QMLJ (2021) 2, 15
DOI: 10.26494/QMLJ3939

Blockchain and the General Data Protection Regulation: an irreconcilable regulatory approach?

Enza Cirone*

Abstract *A blockchain is a class of technology that allows the creation and management of different forms of decentralised and distributed digital ledgers where data are stored, chronologically recorded, transferred and finally shared between the 'nodes' participating in a peer-to-peer network. These features prima facie clash with the GDPR that informs the EU data protection legislation and is based on a centralised representation of the reality in which data are processed, collected, and recorded in a database controlled by identified subjects. The underpinning idea of this article is diametrically opposed to the one which considers the technology not GDPR-compliant by default. First, the author argues that the points of tension can be mitigated by technical and/or governance methods, thus acting at both application and infrastructure level. In essence, a case-by-case analysis is the only feasible option to assess the compliance between the regulation and the technology. Second, a further and closer look at blockchain's underlying concepts reveals how both the GDPR and the blockchain have the same purposes but different approaches. More interestingly, the article suggests that the blockchain could be seen as a Privacy Enhancing Technology (PET), which might help data subjects gain more control over their personal data and hence support one of the GDPR's purposes (recital 7).*

1. Introductory remarks

Blockchain technology[1] has rapidly become the best-known and most widely used application of distributed ledger technology (DLT) globally.[2] It has been depicted as the ultimate disruptive technology since the advent of the internet. As such, it may radically change the way socio-economic interactions take place and eventually create great opportunities and serious challenges for society.

*PhD Candidate in European and transnational legal studies, University of Florence, enza.cirone@unifi.it. I am grateful to the anonymous reviewers as well as to Professor Adelina Adinolfi for her precious comments on a draft version of this article. The usual disclaimers apply.

[1] The origins of blockchains can be found in the development of the digital currency, Bitcoin, as outlined in Satoshi Nakamoto's 2008 White Paper (*Bitcoin a Peer to Peer Electronic Cash System*, 2008, <https://bitcoin.org/bitcoin.pdf>), in which he (or maybe better to say they) were developing a new form of payment through digital means that was a 'purely peer-to-peer version of electronic cash'. See Julie Pitta, *Requiem for a Bright Idea* (1999) Forbes <forbes.com/forbes/1999/1101/6411390a.html#5c162ff0715f>, accessed 25 January 2021.

[2] Recently, with the tremendous development of crypto-currencies, like - by way of example - Bitcoin, the underlying distributed ledger technology has attracted significant attention.

It is essentially an immutable, decentralised and publicly available database geographically spread across a network of multiple nodes[3] with no central administrator or centralised data storage. Any changes to the ledger are reflected in the various copies as a consensus algorithm[4] is used to check the validity of the information that a node requires adding to the chain. Thus, the security and accuracy of the ledger are cryptographically maintained according to the rules agreed by the network. This allows for the preservation of data confidentiality. However, some critics suggest that 'unless additional technical means are used to protect the confidentiality of online communication, it might result that decentralized infrastructure – designed to promote privacy and autonomy – is more vulnerable to governmental agencies or corporate scrutiny than their centralized counterparts'.[5]

Given these qualities, a multitude of legal questions arise. Especially, how should data protection law deal with the developments of this new paradigm?[6]

The core technical features of the blockchain clash at first glance with the regulatory model informing the European Union's (EU) data protection legislation. The General Data Protection Regulation (GDPR)[7] is a piece of far-reaching privacy legislation designed to enhance the protection of personal data and provide individuals with greater control over their own data.

Prima facie, a structural tension seems to exist between the technical underpinning of the regulation - the centralised processing of data- and the inherently decentralised nature of

[3] For general overview see: William Mougayar, *The business blockchain* (Hoboken 2016), 17; Aaron Wright and Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (2015) <https//ssrn.com/abstract=2580664>.

[4] Miners determine which blocks are to be added to the blockchain, through different *consensus* protocols. The latter make possible for distributed network of peers to store information in a blockchain without the need to rely on any centralised operator or middleman. They indeed allow actors on the network to agree on the content recorded on the blockchain itself. Proof-of-work and proof-of-stake are the common consensus methods. In proof-of-work-based blockchains, such as the one used for the Bitcoin, the mining nodes compete to add the next block by solving a cryptographically complex calculus that requires a high amount of computational power and electric energy. In proof-of-stake-based blockchains, an important factor in determining which node will add to the next block is the stake that this node has, that is the amount of token it owns. See Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Godfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* (Princeton University Press 2016).

[5] Primavera De Filippi, *The interplay between decentralization and privacy: the case of blockchain technologies* (2016) Journal of Peer Production, Issue n.7: Alternative Internets.

[6] Michèle Finck, *Blockchains and data protection in the European Union*, (2017) MPI Paper, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322>, 1: [there is] '*the risk that data protection legislation renders the operation of blockchains unlawful, hence asphyxiating the development of an innovative technology with much promise for the Digital Single Market'.*

[7] European Parliament and Council Regulation (EU) 2016/679 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, OJ 2016 L 119/1.

the blockchain technology. The ostensible incompatibility[8] between the 'genetics' of the blockchain and that of the EU data protection legislation triggers the question of whether the GDPR, whose provisions are in principle 'technologically neutral',[9] can guarantee an adequate protection to the huge amount of data registered on the blockchain. While the EU Commission expects the GDPR to enable 'innovation to continue to thrive under the new rules',[10] many have voiced concerns[11] that the GDPR will stifle the innovation of this emerging technology. Similarly, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) also highlighted that 'blockchain presents both opportunities and challenges in terms of data protection.'

Consequently, this article will address some crucial issues arising at the interplay between blockchain and data protection, thus outlining the essential characteristics of this topic. The overarching aim of this article is to identify and highlight these tensions to understand whether the GDPR is able to adequately regulate data processed through this new technology.

This author essentially argues that GDPR compliance is not about the technology itself but is concerned with how the technology is used. There is no such thing as a GDPR-compliant BC technology *per se*. On the contrary, the article demonstrates that there are only GDPR-compliant uses of technology.[12]

Essentially, the underlying idea is that it is a matter of technological design and governance to ensure compliance with (EU) data protection law. The focus is on the principle of data protection by design[13] which represents a key element to ensure conformity with the applicable regulations as it may play a crucial role in building blockchains compliant with data protection from their design phase and then throughout their life cycle.[14]

---

[8] EU Blockchain Observatory and Forum (EuBOF), *Blockchain and the GDPR* (2018) <https://www.eublockchainforum.eu/reports>; Aaron Wright and Primavera De Filippi, *Blockchain and the Law* (2018 Harvard University Press); Lucie Munier and Ashley Kemball-Cook, *Blockchain and data protection regulation: reconciling protection and innovation* (2019) Journal of security operations & custody 145, 157; Andries Van Humbeeck, *The Blockchain-GDPR paradox* (2019) Journal of data protection & privacy 208-212; European Parliamentary Research Service (EPRS), *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (2019) <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf>

[9] Recital 15 of the GDPR.

[10] European Commission, *Questions and Answers, Data Protection Reform Package* <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441>

[11] David Meyer, *Blockchain technology is on a collision course with EU privacy law* (2018) <https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/>

[12] Report on Blockchain and the GDPR by EuBOF (2018) (n 8) 4.

[13] EDPB Guidelines 4/2019 on *Article 25 Data Protection by Design and by Default* adopted on 20 October 2020.

[14] EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 85.

On the flip side,[15] a closer review of blockchain's underlying concepts reveals how both the GDPR and blockchain technology have the same purposes but different approaches. Blockchain may be basically seen as a Privacy Enhancing Technology (PET) [16] structured in the form of a Personal Information Management System (PIMS)[17] which due to its strong encryption of stored data, allows it to operate as a kind of enabler for solutions. This ensures wider data protection rights than the GDPR. As a result, data subjects are the central focus and operate as active agents of the data governance architecture. This means that data subjects could gain stricter control over their personal data while helping data controllers meet the requirements imposed by the GDPR (e.g., for the traceability of consent).[18]

2. Blockchain in a nutshell

Based on the above considerations, this section provides an overview of the characteristics constituting a blockchain. While a detailed presentation of the features underlying this new paradigm[19] is beyond the scope of the article, this analysis requires some of the technical key mechanisms to be addressed. These include the core concepts of decentralisation, transparency, and immutability that are also shared by other distributed-ledger technologies. This article will therefore clarify how blockchain works, the function of the consensus protocol, and ultimately, the differences among all types of blockchains (i.e. public, private and consortium).

2.1. The three pillars: decentralisation, transparency, and immutability

First and foremost, any overview of blockchain must commence with the consideration that there is not simply just one version of this technology. Rather, blockchains are both a class of technology for data storage but also programmable platforms that enable new applications

[15] Interestingly, blockchains can also be shaped as decentralised data solutions fitting in the so-called data marketplaces, that are digital marketplaces where personal and non-personal data can be traded as commodities (for instance, blockchains may enable data sharing without the need of a central trusted intermediary).
[16]G.W van Blarkom, J.J Borking, J.G.E. Olk, *"PET", Handbook of Privacy and Privacy-Enhancing Technologies* (College bescherming persoonsgegevens 2003)
[17] In the Opinion on Personal Information Management Systems (9/2016 – para 49) the European Data Protection Supervisor stressed that personal information management systems 'may facilitate compliance with GDPR'.
[18] See CNIL, *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data* (2018), < https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>.
[19] Arvind Narayanan and Jeremy Clark, *Bitcoin's Academic Pedigree* (2017) Communications of the ACM 36: rather than being a completely novel technology, blockchain is better known as an inventive combination of existing mechanisms. Almost all the components in fact originated in academic research from the 1980s to 1990s and many digital currencies (such as Digicash, for instance) can trace their origins as far back as 1989.

such as smart contracts.[20] As a matter of fact, various definitions of blockchains[21] exist and they highlight different technical features of the respective forms of data management.

The term 'blockchain'[22] refers to a technology that allows the creation and management of a decentralised and distributed digital ledger in which data, usually called 'transactions', is stored, recorded in chronological order, transferred and finally shared among the nodes[23] participating in the network. The latter are hardware devices able to communicate with others in the so-called peer-to-peer network.

As a result, a blockchain allows for the storage and transmission of information in a transparent and secure manner without the need to rely on a trusted third party. As its etymology reveals, it is structured as a series of encrypted blocks[24] which are 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 the process of using an algorithm to transform data of any size into a unique fixed-sized output.[25] Cryptography[26]

---

[20] Pieces of code stored on a blockchain that will self-execute once deployed. In more detail: Blaise Carron and Valentin Botteron, *How smart can a contract be?,* in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar 2019).

[21] Given the lack of definitional consensus, the author will use both singular and plural.

[22] Michael Nofer, Peter Gomber, Olivier Hinz and Dirk Schiereck, *Blockchain* (Business and Information Systems Engineering 2017) 183-187; Bikramaditya Singhal, Gautam Dhameja and Priyansu Sekha Panda, *Beginning Blockchain – a beginner's guide to building blockchain solutions* (Springer 2018); Vikram Dhillon, David Metcalf and Max Hooper, *Blockchain enabled application* (Springer 2017).

[23] Nodes can be divided into full nodes and light nodes. A full node contains a full copy of all the transactions that have ever been performed on the blockchain. Accordingly, a 'mining node' able to validate the new transactions requested by participants always needs to run a full node to select valid transactions to form a new block. Full nodes are thus essential to ensure the integrity of a blockchain by downloading and verifying the whole chain of blocks. Nonetheless, taking into account that this operation is costly in terms of time and resources, a participant that is unwilling to engage in this effort can be a 'light node'. Light nodes do not interact directly with the blockchain but they can send transactions by using full nodes as intermediaries. This enables them to only keep a partial copy of the whole chain of transactions.

[24] 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 of the transactions that are 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 Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Godfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press 2016).

[25] It is relevant to stress that a hash cannot be reversed, thus making it not possible to run the hash functions backwards for finding the piece of information based on the string of numbers. Decentralisation in the blockchain is reached through a *consensus mechanism* by which the miners verify and validate the information; once the piece of information is validated, it is then chronologically registered in blocks to make the data impossible to be altered. However, it is to be noticed that this is true as a matter of principle due to possible exceptions. See Aatif Jamshed, Megha Bhardwaj, Medhavi Pandey and Krishna Kant Agrawal, *Securing through pseudorandom number generator and hashing in cryptography: review* (2019) JETIR 203-206.

[26] Another important cryptographic tool is the public key infrastructure (PKI). It enables participants in a blockchain to digitally sign transactions while remaining pseudonymous. 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 key (both are strings of letters or numbers representing the user). The former is an account number shared with others to enable transactions; the latter is

is indeed a blockchain's distinctive architectural element and it ensures its immutability. In short, this means that, once recorded in a given block, data cannot be retroactively altered, unless all subsequent blocks are altered.[27]

Accordingly, before being added to the chain, each block has to be checked, validated and executed according to the chosen validation protocol (consensus algorithm or consensus mechanism).[28] The consensus algorithm defines what the validating algorithms are and who can be a miner. For example, who can verify the validity of the information that a node contains before being added to the blockchain. Thus, the validation protocols are a distinctive element of this new technology as they govern how information can be added to the shared repository. Namely, it is a method for choosing how blocks are added to the blockchain. They also ensure that the content of each block (i.e., transactions) is consistent across the whole network so that every node has the same version of the blockchain. To verify the authentication of the transactions, digital signature based on asymmetric encryption (public and private keys) is generally applied. These are both strings of letters and numbers: the public key represents the user while the private key is like a password. The typical digital signature includes two phases: the signing phase and the verification phase. When a node creates a transaction, this is signed by the node's private key. Once other nodes receive the transaction, the initiator's public key is used to verify the authentication of the received transaction.[29]

instead a password usually generated using a secure random function necessarily known only by its owner so as to create a digital signature through an algorithm. The mathematical relationship between these keys allows the private key to decrypt data encrypted through the public key. This means that once the transaction is digitally signed, the public can use the sender's public key to verify that it was made by the owner of the pair. Therefore, other users are enabled to verify that the pseudonymous owner of a public key performed a transaction, but they cannot trace the public key back to the private one, unless they add additional information. See Dylan Yaga, Peter Mell. Nik Roby and Karen Scarfone, *Blockchain Technology Overview* (2018) Draft NISTIR US Department of Commerce, National Institute for Standards and Technology, <https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf>

[27] This is not completely true and may be misleading, as there are particular and extraordinary circumstances in which data can be manipulated. For instance, it is possible that various participants collude to change the state of the ledger, but this would be extremely hard and expensive since the blocks are linked through hashes. See, Daniel Conte de Leon et al, *Blockchain: Properties and Misconceptions* (2017) APJIE 286, 290; Kevin Werbach and Nicolas Cornell (2017), *Contracts Ex Machina* (2017) Duke Law Journal 313, 335; Primavera De Filippi and Aaron Wright, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (2015) <https://ssrn. Com/abstract=2580664> 4; Michèle Finch, *Blockchains: Regulating the Unknown* (2018) Ger. Law J. 665, 670.

[28] The *consensus mechanism*s make possible for distributed network of peers to store information in a blockchain without the need to rely on any centralised operator or middleman. See Arvind Narayanan et al, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (n 4).

[29] F. Richard Yu, *Blockchain Technology and applications – From theory to practice* (Independent publisher 2020).

Blockchain is quite often compared to the Internet.[30] However, there is no single model or set of standards for blockchain systems that come in different forms and shapes, some of which are better suited to deal with data privacy issues more effectively than others.

There are also broadly three blockchain categories: private, public and consortium[31].

A private blockchain creates a group of known participants who work in a closed but decentralised network where access needs to be validated by an organization or entity. Reading rights can be granted to nodes that belong to the network or to selected external nodes.

In public blockchains, anyone can join the network to participate in the consensus process, read and access the information, as well as maintain the shared ledger (e.g., Bitcoin and Ethereum).

Consortium blockchains, on the contrary, sit on the fence between public and private blockchains, combining elements from both. They are not open systems, considering that a predetermined group of nodes can access the network (a minimal number of participants who are also known). However, this type of blockchain is at the same time semi-decentralised since it runs under the supervision of members from limited groups. Additionally, consortium blockchains have multi-party consensus, as all operations are verified by a selected number of nodes. Similarly, reading rights can also be controlled here.

To conclude, permissioned blockchains are open only to predefined subjects, whereas permissionless blockchains allow all those who have technical capacity to participate. Private and consortium blockchains are mostly (but not necessarily) permissioned, while public blockchains are mostly permissionless. This difference will be used further in this article.

3. Privacy vs decentralisation: State of play

It is now necessary to review the foundation of data protection law to focus on the interplay between blockchains and GDPR. It has already been highlighted that this interaction gives rise to a wide range of questions. Since it is not possible to delve into each question, this article will address the most significant ones. Before beginning this analysis, an introduction to the GDPR is required.

---

[30] See Don Tapscott and Alex Tapscott, *Realizing the Potential of Blockchain, A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies*, in White Paper, World Economic Forum (2017), <www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf>: in this report the authors describe BC as a new global resource, like the internet, that requires global stewardship.

[31] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and Robbert van Renesse, *Bitcoin-ng: A scalable blockchain protocol* (2016) Proc. 13th USENIX Symposium on NSDI, <https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal> 45-49.

The GDPR is the EU's landmark data protection legislation and it represents a proactive response to the challenges posed by technological developments. The decision to repeal the previous directive[32] marks a significant evolution in data protection law. Further, it creates a stronger, much more coherent, and harmonised framework for data protection rights recognised by primary EU law.[33]

The GDPR pursues a twofold objective: it strives to facilitate free movement of personal data among the EU's various Member States while providing a detailed framework to give effect to the fundamental right of data protection. However, it is worth noting that this right is not absolute and must be balanced against other fundamental rights in conformity with the principle of proportionality (article 52 Charter of Fundamental Rights of the European Union[34]).[35]

Because it applies to any personal data of individuals in the EU, the material and territorial scope[36] of the Regulation is broad. It is nevertheless essential to consider that blockchains are not data processing operations by themselves, but rather technology for different functions. Hence, the key question is not whether the GDPR applies to the blockchain, but more precisely, whether these functions comply with the regulation.

Relevant experts' studies identify possible tensions between data protection law and the blockchain.[37]

First, as already affirmed, immutability is one of the core concepts underlining blockchain's infrastructure. Data is indeed recorded in an immutable manner, so that its erasure or modification, in principle, is not possible. This blockchain feature seems to conflict with the GDPR's assumption that data can be erased, or at least modified where necessary, to comply with article 16 and 17. Nonetheless, based on interpretative guidance by the European Data

[32] 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, GU L 281 del 23.11.1995.
[33] Article 8 of the Charter of fundamental rights, CFR, states that everyone has the right to access personal data relating to them, as well as that personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. Moreover, Article 16 TFEU claims that everyone has the right to the protection of personal data concerning them, providing that the Parliament and the Council '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.'
[34] 2000/C 364/01
[35] Recital 4 GDPR.
[36] *Ivi,* articles 2 and 3.
[37] EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) II.

Protection Board (EDPB) and European Court of Justice (CJEU), data erasure does not entail an outright deletion of data.

Second, to assess compliance with data protection, this section must address the identification of the data controller who is responsible for data processing and whom data subjects can address to enforce their rights. The definition of roles and the allocation of responsibilities could be a real challenge in public permissionless blockchain where there is not a single legal entity that makes decisions.[38] Furthermore, recent rulings of the CJEU have held that joint controllership - which in the GDPR has uncertain contours - is much more complicated, particularly in relation to the principle of accountability[39] and then to the allocation of responsibilities. While there may be a lack of consensus, this article will now address whether data stored on the blockchain can be considered personal data.

Section 3 defines the concept of personal data and the related notions of anonymisation and pseudonymisation. This leads to evaluating whether data contained in a blockchain is personal data under the GDPR. Secondly, it will assess whether data subjects can invoke the right to be forgotten which seems to be difficult to apply to the blockchain system. Finally, the article will determine who the GDPR obligations address (i.e., the identification of the data controller).

3.1. Does data stored on a blockchain qualify as personal data?

The core of the GDPR is the protection of users' data.[40] Its material scope is wide[41] and it applies to the processing of personal data wholly or partly by automated means. In addition,

[38] *Ivi,* 43: 'Regarding public and permissionless blockchains the given governance arrangements influence the modalities of the means of processing. As a general rule, there is not a single legal entity that decides which software, hardware and data centers to use. Rather, these decisions are made by a range of different actors. To illustrate, in proof-of-work systems, miners make the decision of what hardware (for mining) and data centers (for mining) to use whereas core developers suggest whether and if so how software should be updated.300 Depending on the chosen governance set-up, miners, nodes and/or coin holders then make a decision as to what software to actually implement.'

[39] Article 5(2) GDPR mandates that the data controller is responsible for and should be able to demonstrate compliance with the requirements under Article 5 GDPR.

[40] The GDPR sets out special categories of personal data, whose processing is subject to stricter regulation. These more sensitive categories include those data revealing racial or ethnic origins, political opinions, religious beliefs and health information. In contrast to the Directive, the GDPR adds special categories of 'sensitive data' which include both biometric and genetic data.

[41] Article 4 GDPR provides for a broad definition of personal data, namely any information relating to an identified or identifiable natural person (i.e. data subject), including names, addresses, identification numbers, location data, and IP addresses. Also, the recent ECJ case law has clarified some uncertain aspect of this concept: Case C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland* (2016) ECLI:EU:C:2016:779, para 36. On the notion of personal data, see also C-434/16 *Peter Nowak v. Data Protection Commissioner* (2017) ECLI:EU:C:2017:994. In *Breyer* the ECJ considers that even dynamic IP addresses (i.e. provisional addresses which are assigned for each internet connection and change from time to time) may also constitute personal data (for more on this ruling refer to footnote 50).

it applies to non-automated processing of personal data, if the personal data forms part of a filing system or is intended for this purpose.

The relevant criterion to define data as personal is that of identifiability. This is an uncertain standard as the regulation does not clarify what elements ought to be adopted to assess the risk of identification. In this regard, the distinction between personal and non-personal data is likely to vanish over time, especially because increasingly advanced techniques, together with all the means reasonably likely to be used, must be considered when determining a possible risk of re-identification (recital 26).[42]

As far as the notion of personal data is concerned, the concepts of anonymisation and pseudonymisation[43] are of pivotal importance. While anonymous data falls outside the scope of the legal framework as it is impossible to trace back information to a living individual, pseudonymous data continues to qualify as personal, as long as the indirect identification of a natural personal by an identifier remains possible. Anonymisation is defined in the GDPR 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'.[44] Hence, personal data that has been irreversibly anonymised would not fall within the scope of the GDPR. This means that allegedly, the GDPR would not apply.

It has already been pointed out when explaining permissionless blockchains, that this type of blockchain relies on hashing and public/private key cryptography.[45] Hashes enable the efficient storage of transactions in a format that permits their verification, while public/private key cryptography provides the means to validate the sender and the receiver of a transaction.

Similarly, permissioned blockchains integrate those techniques in their protocols for privacy reasons rather than efficiency.

So, what about personal data in the blockchain environment?[46]

---

[42] Michèle Finck and Frank Pallas, *They who must not be identified—distinguishing personal from non-personal data under the GDPR* (2020) Int'l Data Privacy Law 11-36.

[43] Art 4(4) GDPR: pseudonymisation is the processing of personal data in such a manner that 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 or organizational measures to ensure that the information is not attributed to an identified or identifiable natural person.

[44] Recital 26 GDPR. In its opinion on Anonymization techniques (05/2014, WP 216) adopted on 10 April 2014, the Article 29 Working Party provided guidance on the difference between pseudonymised and anonymised data, from which various legal consequences stem. According to the document, in order to qualify data as truly anonymous, each anonymisation technique has to be analysed in light of the following three questions: (1) is it still possible to single out an individual? (2) is still possible to link records relating to an individual? (3) can information concerning an individual be inferred?

[45] (n 26).

[46] The participant identifiers, i.e. the public keys, are essential to the proper functioning of the blockchain, therefore it is not possible to minimise them.

Experts and good practice recommend[47] not storing personal data in a clear text on the blockchain (i.e., off-chain storage) especially in public permissionless blockchain. However, there might be business or policy reasons to put personal data directly on the chain. Should this be the case, personal data or a commitment or a hash are stored on chain.[48] In those cases, two risks shall be addressed: the reversal risk – that is the possibility to reverse cryptographic processes, so as to reconstitute the original data - and the linkability risk, i.e. the prospect of linking encrypted data to an identity through comparison with the original document.

Indeed, applying those concepts to a decentralised environment triggers the question of whether encrypted or hashed personal data is still personal data. The mere use of a hash function[49] does not automatically entail that the data is anonymous.[50] With respect to encrypted or hashed data, data is still classified as personal, as it falls under the category of pseudonymised data. Essentially, pseudonymisation gives the organisation more leeway for processing because the hazards are correspondingly lower. Yet, the European Blockchain Observatory and Forum, in an effort to balance different rights, stated that: 'It would be beneficial to the blockchain industry that a hash in this context is not systematically interpreted by the EDPB as personal data'.[51] In this respect, it is worth mentioning that some hash functions – such as 'salted' or 'peppered' hash – offer stronger privacy safeguards.[52] Thus, some argue that data complies with the test under recital 26 GDPR ('means reasonably likely to be used') and does qualify as anonymous data.

Finally, a note on public keys which are account numbers for each user to share with others to enable transactions. Recently, practice has revealed that public keys combined with

[47] Jacob Eberhardt and Stefan Tai, *On or Off Chain the Blockchain? Insights on Off-Chaining Computation and Data* (2018), < https://allquantor.at/blockchainbib/pdf/eberhardt2017or.pdf>.
[48] According to the CNIL guidance (n 18), in order to ensure compliance with privacy by design, default and data minimisation, solutions where data is processed outside the blockchain are preferable.
[49] (n 25).
[50] In its opinion on Cloud computing (5/2012, WP 196), the Article 29 Working Party sustained that encryption 'may significantly contribute to the confidentiality of personal data if implemented correctly' but ' it does not 'render personal data irreversibly anonymous.'
[51] *Blockchain and the GDPR –The European Union Blockchain Observatory forum* (n 8) 30.
[52] *Ivi*: '[These techniques involve] adding extra information to the data to make it large enough that a brute force attack would be extremely unlikely to reverse the data in, say, the next fifty years'.

additional information[53] can reveal the identity that is hidden behind the address account.[54] Some commentators have noted that public keys may constitute personal data under the GDPR.[55] The French Commission nationale de l'informatique et des libertés (CNIL) and the EU Observatory and Forum on Blockchain have reached the same conclusion. The latter, in particular, has raised more concerns on the linkability risk.

While a scrupulous case-by-case analysis is undoubtedly necessary, based on current experts' opinion,[56] it can be stated that public keys - directly or indirectly related to an identified or identifiable natural person - qualify as personal data under data protection law. Anyhow, to prevent the risk of identification, technical and organisational measures need to be taken.

This analysis provides the foundation for focusing on the implications of blockchain on the right to be forgotten in the following section.

3.2. The right to be forgotten through the prism of blockchain

Article 5 GDPR builds upon the overarching principles[57] governing the regulation and provides a set of detailed rights for individuals.[58] From a technical perspective, there is no

[53] Note that it is possible to trace a parallel with C-582/14, Patrick Breyer vs. Bundesrepublik Deutschland (2016) relating to dynamic IP addresses. The Court of Justice stated that dynamic IP addresses collected by an online media service provider only constitute personal data if the possibility to combine the address with data necessary to identify the user of a website held by a third party (i.e. user's internet service provider) constitutes a means 'likely reasonably to be used to identify' the individual or a third party, with the caveat that 'if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.'

[54] EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 27: 'There have been instances where data subjects have been linked to public keys through the voluntary disclosure of their public key to receive funds; through illicit means, or where additional information is gathered in accordance with regulatory requirements, such as where cryptoasset exchanges perform Know Your Customer and Anti-Money Laundering duties. Wallet services or exchanges may indeed need to store parties' real-world identities in order to comply with Anti-Money Laundering requirements while counter parties may do so, too for their own commercial purposes'.

[55] Matthias Berberich and Malgorzata Steiner, *Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?* (2016) EDPL 422-426.

[56] EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 27.

[57] Without dwelling too long on the subject, it is worth to say that the core privacy principles are lawfulness, fairness and transparency towards data subjects; the processing of data has to be made in accordance with the purpose for which the data were collected (purpose limitation); information has to be kept accurate and up to date (accuracy); the processing has to be limited to what is necessary (data minimization); the integrity and security of the data have to be guaranteed (integrity and confidentiality), and finally data have to be stored for no longer than necessary.

[58] Articles 12-22 GDPR.

friction with the right to access[59] and the right to data portability.[60] The exact application and respect of these rights are not so problematic in the blockchain environment. Indeed, the article argues that data portability solutions could help data subjects gain more control over sharing their personal information.

Things may become complicated in respect of the right to be forgotten and the right of rectification,[61] as they seem barely compatible with the decentralised structure of such a blockchain system where data once registered cannot be deleted or amended.

In essence, the main feature of the blockchain (strong immutability and inalterability) may fully collide with the intrinsic assumptions of those rights. This conflict - surely exacerbated when it comes to public permissionless blockchain - is rooted in two fundamentally different philosophies/ontologies on how to best protect data privacy.

On the one hand, the GDPR has broadened the scope of the right to be forgotten, which was already recognised in case law.[62] The GDPR empowers any data subject to ask for the correction or even deletion of personal data that affects them when one of the grounds listed in article 17 applies. In that case, the controller has the obligation to erase that personal data without undue delay.

Nonetheless, the right to be forgotten is not an unconditional right and many exceptions apply, so the data subject does not have an absolute right to obtain the erasure of data concerning them as they please.

On the other hand, the GDPR does not specify what qualifies as 'erasure'. [63] It seems that the obligation inherent to article 17 GDPR does not have to be necessarily interpreted as

[59] Pursuant to the right of access, the data subject shall have the right to obtain confirmation from the controller as to whether personal data concerning them are being processed, and, where that is the case, to access such data and receive some additional information (including what the purpose of the processing is and who the recipients or categories of recipient are to whom the personal data have been or will be disclosed).

[60] The right to data portability, recognised for the first time in the GDPR, allows individuals to obtain and reuse their personal data for their own purposes across different services in a commonly used and machine-readable format. It provides data subjects with the possibility to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. In addition, the data subjects have the right to transmit those data to another controller without hindrance from the controller to whom the personal data have been provided.

[61] Article 16 GDPR provides the data subject with the right to obtain from the controller the rectification of inaccurate personal data concerning them without undue delay.

[62] C-131/12, *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzàles* (2014) ECLI:EU:C:2014:317 in this case the delisting of information from research results was considered to amount to erasure.

[63] The GDPR is a regulation, so it does not require implementation under article 288 TFUE. Nevertheless, there is the possibility that certain national laws implement the notion of 'erasure'; for instance, the German framework provides that data is not deleted in cases of non-automated processing if the specific mode of storage makes it possible (Article 35 of the Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 and zur Umsetzung der Richtlinie (EU) 2016/680).

requiring the outright destruction of data.[64] Similarly, the qualified right to erasure does not oblige blockchain members to delete personal data if a valid purpose still exists to process that data. This right may be ensured on a granular level by considering the impact on and of various technologies.[65]

The question of whether 'erasure' always amounts to destruction per se is unclear, even if case law and interpretative guidance indicates that it does not. According to a recent EPRS report, the issue that originated the case *Google Spain* '[…] may be taken as an indication that what the GDPR requires is the obligation resting on data controllers to do all they can to secure a result as close as possible to the destruction of their data within the limits of their own factual possibilities.'[66] The delisting of information from search results was indeed considered to amount to erasure, although it was the only request the applicant made to Google.

Furthermore, what also emerges from the above-mentioned report is that erasure does not mean destruction. This was also submitted by the Cloud Computing Opinion of the Article 29 Working Party,[67] as well as by considerable data protection authorities (particularly the Austrian[68] and the UK[69] Data Protection Authorities (DPAs)). They all agree that these technical solutions may be satisfactory.

However, there is no *consensus* among DPAs. Thus, the question still arises whether the threshold of erasure under the GDPR can be met without erasure itself occurring in the literal sense. Regulatory and/or interpretive guidance are much needed.

In the meantime, some practical solutions implementing the 'right to erasure' on blockchain can be explored. The following remarks are based on the idea that the right of erasure does not equate to a complete destruction of data. Further, the protection of data subject

---

[64] In its opinion on cloud computing, the Article 29 WP (Opinion 5/2012 on Cloud computing, WP 196 01037/12/EN, 12) considered that the destruction of hardware could qualify as erasure for the purpose of Article 17 GDPR. Therefore, the EDPB's *Guidelines on the Criteria of the Right to be Forgotten in the Search Engine Cases,* n. 5/2019 clarify that a request by an individual under Article 17 GDPR entails the delisting of particular content that would not involve their personal data being completely deleted. Pursuant to the Guidelines, the right to be forgotten does not usually require that personal data be erased from the source website, nor from the indexes or caches of the search engine operator.

[65] Article 17(2) GDPR provides that, if faced with a request for erasure, the data controller shall take 'account of available technology and the cost of implementation' when data are public and processed by other controllers. Hence, the question arises as to whether the notion of 'available technology' – which leaves room for a broad interpretation - could be understood in a way that leads to alternative solutions to the outright erasure.

[66] EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledger be squared with European Data Protection Law?* (n 8) 76.

[67] (n 47).

[68] Austrian Data Protection Authority, DSB-D123.270/0009-DSB/2018 (05 December 2018) https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB _D123_270_0009_DSB_2018_00.html.

[69]<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/>

can be achieved by severing the link between personal data stored on the blockchain and original information. Thus, it is worth considering both the aforementioned recommendations on pros and cons of on chain/off-chain storage solutions and the suggestions on responsibilities of the platforms stemming from the *Google Spain* case.

In *Google Spain*, the delisting of information from search results was considered sufficient. By analogy, the application of the ECJ case law to the blockchain environment lends itself to affirming that, in practice, the deletion of data may be required from the data controller of the blockchain's applications who will erase data stored off-chain. According to the EPRS report: 'This may be taken as an indication that what the GDPR requires is that the obligation resting on data controllers is to do all they can to secure a result as close as possible to the destruction of their data within the limits of their own factual possibilities'.[70]

Another solution is to destroy the private key that decrypts personal data stored on chain. Both options exclude the possibility to reverse and/or link the encrypted value stored on chain with the original information.

A parallel rationale applies to the right of rectification: the updated data can be entered in a new block, even though the first transaction will still be visible; nevertheless, data in the first block can be made inaccessible.[71]

Beyond the difficulties surrounding the right to be forgotten, other related concerns are grounded in the issue of identifying the roles prescribed under data protection law. Indeed, there is the idea that within a blockchain-enabled data processing operation it is not possible to determine the identity of the data controller (and possibly the data processor). Thus, the article argues that these concepts should be functional and based on a factual rather than formal analysis as the determination of controllership is informed by 'an actual activity [of the participant] in a specific situation, rather upon formal designation.'[72]

3.3. Who is the data controller?

The GDPR[73] is technology neutral and defines the data controller as the natural or legal person who 'determines the purposes and means of the processing of personal data'. The

[70] EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledger be squared with European Data Protection Law?* (n 8) 76.
[71] CNIL report (n 18) 9.
[72] EDPB, *Guidelines on the concepts of controller and processor in the GDPR* (07/2020), <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_it>
[73] To complete the "player's list", it is necessary to add references to the data processor who, pursuant to article 4(8) GDPR, is 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. However, not every personal data processing operation necessarily involves a data processor, as they are not an indispensable player.

identification of the controller (or the joint controllers)[74] is far from a purely theoretical issue. It is crucial for two reasons. Firstly, it guarantees the respect of the principle of accountability[75] by clarifying who must comply with the GDPR obligations.[76] Secondly, it allocates the responsibilities for ensuring the rights of data subjects.

The identification of the data controller is certainly complicated due to the decentralisation of control over data at network level. In this respect, there is no agreement on who should be the controller of a given blockchain-enabled data processing operation. Most of the expert studies[77] fall short of providing an affirmative definition of who qualifies as data controller in blockchain infrastructures. The analysis reveals that 'controllership cannot be determined in a generalised manner [so] a case-by-case analysis accounting for technical and contextual factors ought to be carried out.'[78] Arguably, the remarks formulated by the French DPA (CNIL) may help solve the issue.

As stated above, permissionless and permissioned blockchains differ by the degree of decentralisation. When dealing with permissionless blockchain networks, it is much more difficult to identify the data controller as these are widely distributed open networks and all users are engaged in the data processing. There is thus no central operator or administrator who determines both purposes and means of data processing.

Given the fact that nodes have access to all data, it has been suggested that they may be controllers[79] because they are not subject to external instructions, but rather autonomously

---

[74] At articles 4(7) and 26, the Regulation also defines the joint controller, i.e. the person who - together with the data controller - determines the purposes and means of the processing, as well as their respective responsibilities for compliance with the obligations under the GDPR. For more on the issue, see J.P. Pesch and Christian Sillaber, *'Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements* (2017) Comput. Law Rev. Int. 169-171; and also Case C–40/17 *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* (2019) ECLI:EU:C:2019:629; Case C210/16 *Wirtschaftsakademie Schleswig-Holstein* (2018) ECLI:EU:C:2018:388; Case C-25/17, *Jehovah's Witnesses* (2018) ECLI:EU:C:2018:551.

[75] Ricardo Neisse, Gary Steri and Igor Nai-Fovino, *A Blockchain-based Approach for Data Accountability and Provenance Tracking* (2017) EC JRC; Uwe Roth, *Blockchain Ensures Transparency in Personal Data Usage: Being Ready for the New EU General Data Protection Regulation* in *Special Theme: Blockchain Engineering* (2017) ERCIM News 32; Edward Felten *Blockchain: What is it good for?* (2018) <https://freedom-to-tinker.com/2018/02/26/bloc>.

[76] Among others: informing data subjects of what is happening with their data and ensuring they have means and knowledge to exercise their rights; conducting data-protection impact assessments, which according to article 35 GDPR are 'an assessment of the impact of the envisaged processing operations on the protection of personal data'.

[77] See, *Blockchain and the GDPR –The European Union Blockchain Observatory* (n 18) 17-18; EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 44-51.

[78] *Ivi,* 52.

[79] J.P Pesch and Christian Sillaber, *Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements* (n 74) 169: 'in the absence of central governance, [each participant] is free to choose and configure their hard- and software and to define internal data protection policies, every participant at least controls the data processing that takes place in their own system…Therefore, participants…can be classified as

decide whether to join the chain. This hypothesis overlooks the fact that nodes only contribute to the practical maintenance of the system. It seems much more reasonable to consider the identity as a data controller with a written permission (e.g., a notary who uploads a document received from a client on the blockchain). This view is also shared by the CNIL.

Nonetheless, other authors when considering the decentralised nature of blockchains' system argue that nodes might also act as processors due to the fact that the entire transactional history is stored on the blockchain.[80]

It is widely agreed that miners are not data controllers. They only validate transactions requested by participants. Thus, they are not involved in the definition of the purposes and means of the processing. It is still worth noting that 'they exercise control over the means in choosing which version of the protocol to run'.[81] Further, 'as such their role has been compared to that of telecommunication providers that are not legally liable for the content of the data they transmit.' [82]

Experts argue that users can be considered data controllers when they directly make the transaction and submit personal data to the chain as part of a business activity.[83] Indeed, they are the only persons able to determine the purposes and influence the means of data processing (such as the format of the data and the choice to use a blockchain instead of other technology). To deepen these reflections, it can be added that this scenario – namely users submitting information for business purposes – ought to be distinguished from the case where users send their own data for personal use. In such a case, it is not guaranteed whether they are likely to fall under the 'household' exemption[84] if a public and permissionless blockchain is used. Data is in fact shared with an indefinite number of persons.

---

controllers according to the GDPR'. See also EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 47: 'each node that initiates a transaction or that saves a transaction in its own copy of the database is a controller, considering that in doing so, the node pursues its own purpose: participation in the network.'

[80] European Parliament, *Report on Blockchain: a Forward-Looking Trade Policy* (2018) A8-0407/2018, 22. Also, some academics [here no academic sources are sited, only EU reports – to add] have suggested that nodes could be seen as joint controllers, as they 'have equal influence and freedom to choose (or start) a certain blockchain-network— and can [in certain instances] change the rules' of the network (EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 47).

[81] *Ivi,* 46.

[82] *Ibidem.*

[83] As the CNIL pinpointed (n 18, 3), in such scenario the household exemption (i.e. under article 2 GDPR) does not apply because the purpose of the transaction is professional or commercial.

[84] Article 2(2)(c) GDPR. According to Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) – A commentary* (2020 Oxford University Press): 'It follows from both *Lindqvist* and *Ryneš* that the exclusion of purely personal or house- hold activities must be interpreted as covering only activities that are carried out in the context of the private or family life of individuals. In that connection, an

As regards the possible overlap between data subject and data controller, it is 'an open question whether [this] would be compatible with the broader underlying objective of the GDPR, which was designed precisely to give data subjects rights vis-à-vis controllers in a context of unbalanced power-relations.'[85] This intersection can be seen from two perspectives. First, the overlap may shift responsibility to users who might be unaware of the complex data processing implications. Second, it may help data subjects strengthen the management system of their personal data in view of furthering data sovereignty. While these insights are helpful, additional clarification is required.

It is important to note, by way of conclusion, that the GDPR's broad definition of controllership has far-reaching implications for personal data processing based on DLT.

The current state of the law makes it very difficult to distinguish between different roles due to blockchain design and governance features[86] that apparently hamper the identification.[87]

4. Privacy-enhancing solutions: an overview

In addition to explaining the points of tension between blockchains and GDPR, this article further shows that the technology can be developed to be data-protection law-compliant through the application of the principle of privacy by design.

The underpinning argument of the article is that the blockchain can be structured to support advanced techniques implementing privacy-enhancing solutions for decentralised data management. This can therefore increase the autonomy and ownership of data subjects.

The idea of shaping technology according to data protection principles – among others data minimisation and privacy by design and by default - is not new and it leads to the term Privacy Enhancing Technologies (PETs). This refers to a range of technologies designed to support data protection and privacy. In this regard, recital 7 GDPR foresees that '[n]atural persons should have control of their own personal data'. The same logic is evident regarding

activity cannot be regarded as being purely personal or domestic where its purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends, even partially, to a public space and is accordingly directed outwards from the private set- ting of the person processing the data in that manner.'

[85]EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 50.

[86]Michèle Finck, *Blockchain Regulation and Governance in Europe* (2019 Cambridge University Press); European Commission, '*Commission Staff Working Document on the free flow of data and emerging issues of the European Data Economy'* (SWD/2017/02 final).

[87]EPRS, *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* (n 8) 55: 'The current state of the law makes it moreover difficult to distinguish between data controllers and data processors. The combination of DLT's polycentric design and the current state of the law burdens the determination of data controllers in such networks.'

data subject rights such as the right to data portability (article 20) and right to access (article 15). These articles give data subjects control over what the data controller (or others) do with personal data relating to them as well as the possibility to decide on who should have access to their personal data.

An increasing amount of guidance and reports have addressed the issue of applying the GDPR to a decentralised data system such as blockchain. The foundation for all these documents issued by, among others, the European Data Protection Board, European Parliament,[88] European Data Protection Supervisor[89] and Data Protection Authorities (CNIL in particular) is that the technology might be a useful tool to achieve some of the GDPR's underlying objectives while preserving the blockchains' characteristics of a trusted and human-centred infrastructure.

The European Parliament indeed defined the DLT system as a 'tool that promotes the empowerment of citizens by giving them the opportunity to control their own data and decide what data to share in the ledger, as well as the capacity to choose who else can see them.'[90] At the same time, it stressed the importance of a decentralised system for self-sovereignty, identity, and trust, thus postulating the privacy-enhancing potential of blockchain and DLT in general.

At EU level, there is a wide range of projects demonstrating that blockchain can be used to achieve these objectives. An example is the Decode Project, whose slogan is 'Giving people ownership of their personal data.' The project seeks to provide tools that 'put individuals in control of whether they keep their personal data private or share it for the public good'.[91] The goal is also shared by the MyHealthMyData project[92] which features a data management structure where data subjects can allow, refuse and withdraw access to their sensitive data based on different cases of potential use. Security and data protection are accordingly increased, and this is of paramount importance in sectors like health data management which require both more attention due to the sensitivity of data processed and a faster pace to achieve processing purposes (as the Covid-19 pandemic has shown).

This brief overview has highlighted that there is an open and vivid debate on the development of tools capable of achieving GDPR objectives. These projects reveal that it is

[88] Opinion of the Libe Committee for the Committee on International Trade on blockchain: *a forward-looking trade policy, European Parliament* (2018/2085(INI)); EP Resolution of 3 October 2018 *on distributed ledger technologies and blockchains: building trust with disintermediation*, P8TA(2018)0373.
[89] European Data Protection Supervisor, *Opinion 9/2016 on Personal Information Management Systems* (n 17).
[90] EP Resolution of 3 October 2018 (n 87) A.
[91] https://decodeproject.eu/.
[92] http://www.myhealthmydata.eu/

possible to use blockchain to minimise the risk of manipulation and even gain more control over personal information. It is, however, clear that we are not talking about an automatic mechanism, rather the focus is on ad hoc solutions and use cases. Each tool needs to be assessed on its own merits on a case-by-case analysis.

In conclusion, when it comes to evaluating GDPR compliance, while it is possible to set some key requirements, it is not feasible to state whether a technology or a use case is by default data-protection compliant.

5. Final remarks and key takeaways

At first glance, some GDPR provisions seem ontologically incompatible with the main blockchain characteristics. Hence, manifold points of tension have been identified.

This article focused on three overarching questions that the author considers the most challenging, (i) does data stored on blockchain fall within the scope of the GDPR? (ii) should the right to be forgotten be abandoned due to the blockchain's immutability? (iii) who is the data controller in blockchains?

It is against this backdrop that possible solutions based on living technologies have been outlined and the idea that the blockchain can serve as enabler to achieve GDPR's objectives has been finally illustrated. Both the technology and the regulation share the purpose of strengthening data subjects' control over their personal data. At this stage, some EU-supported projects already exist that explore technical and governance solution to use blockchain as a privacy enhancing technology.[93]

It is worth noting that the starting point for any of the above considerations and, specifically, the argument progressed in this article, is that the interplay between blockchains and GDPR can only be assessed by adopting a case-by-case analysis. Furthermore, the article elaborated on some considerations regarding the fact that permissioned blockchains appear to be more suitable for the regulation.

Whereas some have called for a revision of the regulation claiming it is already outdated,[94] the article argued that the technological neutral structure of the GDPR allows for a different interpretation of some of its requirements and provisions. Regulatory flexibility might be the key to address those issues. The most illustrative example is that of the right to be forgotten which can be interpreted in as many different ways as there are different definitions

[93] Decode and MyHealthMyData projects (n 90-91).
[94] Some authors sustained that, even before the GDPR entered into force, it was already partly outdated: see for instance Tal Zarsky, *Incompatible: The GDPR in an Age of Big Data* (2017) Seton Hall L. Review.

of ‘erasure’. Thus, an initiative by the regulators or interpretative guidance by DPAs are necessary to shed light on those (arguable) problems.

Another essential point to focus on is that the regulation and the blockchain should foster a dialogue when the technology is in the design phase. This means that regulators and developers must come to a mutual understanding on how to blend privacy controls with transparent transactions. This may be possible following the principles set out in the regulation, notably data protection by design and data protection by default. Pursuant to article 25 GDPR, data controllers shall implement technical and organizational measures to comply with EU data protection principles. These obligations are closely related to the data-controller accountability clause (articles 5(2) and 24 GDPR).

However, it is necessary to note that neither the text nor context of privacy-by-design provision offer any clarity about requirements, scope, or limitations.[95] Hence, only a teleological reasoning can offer a way forward in the following directions: on the one hand, regulators must incentivise developers to safeguard established fundamental rights and provide guidance on how to build GDPR compliant systems. Blockchain innovators, on the other hand, must be given freedom to develop their products while respecting regulatory principles.

The author ultimately affirms that, when it comes to identification of data-protection implications of blockchain technology, it is essential to consider two aspects before drawing any conclusion. First, the technology is still under development, meaning that nothing is definitive. Second, there is a lack of standards and consistent interpretation on both the main aspects of the technology and some data protection requirements (i.e., what they actually entail, to what extent they can be interpreted). Thus, the intersection of blockchain technology and the GDPR remains ambiguous. Consequently, as some claim ‘the legal framework set up by the GDPR is still in its infancy’,[96] this article suggests that the debate has merely begun.

[95] Ezra Waldman, *Data Protection by Design? A Critique of Article 25 of the GDPR* (2018) Cornell Int. Law J 147, 148.
[96] Opinion of Advocate General Bobek, C-645/19, *Facebook V. Belgium DPA* (2021) ECLI:EU:C:2021:5, para. 12.