Blockchain and eHealth: seeking compliance with the General Data Protection Regulation

*Marta Arisi, Paolo Guarda**

BLOCKCHAIN AND EHEALTH: SEEKING COMPLIANCE WITH THE GENERAL DATA PROTECTION REGULATION

ABSTRACT: The blockchain ecosystem meets the GDPR in the healthcare sector, where its impact is widely debated. To debunk the narrative of contrast, a complexity of applications is displayed, and the legal background is outlined, introducing the matter of governance and compliance with GDPR principles, rights and obligations. Although this work cannot dispel the uncertainties in the application of GDPR rules to blockchains, such as the one regarding the right to erasure, and given the issues elected for further study, we focus on the room for compliance arising from the diverse potential of this technology, which can be shaped according to different architectural choices.

KEYWORDS: Blockchain; GDPR; eHealth; right to erasure; anonymization

1. Introduction: Law, Technology and Blockchain

Legal matters have always been intrinsically linked to technology. The relationship is one-to-one. An innovation in the field of technology affects the social context and therefore requires a legal response to the new needs that have come about. This assumption is confirmed by the diachronic analysis of many legal institutions: origins of Intellectual Property Rights[1], development of privacy and personal data protection regulation[2], etc. But the same technology is affected by this dialogue and comparison: it attempts, indeed, to respond to social needs and to interact with the legal world in order to find solutions that comply with the regulatory provisions (e.g. the so called privacy

[*] Marta Arisi: Law Graduate from the Faculty of Law – University of Trento, currently working as an Analyst in the field of Data Protection. Mail: marta.arisi@alumni.unitn.it, authored paragraphs 2, 3 and 4; Paolo Guarda: Assistant Professor of Comparative Private Law at the Faculty of Law – University of Trento. Mail: paolo.guarda@unitn.it, authored paragraphs 1 and 5. We gratefully acknowledge our debt to the "Security & Trust" and the "eHealth" Research Units within Fondazione Bruno Kessler, and to the Competence Center on Digital Health "TrentinoSalute4.0" for the support received for our research. In this respect, we would like to expressly quote and thank Dr. Silvio Ranise, Dr. Alessandro Tomasi and Dr. Umberto Morelli for their valuable feedback. All errors remain our own.

[1] See among others R. CASO, F. GIOVANELLA (eds.), *Balancing Copyright Law in the Digital Age*, Berlin and Heidelberg, 2015; S. STOKES, Digital Copyright, 4th, Oxford, 2014; U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico*, Roma, 2010.

[2] See F. GIOVANELLA*, Copyright and Information Privacy*. *Conflicting Rights in Balance*, Cheltenham, 2017, 138-152.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

by design approach)[3], sometimes to avoid and bypass the censorship that the regulatory and judicial systems have tried to affirm (see the history of the evolution of P2P online sharing platforms)[4].

Whenever a new technology asserts itself (or rather becomes of widespread use) and one plans to adopt it in the various application scenarios, the first question that spontaneously arises is whether it still complies with the legal rules provided or if it represents a break from the established framework. Within the context of digital age law, the normative data, then, is often a victim of its early obsolescence. Jurists are therefore asked to find a solution that fits into a legal tradition made up of fundamental principles and detailed rules. They are called upon to show off "creativity", while staying within the framework of a strictly codified and typed system, in order to demonstrate how much they can truly be the ones who are capable of building bridges between types of knowledge and bringing unity and compromise to requests deriving from different plans and opinions[5].

The advent of the so called blockchain confirms what has been written before[6]. We are dealing here with a technological solution, to tell the truth already known for years to a small and closed circle of "experts", which promises to overcome some of the typical problems of the "old" context. Over the years, from centralized registry systems we have moved to decentralized and up till now completely distributed ones, where there is no longer a centre and the logic of governance is built around a new concept of trust between all subjects: we refer to this as a "distributed ledger". This kind of architecture means that the database is not physically located on a single server, but actually resides on multiple computers at the same time, all perfectly synchronized. The Blockchain technology offers some attractive advantages: the immutability of the register (or at least the tendential immutability of the same for the reasons that will be discussed below); total traceability of transactions, with clear benefits in terms of process transparency; security, based on cryptographic technologies; decentralization, typical of a distributed system, which reduces the risk of data loss; the "consensus" rule, a new concept of "trust" but perhaps also a new form of "democracy".

The moments of tension and the clashes with the legislation on the protection of personal data are obviously numerous and not easy to solve. Thus, this paper aims to provide first answers to some of the questions just raised. After this brief introduction, the second paragraph will be dedicated to an initial description of what is meant by blockchain; this without any pretence of completeness, but attempting to offer even the non-expert reader a basic overview of the technological phenomenon: therefore, the "history" of the blockchain, of its various possible variations, of the fundamental differences that exist between public and private, permissioned and permissionless blockchain, will be taken into account. The third paragraph, furthermore, will be devoted to testing the "tightness" of this

[3] On privacy by design, see A. CAVOUKIAN, *Privacy by design: the definitive workshop - A foreword by Ann Cavoukian*, in *Identity Info.* Soc'y, 3, 2010, 247-251; B.J. KOOPS, R.E. LEENES, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data Protection Law*, *International Review of Law Computers & Technology* 28, 1-2013.

[4] See F. GIOVANELLA, *op. cit.*, 210-218.

[5] For an interesting study that singles out and describes the cognitive techniques employed when lawyers are called to answer old and new problems, see G. PASCUZZI, *Cognitive Techniques of Legal Innovation*, in G. BELLANTUONO, F.T. LARA (eds.), Law, *Development and Innovation*, Heidelberg, 2015, 15-23.

[6] For a first reference analysis on legal issues related to blockchain, see M. FINCK, *Blockchain regulation and governance in Europe*, Cambridge, 2019.

innovation with reference to the traditional (even if recently renewed) rules on the protection of personal data, now set at the European level by the General Data Protection Regulation (hereinafter: GDPR)[7]: the main aspects of the regulatory framework will be described with particular attention to the most critical issues (material and territorial scope, definition of personal data, governance of privacy roles, exercising of rights). In order to be able to apply a truly detailed legal analysis to a real operating context, this paper tries to go beyond the level of pure theoretical exercise, and calibrate the reflections on a peculiar and complex application scenario, analysing the possible adoption of blockchain solutions in eHealth (paragraph 4). The conclusions will finally try to sum up what has been described and to propose providing tools to understand, in this particular area of investigation, the traditional relationship between law and technology.

2. Blockchain in a nutshell

Blockchains shall be understood as rooted in the Cypherpunk movement: at the end of the 1980s, inspired by libertarian ideas, *crypto rebels*[8] were fighting for social equality and the right to privacy in the electronic age, by means of encryption and code. Digital cash systems were at the forefront of cypherpunks' projects[9] and Satoshi Nakamoto, the anonymous inventor(s?) of *Bitcoin*[10], can be considered the cypherpunk genius who was able to continue the movement's legacy. Nonetheless, the impact of the most popular cryptocurrency in the world is not to be measured only in terms of the success of the currency itself: *Bitcoin* unlocked the advent of new digital infrastructures characterized by decentralization, transparency and tamper-resistance, embodied in the notion of blockchain, or *blockchain technology*[11]. In this work, as we try to challenge the lack of lexical accuracy for the richness

[7] The European regime on personal data protection is now established by Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). As a first point of reference for further information, see, among others, C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler (eds.), *The EU General Data Protection Regulation: a Commentary*, Oxford, 2020; with regards to Member States implementation, see B. Custers, A.M. Sears, F. Dechesne, O. Georgieva, T. Tani, S. van der Hof (eds.) *EU Personal Data Protection in Policy and Practice*, The Hague, 2019.

[8] S. Levy, *Crypto Rebels*, in *Wired*, Issue 2, 1993, in: https://www.wired.com/1993/02/crypto-rebels/ (last visited 06/04/2020). See examples of Cypherpunks' manifesto: T. May, *Crypto Anarchist Manifesto*, 1988, in: https://www.activism.net/cypherpunk/crypto-anarchy.html (last visited 06/04/2020); E. Hughes, *A Cypherpunk Manifesto*, 1993, in: https://www.activism.net/cypherpunk/manifesto.html (last visited 06/04/2020).

[9] P. De Filippi, A. Wright, *Blockchain and the Law: the rule of code,* Cambridge, Massachusetts, 2018, 18-20. This contribution displays in an exhaustive manner the bond between the Cypherpunk movement, Bitcoin and the current evolutions of blockchain. Examples of the mentioned projects are: D. Chaum, *Blind Signatures for Untraceable Payments*, 1982, in: https://chaum.com/publications/Chaum-blind-signatures.PDF (last visited 06/04/2020); W. Dai, *B-Money*, 1998, in: http://www.weidai.com/bmoney.txt (last visited 06/04/2020); H. Finney, *RPOW - Reusable Proof of Work*, 2014, in: https://nakamotoinstitute.org/rpow/ (last visited 06/04/2020); N. Szabo, *BitGold*, 2005, in: https://nakamotoinstitute.org/bit-gold/ (last visited 06/04/2020).

[10] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, in: https://bitcoin.org/bitcoin.pdf (last visited 06/04/2020).

[11] The notion of blockchain as a technology (often the technology "behind Bitcoin") is debated. On the definition of blockchain as a technology see the work of S. Davidson, P. De Filippi, J. Potts, *Blockchain and the economic institutions of Capitalism,* in *Journal of Institutional Economics*, Vol. 4, Issue 14, 2018, 642-643, in:

Downloaded from www.biodiritto.org.
ISSN 2284-4503

of the ecosystem[12], we elect the *blockchain ecosystem* as the term to refer to the complex interplay of actors and architectures engaged in its disruptive revolution[13] to proceed with the legal analysis.

A good initial step in defining blockchain might be to consider that Nakamoto found a combination of solutions that, altogether, made *Bitcoin* open access, transnational, optionally pseudonymous, transparent and tamper-resistant. Crucially, this appears to indicate that the different elements of the blockchain can be combined to respond to developers' and entrepreneurs' demands[14]. We only turn briefly to these characteristics. Amongst them, decentralization[15] has a vital role: while from a wider level it can be affirmed that in centralized databases, which are also typically proprietary, a central authority validates all the information and thus there could be a single point of failure, blockchains are counted among *distributed ledgers* where "the chain of blocks" identifies the data storage solution. This points to the consensus mechanism as the core notion for understanding this "architecture", because it explains how the nodes commit to the validation of the data independently from a central command within the network. There are several types of consensus[16]: the strategies may not be equal in terms of costs and present different deficiencies, such as speed limitations, and employment of computational power. Consequently, the scalability of blockchains – the capacity to change its size – is targeted as vital for future developments and this has been referred to as the *blockchain trilemma*[17]. The notions of private and public blockchain introduce us to the diversity of the ecosystem[18]. From

https://doi.org/10.1017/S1744137417000200 (last visited 06/04/2020); C. CATALINI, J.S. GANS, *Some simple Economics of the Blockchain*, Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191, 2017, in: https://ssrn.com/abstract=2874598 (last visited 06/04/2020); E. KANE, *Is Blockchain a General Purpose Technology?,* 2017, in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2932585 (last visited 06/04/2020).

[12] A. WALCH, *The Law of FinTech Symposium: The path of the Blockchain Lexicon (And the Law)*, 36 *Review of Banking & Financial Law*, 731 (2016), 4, also in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335 (last visited 06/04/2020).

[13] Inter alia, D. TAPSCOTT, A. TAPSCOTT, *Blockchain revolution: How the technology behind Bitcoin is changing money, business and the world*, London, 2016.

[14] For a comprehensive study, see M. PILKINGTON, *Blockchain Technology: Principles and applications,* 2015, in F.X. OLLEROS AND M. ZHEGUM (eds.), *Research Handbook on Digital Transformations*, Cheltenham, 2016, in: https://ssrn.com/abstract=2662660 (last visited 06/04/2020).

[15] The meaning of decentralization and distribution is debated, although Paul Baran's contribution is often proposed as conclusive: P. BARAN, *On distributed Communications Networks*, RAND Memoranda detailing the Distributive Adaptive Message Block Network Series, 1964, in: https://bit.ly/3dqEvmu (last visited 06/04/2020). However, a particularly useful perspective for our analysis is that of Vitalik Buterin, co-founder of Ethereum, according to whom when dealing with software centralization or decentralization should be analysed at the political, architectural and logical level. The author respectively refers to the possibility of splitting the system in parts, the infrastructural aspects (the number of physical computers the system is made of) and the possibility of controlling data. See V. BUTERIN, *The meaning of decentralization*, 2017, in: https://bit.ly/31q80Se (last visited 06/04/2020).

[16] Amongst them, Proof-of-Work (PoW) is accredited as it is the one applied in Bitcoin; Proof-of-Stake (PoS) or Proof-of-Identity (PoI) are well known alternatives.

[17] This means that in a blockchain a compromise between decentralization, security and scalability is unavoidable. See, inter alia, VV. AA., *On sharding blockchains*, 2018, in: https://bit.ly/2Z8lGyo (last visited 06/04/2020).

[18] See, inter alia, V. BUTERIN, *On public and private blockchains,* 2015, in: https://bit.ly/2CMWVk2 (last visited 06/04/2020).

public blockchains founded upon the idea of open participation and independence from a central authority, as companies and developers embarked on the blockchain venture, several of them decided to restrict access and/or write permission to the network, imposing some rules in the protocol and leading to what are called, despite different synonyms*, private blockchains*. Although the generalisability on this issue is problematic, this term embodies environments where a degree of control is (re)introduced. Blockchain "evangelists" claim that the absence of a central command is the essential feature of blockchain but the concept of private blockchain is, as a matter of fact, layered. While seeking to explain the differences between a private and a public blockchain based on the scopes they would serve may suffer from some limitations, a reasonable approach to tackle this issue could be to consider "permissions"[19]. One first distinction comes with admittance and in this respect identification plays a crucial role, since the protocol may require disclosure of information to participate in the network. Permission of writing means instead that participation to the consensus protocol and validation activity can be restricted to selected participants.

These notions are beneficial in understanding transparency, which is of the utmost importance for the functioning of blockchain and represents a fundamental trait of this work, as we investigate the privacy aspects of this technology. The great promise of blockchain is often said to reside in its transparency, which is why a lot of emerging applications aim to use blockchain in supply chain management or in the financial market. Still, herein the idea of blockchain as a place where data is necessarily correct dangerously fosters, because the blockchain itself does not grant the accuracy of the information[20]. More precisely, transparency can be ascribed to blockchain because of how data is validated (suggesting a strong relation to public blockchains) and, secondly, because of how data is shared in the network. This is how transparency is seen as a privacy deficiency for public blockchain[21] – it may be summed up that «decentralization comes at the price of transparency»[22]. For instance, in *Bitcoin* and *Ethereum* public ledger, details of the transactions, such as addresses, time and amount are disclosed[23], while for private blockchains it is suggested that information would be shared selectively, often according to specific rules, over an enclosed network. Importantly, all across the ecosystem, there is a growing interest in how to avoid disclosure of data in order to respond to the emerging data protection issue for blockchains[24].

[19] Despite their definition vary in the literature, *permissioned* and *permissionless* blockchains are also terms in use.

[20] P. De Filippi, A. Wright, *Blockchain and the Law: the rule of code*, cit., 114-115; A. J. Sulkowski, *Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers?,* 43 *Delaware Journal of Corporate Law* 303, 2019, 321-322.

[21] V. Buterin, *On public and private blockchains,* cit.

[22] P. De Filippi, *The interplay between decentralization and privacy: the case of blockchain technologies*, in *Journal of Peer Production*, Issue 7: Alternative Internets, 2016, 1, in: https://hal.archives-ouvertes.fr/hal-01382006 (last visited 06/04/2020).

[23] In its early stages, Bitcoin was even perceived as an anonymous cash system because of its deployment in online marketplaces, but users' identity can be linked to their public key, as the presence of public addresses grants mere pseudonymity; the choice is ultimately left to users.

[24] This can be achieved with a variety of techniques, e.g. Zero-Knowledge Proofs or ring signatures. See, inter alia, V. Buterin, *Privacy on the blockchain*, 2016, in: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ (last visited 06/04/2020); J. Wahab, *Privacy in Blockchain* Systems, 2018, in: https://arxiv.org/pdf/1809.10642.pdf (last visited 06/04/2020). A milestone in the research on this topic is the

Downloaded from www.biodiritto.org.
ISSN 2284-4503

In conclusion, despite different typologies, blockchains can be substantially described as ledgers and represent a new approach to building and using them. Since ancient times, ledgers have been used to represent data and reach agreement on the status of elements, when making transactions or managing rights[25]. Remarkably, the blockchain potential is that a shared global ledger can be trusted even in the absence of a central clearinghouse, due to modifications being proposed and approved by the participants themselves, thanks to the consensus mechanism. This has been defined as a new type of trust or even a *trustless system*[26]. Since *Bitcoin*, whose proposal of leaving aside the middlemen responded to the outrage of the financial crisis of 2008[27], the mechanics behind this ledger have been extracted and re-mixed and several implementations have departed from the original breakthrough of decentralization, for instance re-proposing a central authority, while hybrid instruments have empowered partial decentralization as well.

Within the emerging ecosystem, the idea of *building on blockchains* may be a simplification but might help to describe the user experience. A case in point is the importance of smart contracts, a notion coined by Nick Szabo[28], and related platforms, either public or private blockchains. Smart contracts may be defined as agreements which can run on a blockchain network according to some given rules written in code: they can resemble creation, execution and enforcement of a function, without the need of intermediaries and have attracted attention in the legal debate about blockchain. They shall be indeed considered at the core of every relationship engaged in the blockchain ecosystem[29], being possibly attached to both private and public contexts. On the other hand DOs and DAOs should also be mentioned as the organizations living autonomously on a blockchain, based on a smart contract and some *internal property*[30], while *decentralized applications* or, in short, *dapps,* have become the comprehensive term for several of the tools which are founded, also partially, upon a blockchain. They may offer some amount of transparency, resiliency, or lack of central control, depending on how they are architectured and to what extent they use the underlying blockchain, which would require correct

MIT Enigma Project: G. Zyskind, O. Nathan, A. S. Pentland, *Enigma: Decentralized Computation Platform with Guaranteed Privacy*, 2015, in: https://enigma.co/enigma_full.pdf (last visited 06/04/2020).

[25] S. Davidson, P. De Filippi, J. Potts, *Blockchain and the economic institutions of Capitalism* in *Journal of Institutional Economics*, cit., 642-643; K. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33. *Berkeley Technology Law Journal* 489, 2018, 501-502, also in: https://ssrn.com/abstract=2844409 (last visited 06/04/2020), citing inter alia Q. Du Pont, B. Maurer, *Ledgers and the law in the blockchain,* 2015, in: https://www.kingsreview.co.uk/qdpledgersandlaw (last visited 06/04/2020).

[26] This is a frequent expression, which K. Werbach, *op. cit.,* 500, refers to R. Hoffman, *Why the Blockchain Matters*, in *Wired*, the 15th of May 2015, in: https://www.wired.co.uk/article/bitcoin-reid _-hoffman (last visited 06/04/2020). See also *The trust machine*, in *The Economist*, the 31st of October 2015, in: https://www.economist.com/leaders/2015/10/31/the-trust-machine (last visited 06/04/2020).

[27] This may be retraced in the note that Nakamoto attached to the first bitcoin transaction: see P. De Filippi, A. Wright, *Blockchain and the law: the rule of code*, cit., 205.

[28] N. Szabo, *Smart Contracts: Building Blocks for Digital Markets,* 1996, in: https://bit.ly/2VoQFpc (last visited 06/04/2020).

[29] V. Buterin, *DAOs, DACs, DAs and More: An Incomplete Terminology Guide,* 2014, in: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ (last visited 06/04/2020).

[30] *Ibid.*

information. They stand at the user-front end and spread in almost every sector, including healthcare, offering a variety of services.

3. Applying the General Data Protection Regulation to Blockchains

It is suggested that blockchains have the potential to change the way we transact but regulatory and compliance aspects are called into question as obstacles for global deployment and spread[31]; amongst those, due to the apparent contrast with inherent traits of the technology, Data protection Law issues have caught immediate attention.

In particular, considerable controversy surrounding the GDPR emerged because not only the Regulation triggered a major change in the global Data Protection Law debate, enshrining a comprehensive regulatory approach[32] and raising the bar for new global standards[33], but also set a long-term view in respect to technological advances. The narrative of contrast with blockchain naturally rose due to a few characteristics of the technology itself that, at least at first glance, would suggest incompatibility with data protection principles, such as immutability and transparency, but it also regards whether a solid regime such as the GDPR would leave room for technological innovation[34]. Our study highlights how the European Union has embraced technology advances within the Digital Single Market and how blockchain appears to be an integral part of this challenge[35].

[31] See inter alia M. IANSITI, K.R. LAKHANI, *The Truth about Blockchain,* in *Harvard Business Review*, January- February Issue, 2017, in: https://hbr.org/2017/01/the-truth-about-blockchain (last visited 06/04/2020); M. CHIRIATTI, *The reasons behind the failure of many blockchains projects,* 2019, in: https://bit.ly/2Xu11Ft (last visited 06/04/2020); L. LYONS, L. COURCELAS, K. TIMSIT, *Legal and regulatory framework of blockchain and smart contracts*, Thematic Report of the European Union Blockchain Observatory and Forum, 2019, 9-11, in: https://www.eublockchainforum.eu/reports (last visited 06/04/2020).

[32] The reference is especially to the debated *privacy transatlantic divide*: J. Q. WITHMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 *Yale Law J.*, 2004, 1151 in: https://bit.ly/2Xtj2ng (last visited 06/04/2020); U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008; L.A. BYGRAVE, *Privacy and Data Protection in an International Perspective*, in *Scandinavian Studies In Law*, Vol. 56: ICT Legal Issues, Stockholm, 2010, in: https://scandinavianlaw.se/pdf/56-8.pdf (last visited 06/04/2020); D.J. SOLOVE, P. M. SCHWARTZ, *Reconciling Personal Information in the United States and European Union*, 102 *Calif. L. Rev.* 877 (2014), in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442 (last visited 06/04/2020).

[33] The Regulation stands at the culmination of a journey that started with the first legislative actions of Member States in the 1970s, Directive 95/46/EC, and the incorporation of data protection as a fundamental right in the EU Treaties with the Lisbon Treaty, under Art. 16 TFUE, creating also a novel legal basis for legislative actions. See inter alia G. G. FUSTER, *The emergence of Personal Data protection as a fundamental right of the EU*, Switzerland, 2014, and A. C. EVANS, *European Data Protection Law*, 29, in *The American Journal of Comparative Law* 1981, 571 in: https://www.jstor.org/stable/pdf/839754.pdf (last visited 06/04/2020); H. HIJMANS, *The European Union as Guardian of Internet Privacy - The Story of Art 16 TFEU*, Brussels, 2016.

[34] On GDPR debated technology neutrality, see S. KULHARI, *Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity*, 2018, 38-42, in: https://www.jstor.org/stable/j.ctv941qz6 (last visited 06/04/2020); L. MOEREL, *Blockchain and Data Protection ... and Why They Are Not on a Collision Course*, in *European Review of Private Law*, 26, 6, 2018, 840-842.

[35] Next to different actions, including the foundation of the EU Blockchain Observatory and Forum (https://www.eublockchainforum.eu, last visited 06/04/2020) and the European Partnership of Blockchain (https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership, last visited 06/04/2020), the main normative reference may be the *Resolution of the European Parliament on*

To analyse whether and how the GDPR may apply, we step into the wider regulation debate about blockchains, which falls beyond the scope of the present work[36]. However, we are of the opinion that lawyers may intercept the incoming changes – filling the gap between the «wet code» of legal language and «dry code» of computers[37] – and act as «transaction engineers»[38]. Currently, different studies describe that the trend towards regulation is almost global[39], looking favourably at *permissionless innovation*[40], but on the one hand substantial legal issues emerge in practice, as existing specific laws or principles may be challenged or contrasted by some intrinsic qualities of blockchain; on the other hand characteristics of the blockchain per se imply that it is difficult to qualify subjects and relationships.

The need arises to understand entities and use cases not framed by the law and to apply and elaborate the normative content – most of this challenge may be defined as a «classification exercise»[41]. This observation is consistent with the fact that before delving into the enforcement of the GDPR rights

distributed ledger technologies and blockchains: building trust with disintermediation, of the 3rd of October 2018, in: https://bit.ly/3dy3PHh (last visited 06/04/2020). Furthermore, the matter of distributed ledgers and GDPR was recently subject of a detailed study on the state of art, addressed to the Members and staff of the European Parliament: *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, written by M. FINCK at the request of the Panel for the Future of Technology and Science (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the European Parliament, Brussels, 2019, in: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (last visited 06/04/2020).

[36] Further on this topic: P. DE FILIPPI, S. HASSAN, *Blockchain technology as a regulatory technology: From code is law to law is code*, in *First Monday*, 21, 12, 2016, in: https://firstmonday.org/article/view/7113/5657 - author (last visited 06/04/2020); C. REYES, *Conceptualizing Cryptolaw, Neb. L. Rev, 96,* 385, 2017, in: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3121&context=nlr (last visited 06/04/2020).

[37] N. SZABO, *Wet code and dry,* 2008, in: http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html (last visited 06/04/2020).

[38] M. FENWICK, W. A. KAAL, E. P.M. VERMEULEN, *Legal Education in a Digital Age: Why 'Coding for Lawyers' Matters,* Lex Research Topics in Corporate Law & Economics Working Paper No. 4, University of St. Thomas (Minnesota) Legal Studies Research Paper No. 21, 2018, 7, in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227967 (last visited 06/04/2020).

[39] Legislative efforts have been pursued especially within the Fintech sector, with relevant examples concerning Initial Coin Offerings. Importantly, legal definitions of the technology, including collaborative endeavours towards standardization and interoperability, are noteworthy. We recall the Italian example, Decree of the 14th of December of 2018, n. 135, converted as a Law on the 11th of February 2019, n. 12 came into effect with Legge 11 Febbraio 2019, n. 12, Conversione in legge, con modificazioni, del D.L. 14 Dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione, in: http://www.gazzettaufficiale.it/eli/gu/2019/02/12/36/sg/pdf (last visited 06/04/2020). The Italian choice is to identify distributed ledgers within an existing subject - electronic documents and digital signatures. It may be important to note the correspondence with digital signatures, and the reference to the respective EU Regulation on digital signatures, so-called Regulation eIDAS, Regulation (EU) 2014/910 of the European Parliament and of the Council of the 23th of July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[40] A "sandboxing approach" would result in temporary, flexible obligations, on controlling scale for blockchain products. See V. AKGIRAY, *Blockchain Technology and Corporate Governance Technology, Markets, Regulation and Corporate Governance,* OECD Report, 2018, 19-20, in: https://bit.ly/371LeAT (last visited 06/04/2020).

[41] K. WERBACH, *op. cit.,* 531.

and obligations in the blockchain ecosystem, material scope and territorial scope of the Regulation must be framed in light of the peculiarities of the technology.

This study implies understanding the attribution of roles under the GDPR first and in the pages that follow we refer to this as the blockchain governance[42]. This is a decisive step in applying the entirety of the GDPR rules because the Regulation is deeply inspired by accountability as a principle. In this respect, we observe that previous studies have focused on the public model, where the user directly interacts with the network, considering that the private model would merely re-propose centralization; however, many scholars hold the view that blockchain may result – if not in the erasure of all the middlemen – in deep changes to the existing actors and emergence of different, possibly hybrid, ones, and their interaction with users would be of the utmost importance[43].

Let us now look at the GDPR definitions and blockchain "actors". For such an analysis, authors generally place an emphasis on developers, who can be loosely described as the authors of protocols, smart contracts and other components of the project, and nodes, or peers – namely the members of the network. In simple terms, the latter are considered on the basis of the activity they perform, e.g. the validation and storage of data, or the creation of blocks (namely the *miners* in the *Bitcoin* blockchain). They are also generally distinguished as operating with an integral or partial version of the blockchain (so-called *full nodes* and *light nodes*). Given such notions, and against the backdrop of public and private environments, a precise definition of users in the blockchain ecosystem has proved elusive. We remarked the importance of calling into question the concrete application of blockchain, including blockchain-based products, to identify such users and other stakeholders, and this is particularly helpful to outline the GDPR roles in blockchains.

The literature on the subject is copious and different nuances between the authors could be appreciated only through a detailed study[44]. It is first debated whether there could be Data controllers

[42] We remind our readers that governance is herein understood in relation to roles and Data Protection and as separate from the problem of governance of the infrastructure in the blockchain ecosystem. On this topic see: A. TAPSCOTT, D. TAPSCOTT, *Realizing the Potential of Blockchain - A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies*, World Economic Forum White Paper, 2017, 9-10, in: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf (last visited 06/04/2020). On Bitcoin governance, also in reference to the *block-size debate* see P. DE FILIPPI, B. LOVELUCK, *The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure*, in *Internet Policy Review: Journal on Internet regulation*, Vol. 5, Issue 3, 2016, in: https://policyreview.info/node/427/pdf (last visited 06/04/2020).

[43] P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law: the rule of code*, cit., 178-179; L. MOEREL, *op. cit.,* 834-835. As Michèle Finck wrote in her timely survey: «Whereas, in the early stages of the technology's development, many Data subjects have directly engaged with the network itself, this may become exceptional in the future, as Data subjects are more likely to communicate only with the application layer. This is easier for GDPR purposes, because it reintroduces the central entity the legislation was crafted for». See M. FINCK, *Blockchain Regulation and Governance in Europe*, cit., 101.

[44] M. FINCK, *Blockchain Regulation and Governance in Europe*, cit., 100-102; *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data,* Report of Commission Nationale de l'Informatique et des Libertés (CNIL), French Data Protection Authority, 2018, 1-4, in: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (last visited 06/04/2020); T. LYONS, L. COURCELAS, K. TIMSIT, *Blockchain and the GDPR*, Thematic Report of the European Union Blockchain Observatory and Forum, 2018, 17-18, in: https://www.eublockchainforum.eu/reports (last visited 06/04/2020); A. GIANNOPOULOU, V. FERRARI, *Distributed Data Protection and Liability on Blockchains*, Amsterdam Law School Legal Studies Research Paper No. 6, Institute for Information Law Research Paper No. 3,

and Data processors in the blockchain[45]. As a premise, the role of protocol developers or smart contracts publishers as Data controllers is contended, but numerous authors suggest that, in light of their commitment, the same nodes may be Data controllers, also Joint Data Controllers. On the other hand, because every node pursues its own objectives when joining the network, the same «determination of purposes and means» in their participation to the network is discussed, while it is argued that the technical functioning of public blockchain may imply that nodes shall be considered Data processors, given also possible distinctions between full and light nodes and miners. In all circumstances, significant difficulties, also considering pseudonymity and potential expansion of the chain, emerge, especially regarding the transparent arrangements required and the execution of corresponding obligations of Data Controllers and processors. Collectively, the current studies present more effective solutions for the private and/or permissioned environments, in light of potential ad hoc arrangements for allocation of roles and the fact that the processing of personal data could be governed at the application layer. However, in both the public and private environments, it is realistic that qualification of Data subjects[46] would depend on whether their personal data converge in the blockchain, and this is rather consistent with the material scope of the GDPR in blockchains.

Looking at the territorial scope, since it fundamentally relies on the participants in the blockchain, the obvious mentioned criticalities in identifying actors are important; still, based on the above, one may suppose that because there is a peer-to-peer network, no matter the level of decentralization and distribution, and thus whether the blockchain is public or private (or, again, hybrid), the potential for cross-nationality is an intrinsic feature[47]. We conclude that with regards to territorial scope the GDPR

2019, 7-10, in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316954 (last visited 06/04/2020); S. KULHARI, *op. cit.*, 42-44; L.D. IBÁNEZ, K. O'HARA, E. SIMPERL, *On Blockchains and the General Data Protection Regulation*, 2018, 5, in: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (last visited 06/04/2020). For a detailed study on *Bitcoin*, see T. BUOCZ, T. EHRKE-RABEL, E. HÖDL, I. EISENBERG, *Bitcoin and the GDPR: Allocating responsibility in distributed networks*, in *Computer Law & Security Review*, Vol. 35, Issue 2, 2019, 196-197, also in: https://www.sciencedirect.com/science/article/pii/S0267364918303170 (last visited 06/04/2020).

[45] Defined by Point 7 and 8 of Art. 4 of the GDPR, Data controller means «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», while Data Processor means «the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller». Overall, these definitions have not changed from the Directive 95/46/EC to the GDPR, but the Regulation has enshrined the correct interpretation as an "external" Data processor, who is outsourced or in another way delegated the processing. Art. 28 details the relationship established between the Data controller and Data Processor, governed through a contract or other legal act (Art. 28.3). See also Art. 29 Working Party Opinion n. 1/2010 on the concepts of "controller" and "processor", adopted on the 16th of February 2010, in: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (last visited 06/04/2020). Finally, according to Art. 26.1 of the GDPR, Joint Data Controllers are those «who jointly determine the purposes and means of processing. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations (…) 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».

[46] Data subjects are defined under the same Point 1 of Art. 4 of the GDPR, when it explains that «'personal data' means any information relating to an identified or identifiable natural person ('data subject'); (...)».

[47] M. FINCK, *Blockchain Regulation and Governance in Europe*, cit., 102.

is likely to apply to blockchains in an extensive manner, while the present work sets aside the issue of blockchains and data transfers to third countries.

However, for the GDPR to apply, material scope requires that personal data are processed as well: we consequently step into the wide definition of personal data under the GDPR[48]. This notion, to which pseudonymization[49] and anonymization[50] are complementary, brings about the studies around re-identification and the «failure of anonymization»[51], a key-issue for the literature, which started within the growing mediation of technology in our life and extensive *datification* of our daily behaviours[52]. The ongoing debate on the dichotomy between personal data and anonymous data points to the probability that Data Protection Law is facing a crisis in the definition of personal data[53] and may assert the very outdate of anonymization and the need for lexical reconsideration.

[48] According to Art. 4 Point 1 of the GDPR «'personal data' means any information relating to an identified or identifiable natural person ('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». Recitals n. 26, 27 and 30 are also relevant to this definition. According to Art. 4 Point 2 of the GDPR, the processing of data falls under the Regulation where it involves automated means, also partially, or even not automated means if, still, the outcome of the processing is to form part of a filing system. See Art. 29 Working Party Opinion on the concept of personal data no. 4/2007, adopted on the 20th of June 2007, in: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (last visited 06/04/2020).

[49] According to Art. 4 Point 5 of the GDPR, «'pseudonymisation' means 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 subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person». Recital n. 26, 28 and 29 are also relevant to this definition.

[50] A definition of anonymous information can be retrieved in Recital n. 26 of the GDPR, as referring to «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». See Art. 29 Working Party, Opinion n. 5/2014 on Anonymization Techniques, adopted on the 10th of April 2014, 7-8, hereinafter OWP 2014, in: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last visited 06/04/2020). For a detailed analysis see A. KNIGHT, S. STALLA-BOURDILLON, *Anonymous Data v. Personal Data - A false debate: an EU perspective on anonymization, pseudonymization and personal data*, 34, in *Wisconsin International Law Journal,* 284 (2017), in: https://ssrn.com/abstract=2927945 (last visited 06/04/2020); M. FINCK, F. PALLAS, *They who must not be identified—distinguishing personal from non-personal data under the GDPR,* in *International Data Privacy Law,* ipz026, 2020*, in:* https://doi.org/10.1093/idpl/ipz026 (last visited 06/04/2020).

[51] The reference is to P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA L. Rev.* 1701, 2010, in: https://www.uclalawreview.org/pdf/57-6-3.pdf (last visited 06/04/2020).

[52] N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU Data Protection law*, in *Law, Innovation and Technology*, 10, 4, 2018, 41, in: https://bit.ly/2MpJV5n (last visited 06/04/2020).
For a significant contribution on increasing data collection see A. M. FROOMKIN, *The Death of Privacy?,* 52 in *The Stanford Law Review, 1461,* 2000, also in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715617 (last visited 06/04/2020).

[53] For a comprehensive study, see R. DUCATO, *La crisi della definizione di dato personale nell'era del Web 3.0 - Una lettura civilistica in chiave comparata*, in F. CORTESE, M. TOMASI (eds.), *Le definizioni del Diritto, Atti delle giornate di studio del 30-31 Ottobre 2015*, *Quaderni della Facoltà di Giurisprudenza* No. 26, Trento, 2016, in: http://hdl.handle.net/2078.1/195903 (last visited 06/04/2020).

With this in mind, we examine the processing of personal data in a blockchain and we start to consider how personal data can be part of the transactions of the blockchain[54]. As a premise, we highlight that whether an automatic processing of data under Art. 22 of the GDPR happens in a blockchain would require a separate, further reflection[55]. It is useful to think of a blockchain as a state transition system, where the transition is the operation a user wants to execute and where the verification and the upload of the state take place[56]. On the one hand, the processing of data is included in the same execution of the protocol, to which signatures and public keys are essential[57]; on the other hand, it regards the same data included in the transaction[58], which corresponds to the information necessary for that specific transaction.

This confirms that the presence of personal data, as the actual need to process personal data, relies partly with the use-case and one major setback is that the characteristics of transaction data cannot really be comprehensively listed, also presenting possible intrinsic features[59]. Furthermore, the importance of the model, also partially depending on the use-case, cannot be denied, especially considering blockchain products and intermediaries, as the presence of personal data at the application layer may be imposed[60].. Another conspicuous observation is that the same can be said for the deployment of the "architectural" solutions previously mentioned, which has a considerable impact on the presence of the personal data in the blockchain.

Overall, we defer the necessary evaluations on the applicability of the household exemption, that would come into play if natural persons stand before the nodes[61], and we conclude that at the current state of development, the elements highlighted above would indicate that personal data is processed in a blockchain. In the next paragraph we explore the peculiarities and criticalities which arise in applying the GDPR to a healthcare blockchain scenario.

[54] Inter alia, M. FINCK, *Blockchain Regulation and Governance in Europe*, 96-97.

[55] The issue has fresh prominence in relation to smart contracts. For a comprehensive study see M. FINCK, *Smart Contracts as a Form of Solely Automated Processing under the GDPR*, Max Planck Institute for Innovation and Competition Research Paper No. 01, 2019, 9, in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370 (last visited 06/04/2020).

[56] S. SATER, *Blockchain and the European Union's General Data Protection Regulation*, 2017, 19, in: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987 (last visited 06/04/2020). The author refers to V. BUTERIN, *Notes on Scalable Blockchain Protocols (version 0.3.2)*, 2015, in: https://bit.ly/304F8y9 (last visited 06/04/2020).

[57] L.D. IBÁNEZ, K. O'HARA, E. SIMPERL, *op. cit.,* 5-6.

[58] The term «transactional data» is elected by Michèle Finck. See FINCK, *Blockchain Regulation and Governance in Europe*, cit., 96-97.

[59] In *Bitcoin* for example, the script function OP_RETURN allows for the inclusion of arbitrary data.

[60] FINCK, *Blockchain Regulation and Governance in Europe*, cit., 96.

[61] *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, cit., 4. For further on the household exemption, explained by Art. 2.2 letter c) of GDPR, see Art. 29 Working Party Statement on current discussions regarding the data protection reform "package", of the 27th of February 2013, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, in: https://bit.ly/2Y1lUqR (last visited 06/04/2020); Court of Justice of the European Union, Judgment of the 6th of November 2003, *Bodil Lindqvist*, Case C-362/14, in: https://bit.ly/302CpFC (last visited 06/04/2020).

4. GDPR compliance in Blockchain-based projects for the Healthcare

Healthcare is often referred to as the ultimate use-case for blockchains[62]. The need for interoperability, selective access and security and integrity of data are an essential feature of this sector and this is why several blockchain-based projects can be found, but the reference is especially to the opportunities related to private and permissioned blockchains, which ensure confidentiality of the data. We primarily mention the relevance of projects aimed at the management of electronic health records, a number of them being consistent with a patient empowerment perspective in line with blockchain potential for self-identity-management[63].

In the processing of health information, data protection provisions are normally supplemented by administrative laws that govern retention, resulting in different obligations and conservation timescales, deontological rules and sectoral norms. The scenario is characterized by the coexistence of normative sources and different actors, given a strong need for self-regulation[64]. However, in light of the sensitivity of the data to be processed, Privacy and Data Protection are certainly key issues for the healthcare applications, eHealth requiring specific attention as it introduces new use-cases and vulnerabilities. In the European Union context, aimed at fostering the digital transformation of healthcare[65], compliance with the GDPR is vital in understanding how blockchains may be usefully deployed for this scope. Even if the Regulation does not address specific provisions to the sector[66], in

[62] See, inter alia: A. Santos Rutschman, *Healthcare Blockchain Infrastructure: A Comparative Approach* in *Legal Studies Research Papers,* Issue 6, 2018, in: https://ssrn.com/abstract=3217297 (last visited 06/04/2020); A. Hesselgren, K. Kraslesvka, D. Gligoroski, S.A. Pedersen, A. Faaxvag, *Blockchain in the Healthcare and health sciences,* in *International Journal of Medical Informatics,* 134, 2020, in: https://doi.org/10.1016/j.ijmedinf.2019.104040 (last visited 06/04/2020); C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, *Blockchain Technology in Healthcare: A Systematic Review,* in *Healthcare*, 7, 2, 56, 2019, in: https://www.mdpi.com/2227-9032/7/2/56 (last visited 06/04/2020).

[63] Examples in this field are, inter alia: *MedRec* (https://medrec.media.mit.edu/, last visited 06/04/2020) and *MyHealthMyData* (http://www.myhealthmydata.eu/, last visited 06/04/2020). However, in this work we intend to take as a reference a Proof-of-Concept project in which we the authors had the chance to collaborate at Fondazione Bruno Kessler in Trento, Security and Trust Unit.On blockchain self-identity management potential see Moerel, *op. cit.*, 850-851.

[64] With regards to the italian context, see E. Lamarque, *Privacy e Salute*, in G. Losano (ed.), *La legge italiana sulla privacy - Un bilancio dei primi cinque anni*, Roma-Bari, 2001, 338-339. For instance, Guidelines and Opinions by the Italian Data Protection Authority are fundamental to the interpretation of the legislative content; on this point see G. M. Riccio, *Privacy e Dati sanitari*, in F. Cardarelli, S. Sica, V. Zeno-Zencovich (eds.), *Il Codice dei dati personali - Temi e problemi*, Milano, 2004; G. Finocchiaro, *Privacy e protezione dei Dati personali - Strumenti Operativi*, 2012, Bologna, 295-317.

[65] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, of the 30th of April 2004, *E-Health - making healthcare better for European citizens: An action plan for a European e-Health Area*, in: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0356&from=EN (last visited 06/04/2020) and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of the 25th of April 2018, *On enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*, in: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0233&from=EN (last visited 06/04/2020).

[66] For an analysis of blockchain-based solutions for managing health records and seeking compliance with the Health Insurance Portability and Accountability Act of 1996 [Pub. L. No. 104-191, 110 Stat. 1936 (1996)], see S. Sater, *Blockchain Transforming Healthcare Data Flows*, 2018, in: https://bit.ly/2AEBJf3 (last visited 06/04/2020).

accordance with the choice of a homogenous approach, it defines special precautions with regards to health data and leaves room for Member States to enact detailed provisions.

Keeping in mind the considerations on the applicability of the GDPR to blockchains from the previous paragraph, we proceed to consider the principles of Art. 5 of the GDPR and to introduce a limited number of relevant rights and obligations in such blockchain-based projects, underlying the cases in which the presence of health data would require special consideration.

With regard to lawfulness (Art. 5.1 letter a) and thus the legal basis of the processing (Art. 6), generally speaking the user-Data subject's choice to use the blockchain leads us to consider that the processing would normally be based on consent (Art. 6.1 letter a) or the necessity to enter into a contract (Art. 6.1 letter b). Still, this may be deemed a passive act and the possibility of using such basis remains unclear in absence of an agreement or defined governance[67], being this matter also strongly tied to the right to information of the user (Art. 13).

However, it is important to consider that these deficiencies are more easily solved with private blockchains or blockchain applications where authorities or intermediaries are present, which, based on the above, are more likely to be used in the selected scenario. Besides, notionally, different legal bases could be considered according to the use-case: when it comes to the processing of health data, other than consent, we may rely on necessity of a performance of a task carried out in the public interest or in the exercise of a public authority vested in the Data controller (Art. 6.1 letter e), which may be further specified by national laws.

An additional fundamental consideration about lawfulness is that Art. 9.1 of the GDPR states the prohibition of the processing for special categories of data. In the selected scenario, genetic data (Point 13 of Art. 4) and data concerning health (Point 16 of Art. 4) come to our attention as falling under these categories. Data concerning health is defined as the personal data related to the physical or mental health of a person, including the provision of healthcare services, which reveal information about his/her health status. Recital 35 is also valuable for this definition: information about the health status may regard, with no distinction, past, current or future physical or mental health status and this should include the information collected during registration for, or the provision of, healthcare services, as is specified in Directive 2011/24/EU[68]. In particular, this information may consist, inter alia, in a number, symbol or particular which was assigned to a natural person to uniquely identify the natural person for health purposes and this seems particularly important considering the management of health records. Because Art. 9.2 establishes a series of conditions under which the prohibition of processing should not be applied, we consider, next to consent (Art. 9.2 letter a), the necessity of processing for a public interest (Art. 9.2 letter g) and for the provision of a service related to healthcare (Art. 9.2 letter h) relevant for our use-case[69].

[67] LYONS, COURCELAS, TIMSIT, *Blockchain and the GDPR*, cit., 24-25.

[68] Directive 2011/24/EU of the European Parliament and of the Council of the 9th of March 2011 on the application of patients' rights in cross-border healthcare, in: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0024&from=IT (last visited 06/04/2020).

[69] With particular regard to the latter, Art. 9.2 letter h) of the GDPR refers to the necessity of the delivery of social care or treatment and, in addition, to the management of health or social care systems and services. The conditions established by Art. 9.3 should apply to Art. 9.2 letter h), so we consider that the presence of a professional, subject to the obligation of secrecy, shall be met in the selected scenario. Nonetheless, one relevant

With regards to the principle of fairness and transparency under the same Art. 5.1 letter a), authors argue that these objectives are easy to achieve in a blockchain, if the validation rules shall be disclosed to users[70], despite the potential for information asymmetry. Considering the right to information (Art. 13 and Art. 14), information about the Data controllers (Art. 13.1 letter a, Art. 14.1 letter a) in a blockchain seems difficult to define, as well as information such as the storage period or its criteria (Art. 13.2 letter a, Art. 14.2 letter a) and purposes of the processing (Art. 13.1 letter c, Art. 14.1 letter c). This is again partially easier for our use-case for our use-case, because rules would be set by defined actors, but indicating a storage period remains complex for it deals with immutability as a characteristic of a blockchain itself[71].

It is also affirmed that the right to access (Art. 15), as the right to data portability (Art. 20), would be easily implemented because everyone can access the blockchain[72]. Overall, we stress that the relevant uncertainties would be mostly related to how to exercise these rights and relate to the Data controller, so they remain tied to the governance and shall be commented as above.

Purpose limitation under Art. 5.1 letter b) is consistent with the fact that the processing of data in a blockchain normally attains to a specific protocol and function; on the other hand, the inability to exercise control over the spread and usages of data, if made publicly available, would likely render compliance impracticable[73]. Furthermore, the fact that all the nodes process the information, which is an intrinsic feature of the technology, may be considered at odds with data minimization under Art. 5.1 letter c)[74]. However, both these matters rather rely on the design of the network[75] from a more general perspective.

More specifically, data minimization may be defined in a concise manner as first of all rendering the presence of personal data limited to what is strictly necessary for the blockchain to work[76]. Dealing with blockchain for healthcare, i.e. for the management of healthcare records, and with other use-cases of particular sensitivity as well, this primarily means balancing the need to keep data confidential with the transparency and decentralization of the blockchain[77] – we mentioned the option for healthcare would be rather a private environment instead of a public one – and considering carefully what shall be stored (and eventually removed) from the blockchain. Ultimately, this means considering

aspect to bear in mind is that the mentioned legal bases would only cover the processing which is necessary to the treatment: whereas such processing would not be deemed as necessary, another legal basis should be chosen. See also what was affirmed by the Italian Data Protection Authority in an official document on the application of data protection with regard to data concerning health in the healthcare sector, Provision n. 55 of the 7th of March 2019, in: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942 (last visited 06/04/2020).

[70] L.D. IBÁNEZ, K. O'HARA, E. SIMPERL, *op. cit.,* 6.

[71] D. SCHMELZ, G. FISCHER, P. NIEMEIER, L. ZHU, T. GRECHENIG, *op. cit.,* 227.

[72] *Ibid.*

[73] L.D. IBÁNEZ, K. O'HARA, E. SIMPERL, *op. cit.*, 6; FINCK, *Blockchain Regulation and Governance in Europe*, cit., 104.

[74] *Ibid*.

[75] Inter alia, L. LYONS, L. COURCELAS, K. TIMSIT, *Blockchain and the GDPR*, cit., 25.

[76] S. KULHARI, *op. cit.*, 44-45; L. MOEREL, *op. cit.,* 846-851; L.D. IBÁNEZ, K. O'HARA, E. SIMPERL, *op. cit.*, 7-8; M. FINCK, *Blockchain Regulation and Governance in Europe*, cit., 104.

[77] P. DE FILIPPI, A. WRIGHT, *Blockchain and the Law: the rule of code,* cit., 115-116.

for which purposes the blockchain can be used[78]. Also applicable to this matter, we mention that the presence of personal data could be substantially limited, although not avoided, from the design, with the application of solutions previously mentioned for limiting the presence of personal data in the blockchain, and amongst those pseudonymization or other encryption techniques may be extremely useful for adherence to these principles[79.]

These same observations are also constructive for complying with the storage limitation principles under Art. 5.1 letter e). The amount of time for which the information is retained could not be easily determined in a blockchain, as anticipated, but the solutions described above for limitation of personal data shall be evaluated by means of a legal appreciation of re-identification risks. Storage limitation refers indeed to data «kept in a form which permits identification of Data subjects for no longer than is necessary for the purposes for which the personal data are processed (…) ». Considering our use-case, retention of health data would also be maximized according to the pertinent sectoral rules, depending on the characteristics of the documents.

To sum up, the rules described above and regarding purpose limitation, minimization and storage limitation are also in apparent conflict with the technology because data cannot be modified or deleted from the blockchain: this brings us to consider the principle of accuracy under Art. 5.1 letter d) and the right to rectification (Art. 16) and erasure (Art. 17), as well as restriction of the processing (Art. 18). From a broad perspective, accuracy of data is one of the core ideas of the blockchain because the ledger is created to give users access to the adjourned status of transactions, even if, as stated, the blockchain itself does not guarantee data is correct. Still, if a rectification occurs, the pertinent records would remain in the ledger since data on the blockchain is not supposed to be modified, despite recent work on blockchains which can be rewritten[80]. Among the presumed incompatibilities with the GDPR, the right of erasure is indeed the most controversial one, raising the most hype, in light of the conflict within the unmodifiable and tamper-resistant nature of the blockchain.

Different solutions for erasure, covering also restriction of processing, are plausible. Considering the nature of blockchains, the mechanisms that can limit the amount of personal data in a blockchain application, such as the one previously mentioned, are primarily considered in the literature; amongst them, deletion off-chain firstly has drawn attention, even though it can be said that the problem shifts to the data on-chain. Also, despite these efforts, broadly speaking the problem of erasure is always left with the remaining data in the blockchain. Still, this leads us to consider that with regards to these solutions and encryption for erasure, because within the current legal framework there is not really a

[78] The reference is to the project analysed in our previous study at FBK: the system was designed with “off-chain” and “on-chain” components and exploiting the blockchain network to create an Attribute-Based-Access-Control to the health records.

[79] More specifically, pseudonymization is mentioned as a factor for privacy by design in Art. 25.1 of the GDPR. On this point see also OPW 2014, cit., 20.

[80] For instance, considering *editable blockchains*, a chameleon hash function makes it possible to change the information while maintaining the same outcome of the hash function. See G. Ateniese, B. Magri, D. Venturi, E. Andrade, *Redactable Blockchain - or - Rewriting History in Bitcoin and Friends, 2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017, in: https://ieeexplore.ieee.org/document/7961975 (last visited 06/04/2020).

recognized technique which is deemed to set at zero the chance to restore the information[81], we may keep pointing towards the evolving case-law and regulation developments[82].

In this respect, it is suggested that Art. 17.2 may fit the blockchain reality[83], as there are more Data controllers and the personal data was made public. The norm establishes that controllers, taking into account the available technology and cost of implementation, must take all reasonable steps, including technical measures, to inform other Data controllers which are processing the personal data of the request of the Data subject, which affects any links or copy or replication of those personal data.

Nevertheless, a few considerations regarding the same nature of the right of erasure also seem important. Not only the norm can be subject to interpretation and authors hold there may be partial room for exploring different solutions of erasure which could get past shortcomings of blockchains, but the exercise of the right is conditioned as well[84]. Paragraph 3 of Art. 17 is decisive to our analysis of healthcare applications, explaining that the right to erasure shall not apply in some circumstances: for instance, if performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 17.3 letter b) or if the processing is necessary for reasons of public interest in the area of public health – in accordance with Art. 9.2, letter h) and i), and Art. 9.3 – (Art. 17.3 letter c).

Coming to letter f) or Art. 5 at last, proclaiming security as a principle, the bond between security and blockchains is one of multiple opportunities[85]. On one hand, with regards to the integrity of personal data, blockchain technology is generally noted for its resiliency and the absence of a single point of failure, since blockchain is also possibly conceived as a tool for enhanced security, but as already noted the requisite of confidentiality may be in contradiction with the nature of public blockchain. In addition, as referred above, once personal data are accessible concerns about the lawful processing cannot be avoided. For the remainder, security of personal data appears to be left with the adoption of technical measures and accurate design in the blockchain. This brings us to consider the measures that Data controllers and processors may take under Art. 32, related to security, where the event of data breach (Art. 33 and Art. 34) is also mentioned.

[81] As the Art. 29 Working Party does, it shall be concluded that encryption solutions aim at improving security but are not primarily meant to anonymization. See OWP 2014, cit., 20 and supra note n.49.

[82] L.D. Ibáñez, K. O'Hara, E. Simperl, *op. cit*., 7-9; M. Finck, *Blockchain Regulation and Governance in Europe*, cit., 107; *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*, cit., 8-9.

[83] M. Finck, *Blockchain Regulation and Governance in Europe*, cit., 107.

[84] S. Kulhari*, op. cit*., 47-48; M. Finck, *Blockchain Regulation and Governance in Europe*, cit., 108. A mentioned reference is to Art. 35 Bundesdatenschutzgesetz, Federal Data Protection Act of the 30th of June 2017, in: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html (last visited 06/04/2020). For further considerations on the right to erasure see, inter alia, L. Moerel, *op. cit.*, 845-846; L.D. Ibáñez, K. O'Hara, E. Simperl, *op. cit*., 8. The authors refer, inter alia, to Court of Justice of the European Union, Judgment of the 13th of May 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, in: https://bit.ly/2BnlV0m (last visited 06/04/2020) and Court of Justice of the European Union, Judgment of the 9th of March 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, Case C-398/15, in: https://bit.ly/2Y1t6D6 (last visited 06/04/2020).

[85] For a recent study on this topic, see *Blockchain & Distributed Ledger: aspetti di governance, security e compliance*, Clusit – Associazione italiana per la Sicurezza informatica, 2019, in: https://clusit.it/wp-content/uploads/docs/BC-e-DLT-Governance-Security-Compliance-v1.pdf (last visited 06/04/2020).

Accountability is the last principle enshrined in Art. 5.2. Nonetheless, it is easy to see how this last part of the analysis is mostly related to blockchain governance, which was discussed with respect to healthcare giving evidence of the preference for a private environment for this use case. Subsequent provisions of the GDPR, such as those concerning the record of processing activities (Art. 30), the abovementioned Security of the processing (Art. 32), and the Data Protection Impact Assessment (Art. 35) – to name a few – refer to Data controllers and, in part, Data processors, as the recipients of the obligations and duties to ensure the rights of Data subjects.

These rules are certainly relevant for our use case. The nature of data processed in a blockchain for healthcare would probably require, for instance, the adoption of certain measures in the event of data breaches, a Data Protection Impact Assessment – because of the processing on a large scale of special categories of data referred to in Art. 9.1 (Art. 35.3 letter b) – or the appointment of a Data Protection Officer - at least because the core activities of the controller or the processor consist of processing on a large scale of special categories of data (Art. 37.1 letter c). Still, more importantly, from a broader point of view, it is the compliance with the GDPR altogether that is the primary responsibility of the Data Controller (Art. 24); as the analysis may have shown for blockchains, and especially for healthcare applications, given the special cautions to be adopted, this can be traced back to a number of foundational choices to be applied "to the code", primarily intended for data minimization, and constantly adjourned to the best practices and most updated technical advances, under the sign of privacy by design and privacy by default (Art. 25).

In conclusion, we may confirm that governance is the most prominent issue for blockchain compliance with the GDPR. This is a critical point to our analysis: we highlighted that most of the examined issues would find an easier answer in a private blockchain environment, given identified actors are present, but the latter is eventually the most apt to our use-case. Still, to implement data protection roles in a blockchain healthcare project may be challenging because definition of data protection roles in the sector can be complex per se and has been debated through time[86]. For instance, considering management of health records, exchange of data takes place in diverse environments, presenting different structures according to existing organizational practices, and digitalization is ultimately contributing to create a new scenario[87]: the possibility to build a blockchain that can mirror the logic of this complex data exchange represents a great opportunity[88].

On the other hand, we mention the presence of personal data in the blockchain as another issue to be further explored: work-in-progress technical solutions to limit personal data on the blockchain were discussed and we believe that they may be promising, especially because the legal literature is facing the crisis of the definition of personal data. However, since the same presence of personal data on the blockchain can be tackled as a matter of design, in the present overview on the hyped impossible compliance between blockchains and the GDPR, the first manifest result is beyond the hype. As alleged almost unanimously by the literature and far from being trivial, the preliminary study of whether a

[86] P. GUARDA, *Fascicolo Sanitario elettronico e protezione dei dati personali*, Trento, 2011, 106.

[87] P. GUARDA, *I Dati sanitari*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (eds.), *I dati personali nel diritto europeo*, Milano, 2019, 609-617.

[88] The reference is in particular to the FBK project on which we collaborate: in that implementation, the proposed private blockchain network took the off-chain status "on-chain", enabling the harmonic realization of data protection roles.

blockchain would be needed in the as–is healthcare application scenario and how a blockchain–based project really would be essential to the desiderata for this sector are of the utmost importance.

Our analysis could not provide the ultimate solution for Data protection for healthcare blockchain applications: indeed, only a detailed case-study would allow for a complete compliance assessment. Still, in spite of the scepticism and without denying a few challenging inconsistencies, such as the one regarding the right to rectification and the right to erasure, we measured that organizational and technical measures, to be converted in specific design choices, should be seen as the ultimate opportunities for compliance[89].

Insisting on the risks, although they are present, and denying the room for compliance with the GDPR, as well as with other laws, may even be premature and dangerous to these early innovation efforts[90]. To take advantage of the innovative core of this technology would surely require a certain amount of transparency, which presents some obstacles with regards to data protection, especially in the selected use-case. Nonetheless, we have tried to mitigate them with an account of current developments and a few open-ended questions, and eventually we cannot exclude that blockchain may embody a tool for enhanced data protection, as described by several authors and as suggested by its history and roots[91]. On the other hand, it also remains to be seen whether the Regulation would be conceived beyond a mere imposition of its contents, and this paper sides with those authors who look with a positive attitude at the space that the GDPR left to the inventive developers, primarily under the notion of privacy by design and by default[92]. In this manner, the Regulation may find a way to accommodate the plural issues of the ecosystem, mirroring the different contemporary demands of the digital space of the European Union but admittedly including users' privacy and data protection demands, which are imperative for eHealth.

5. Final remarks

Blockchain, blockchain everywhere. The technological suggestions, as it happens for those of a social nature, tend to become overwhelming and upsetting with respect to possible application scenarios. As often happens therefore, there is no longer any serious and critical question as to whether the fashionable technical solution represents a real improvement on the previous framework, but it is trusted in it as new and "universally" accepted. This is what has happened and is happening to the topic of distributed registers and their possible variations. If this has critical implications in the technological field, the problem is even more evident in the legal field. It is never easy to apply rules

[89] Inter alia, F. Cate, C. Kuner, O. Lynskey, C. Millard, N. Ni Loideain, D. Svantesson, *Blockchain versus Data Protection*, 8 *International Data Privacy Law* 103 (2018), also in: https://bit.ly/3042G6o (last visited 06/04/2020).

[90] Inter alia, S. Sater, *Blockchain and the European Union's General Data Protection Regulation,* cit., 38-39; Moerel, *op. cit*., 851.

[91] From a more general perspective see J. Hall, *How Blockchain could help us take back control of our privacy,* in *The Guardian*, the 21st of March 2018, in: https://bit.ly/2YbRa6D (last visited 06/04/2020) and S. A. Pentland, T. Hardjono, *Digital Identity Is Broken. Here's a Way to Fix It*, in *Wall Street Journal,* the 3rd of April 2018, in: https://blogs.wsj.com/cio/2018/04/03/digital-identity-is-broken-heres-a-way-to-fix-it (last visited 06/04/2020), discussing the MIT Enigma Project mentioned above.

[92] Inter alia, S. Kulhari*, op. cit*., 38-42, 53-55; L. Moerel, *op. cit*., 840-842. The author refers to Recital 78 of the GDPR.

shaped around different technological scenarios to such highly innovative and disruptive solutions. The real question, and the correct way to ask yourself, is whether the innovation is truly better than what was previously offered. This is in terms of effectiveness and technical efficiency, and, above all as far as we are concerned, in terms of compliance with the legal data.

Much has been said and written about possible applications of the blockchain (to the financial sector and in online payment systems, the context of land registers, the tracing of the food supply chain, etc.). All the effects that this application could cause have not yet been fully evaluated, net of the promised benefits. From this perspective, the health context, chosen as a paradigmatic one in our paper, certainly represents one of the most complex and challenging frontiers, especially with reference to compliance with the legislation on personal data protection. Here the risk is among the highest possible (processing of health data); here the solutions aimed at increasing the safety in the management of the systems are among the most desirable. A careful technical-legal analysis must however try to be as neutral and objective as possible. The jurist does not have the expertise to verify whether the technical choice is truly more desirable than those that the state of the art offered (in this computer experts have obviously much more to argue); however, she can describe the critical issues that the application scenario presents in terms of the processing of personal data and offer a further evaluation framework to a general and necessarily interdisciplinary choice. From this perspective again, as highlighted in the pages above, the reader has grasped the complexity of the matter, the necessary determination of which, among the varied constellation of possible choices, type of blockchain is more reliable to use, the critical issues compared to the interpretation of legal institutions not directly designed for this innovative context, however, in the face of some evident guarantees that the system offers.

We have not tried to, nor did we want to, propose a definitive landing point. «The journey, not the arrival matters» (T.S. Elliot). An attempt was made to indicate a possible methodology of analysis and approach to a specific problem with respect to a peculiar application context. Other studies will deal with further defining the interpretive solutions and approaches. The important thing was to start a journey, together with the work of many others.

Downloaded from www.biodiritto.org.
ISSN 2284-4503