019:773.

Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others,* EU:C:2020:790.

Case C-507/17, *Google,* EU:C:2019:772.

Joined Cases C-59/18 and C-182/18, *Italy and Comune di Milano* v *Council (Seat of the European Medicines Agency)*, EU:C:2022:567.

Case C-311/18, *Schrems II*, EU:C:2020:559.

Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064.

Case C-272/19, *Land Hessen,* EU:C:2020:535.

Case C-422/19 and C-423/19, *Hessischer Rundfunk*, EU:C:2021:63.

Case C-439/19, *Latvijas Republikas Saeima* (Penalty points), EU:C:2021:504.

Opinion of the Advocate General Pitruzzella in case *Sumal, S.L. v Mercedes Benz Trucks España, S.L.*, C-882/19, EU:C:2021:293.

Case C-175/20, Valsts ieņēmumu dienests (Processing of personal data for tax purposes), EU:C:2022:124.

Case C-245/20, *Autoriteit Persoonsgegevens*, EU:C:2022:216.

Case T-557/20, *Single Resolution Board v European Data Protection Supervisor,* EU:T:2023:219.

Case C-77/21 *Digi Távközlési és Szolgáltató Kft. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, , EU:C:2022:805.

Case C-268/21, *Norra Stockholm Bygg,* EU:C:2023:145.

Opinion of the Advocate General Jacobs in joined cases Joined cases C-264/01, C-306/01, C-354/01 and C-355/01 *AOK Bundesverband and Other,* EU:C:2003:304.

European Court of Human Rights

Judgement of the ECtHR of 16 February 2000, *Amann v. Switzerland,* no.27798/95.

Judgement of the ECtHR of 25 February 1997, *Z v Finland, no. 22009/93.*

Judgement of the ECtHR of 4 May 2000, *Rotaru v. Romania,* no. 28341/95.

Reports

B. Wynne et al., *Taking European Knowledge Society Seriously*, Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission, Luxembourg: Office for Official Publications of the European Communities, 2007.

C. Di Bernardino, A. Chomczyk Penedo, J. Ellul, A. Ferreira, A. von Goldbeck, R. Herian, A. Siadat, N. L. Siedler, *NFT - Legal Token Classification*, July 22, 2021, EU Blockchain Observatory and Forum NFT Reports.

CEN/CENELEC, *Workshop Agreement, Digital Sovereignty - European perspectives, general approach, and implications on standardisation*, June 2023.

Commission Nationale de l'Informatique et des Libertés, *Solutions for a Responsible use of Blockchain in the context of Personal data*, 2018.

D. Yaga, P. Mell, N. Roby, K. Scarfone, *Blockchain Technology Overview*, Draft NISTIR US Department of Commerce, National Institute for Standards and Technology, 2018.

Decentralization: A Sampling of Definitions, Working Paper by UNDP, 1999.

Distributed Ledger Technology: beyond block chain - A report by the UK Government Chief Scientific Adviser, 2016.

ENISA, *Data Protection Engeneering – From theory to practice,* January 2022.

European Blockchain Observatory and Forum (EUBOF), *PoW Energy Consumption in EU*, 1 November 2022.

European Commission, *Blockchain in practice – Promoting Blockchain and DLTs in European SMEs*, June 2021.

European Investment Bank, *Artificial intelligence, Blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy,* June 2021.

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, 2018.

International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services – Rome Memorandum*, 2008.

ICO, *Overview of the General Data Protection Regulation (GDPR)*, 2017.

ISDA, Clifford Chance, R3, *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology*, October 2020, https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/Private-International-Law-Aspects-of-Smart-Contracts-Utilizing-Distributed-Ledger-Technology-New-York-Law.pdf.

ISO, *Blockchain and Distributed Ledger Technologies, Guidelines for governance*.

Joint paper of the Spanish data protection authority, Agencia española de protección de datos (AEPD), and the European Data Protection Supervisor (EDPS) on hash techniques in data processing activities as a safeguard for personal data', October 2019.

P. de Filippi, G. McMullen, *Governance of Blockchain Systems: Governance of and by Distributed Infrastructure*, in *Blockchain Research Institute and COALA Research Report*, 2018.

S. Nascimento et al, *Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*, Publications Office of the European Union, Luxembourg, 2019.

T. Schrepel, *Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach*, Study for the European Commission.

V. Dieterich, M. Ivanovic, T. Meier, S. Zäpfel, M. Utz, P. Sandner, *Application of Blockchain technology in the manufacturing industry,* Working Paper, Frankfurt School Blockchain Center, 2017.

W. Crumpler et al, *The Human Rights risks and opportunities in Blockchain,* A Joint Report of the CSIS Strategic Technologies Program and Human Rights Initiative, 2021.

World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 2011.

World Economic Forum, *Reimagining Digital ID*, 2023.

Newspaper Articles and Blog Articles

A. Abbas, *What is Determinism in a Blockchain Network? —* Alacrity Network, 2020, https://medium.com/@adilsvp/what-is-determinism-in-a-Blockchain-network-alacrity-network-5d1f58449779.

David D. Clark, *A Cloudy Crystal Ball*, Visions of the Future, plenary presentation, 24th meeting of the Internet Engineering Task Force, Cambridge, MA, 13–17 July 1992, http:/ietf20.isoc.org/videos/future_ietf_92.pdf.

E. Hughes, *A Cypherpunk's Manifesto*, 1993, https://www.activism.net/cypherpunk/manifesto.html

ECB, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, Occasional Paper nr. 223/2019, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf?a31360223fb32f0e50a82ce649a8b7fc.

F. Martin-Bariteau, *Blockchain and the European Union General Data Protection Regulation: the CNIL's Perspective*, Working Paper, Blckchn.ca, 2018

J.P. Barlow, *A Declaration of the Independence of Cyberspace*, 8 February 1996.

M. Orcutt, *States that are passing laws to govern "smart contracts" have no idea what they're doing*, 29 March 2018, https://www.technologyreview.com/2018/03/29/144200/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/

P. Vigna, *Chiefless Company Rakes In More Than $100 Million*, *https://www.wsj.com/articles/chiefless-company-rakes-in-more-than-100-million-1463399393*.

R. McDougall, *Are NFTs Dead?*, in *MarketPlace Fairness*, October 2023, https://www.marketplacefairness.org/cryptocurrency/are-nfts-dead/.

T. May, The Crypto Anarchist Manifesto, 1992, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.

V. Buterin, The meaning of decentralization, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

European Union Legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

European Commission, *Interinstitutional Agreement on Better Law-Making*, 2003, OJ C 321/01.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, L. 316/12.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241.

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89-131.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 *on a framework for the free flow of non-personal data in the European Union*, OJ L 303 p.59-68.

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 910/2014 as regards establishing a framework for a European Digital Identity, COM (2021)281 final.

Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence and amending certain Union legislative acts, COM(2021)206 final.

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance), OJ L 151 of 2.6.2022, p. 1–33.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data, COM(2022)68 final

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/101.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM(2023) 348 final

Proposal for a Regulation of the European Parliament and of the Council, on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

Documents

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981.

Article 29 Working Party, Opinion 4/2007 *on the concept of personal data*, WP 136, June 20, 2007.

Article 29 Data Protection Working Party, Opinion 5/2009 on *Online Social Networking*, 12 June 2009.

Article 29 Working Party, *Opinion 3/2010 on the Principle of Accountability*, WP 173, 13 July 2010.

Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice*, November 2012.

Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, WP 196.

Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, adopted on 23/09/1980 and amended on 11/07/2013.

Article 29 Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, WP 215.

Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP 216.

Article 29 Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, WP 223.

Article 29 Working Party, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain*, 2015.

Article 29 Working Party, *Guidelines on the Right to Portability*, WP 242 rev.01, 5 April 2017.

European Parliament resolution of 3 October 2018 *on distributed ledger technologies and Blockchains: building trust with disintermediation,* P8_TA(2018)0373.

European Parliament resolution of 13 December 2018 *on Blockchain: a forward-looking trade policy,* P8_TA(2018)0528).

EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation*, Nov. 12, 2019.

Commission Nationale Informatique & Libertés, *Blockchain: Solutions for a responsible use of the Blockchain in the context of personal data*, 6 November 2018.

A29 WP, *Guidelines on Automated Individual Decision-Making and Profiling*, 2018.

EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, adopted on 4 May 2020.

EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, adopted on 7 July 2021.

EDPB, *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, adopted on 14 February 2023.

EDPB, *Guidelines 07/2022 on certification as a tool for transfers*, adopted on 14 February 2023.

Council Conclusions on EU Digital Diplomacy, 26 June 2023.