GDPR and Ethereum blockchain: a Compatibility Assessment

Claudia Martorelli*

Abstract: Blockchain technology could bring many advantages to our society, in many different areas. In particular, it could improve individuals' control over their data. Through blockchain, data could be shared easily and in a secure way among different actors, thus preventing its accumulation in single points of failure. As the use of blockchain technology becomes widespread, its compatibility with Regulation (EU) 2016/679 (the General Data Protection Regulation, 'GDPR' or 'Regulation' hereafter) has emerged as a point of tension. Some have argued that blockchain pursues the same objectives as the GDPR, but it does so in ways which are different from those established by the Regulation. This is mainly due to the fact that the Regulation implies a centralized data collection system, where it is possible to single out an accountable central entity, against which users' rights have to be safeguarded. Whereas, in public permissionless blockchain projects, the network is decentralized, no single entity is responsible for it, and the decision-making power is shared among different stakeholders. It has been argued that this incompatibility, and the resulting regulatory uncertainty, will asphyxiate the development of this technology. Being the Ethereum blockchain the one which, at the time of writing, promises to be the most suitable to be adopted in a variety of use cases, this paper assesses whether, having regard to the allocation of GDPR responsibility roles, to the legal bases and principles of data processing, and to the data subject's rights, it is possible to consider the Ethereum blockchain GDPR-compatible.

Keywords: GDPR; blockchain; ethereum; data protection law.

Table of contents: 1. Introduction. – 2. General Data Protection Regulation. – 3. Blockchain Technology. – 4. Territorial Scope of Application of the GDPR. – 5. Material Scope of Application of the GDPR. – 5.1. Personal Data on the Blockchain. – 6. Controllers, Joint controllers and Processors. – 7. Ethereum Governance and Stakeholders. – 8. Controllers and Processors in Ethereum. – 9. Lawfulness of Processing. – 9.1. Performance of a Contract. – 9.2. Legitimate Interest. – 9.3. Special Categories of Data Manifestly Made Public by the Data Subject. – 10. Transparency. – 11. Data Minimization and Storage Limitation. – 12. Accountability. – 13. Right of Access. – 14. Right to Rectification. – 15. Right to Erasure. – 16. Conclusion.

1. *Introduction*

The main focus of this article, rather than a compliance assessment of the Ethereum blockchain, is to be a resource to provide an assessment of its potential to become GDPR compliant.

The issues related to the power that big tech companies gain from the large amount of data they collect have been deeply discussed in the past few years. This continuous harvesting of data has led to the age of "surveillance capitalism, a form of tyranny that feeds on people but is not of the people"[1]. This surveillance is characterized by a strong asymmetry of power between centralized online operators and end-users, who "are generally left in the dark with regard to the data collected, processed or inferred about them"[2]. Not only individuals'

*Claudia Martorelli is a law graduate who attended specialization courses in Privacy and Data Protection from the LUISS Guido Carli University of Rome, Italy; she also boasts a Foreign Languages and Literature degree from the Sapienza University of Rome. After a Master of Laws in Technology in Europe obtained at Universiteit Utrecht in Netherlands, she is currently doing a legal internship at Portolano Cavallo legal firm, which provides legal advice to companies in the Digital, Media and Technology.

[1] See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 513, Profile Books, 2019.

[2] See Primavera De Filippi, *The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies*, Journal of Peer Production, 2016.

privacy, but also competition[3] and democracy[4] have been negatively affected by this concentration of power. The freedom of the individual – conceived as freedom from manipulation – and right to privacy, are increasingly felt to be in danger.

In the last few years another related debate has flourished: blockchain technology as a solution to the drawbacks of the Web 2.0. It expected to take place as a consequence of the spreading of this technology, the new surge of decentralization is supposed to bring many opportunities, such as the empowerment of individuals on their own data,[5] the reduction in hacks and data breaches[6], and the elimination of central points of control acting as intermediaries, thus possibly increasing competition in digital markets[7].

The most relevant project aiming at this new stage of decentralization is the Ethereum blockchain, which, unlike Bitcoin which only allows cryptocurrency transactions, is designed to allow users to carry out operations of varying complexity[8]. In fact, Ethereum blockchain has a far-reaching disruptive potential, that goes far beyond financial applications, and can impact 'asset-registries, voting, governance, and the internet of things'[9], only to name a few.

[3] See Javier Espinoza, *EU vs Big Tech: Brussels' Bid to Weaken the Digital Gatekeepers* (2020), available at https://www.ft.com/content/4e08efbb-dd96-4bea-8260-01502aaf1bd7 (last visited April 8, 2022).

[4] See Eliza Mackintosh, *No Matter Who Wins the US Election, the World's "fake News" Problem Is Here to Stay* (2020), available at https://edition.cnn.com/2020/10/25/world/trump-fake-news-legacy-intl/index.html (last visited April 8, 2022).

[5] See Nguyen Binh Truong and others, *GDPR-Compliant Personal Data Management: A Blockchain-Based Solution*, IEEE Transactions on Information Forensics and Security (2019); Guy Zyskind, Oz Nathan and Alex Sandy Pentland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data, 180, IEEE Security and Privacy Workshops,* 2015.

[6] See Michèle Finck, *Blockchains: Regulating the Unknown* at 670, 19, German Law Journal, 665, 2018.

[7] See Essentia 1, *Why the Web 3.0 Matters and You Should Know about It* (January 30, 2018) available at https://medium.com/@essential/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949 (last visited April 8, 2022).

[8] See Ethereum Foundation, *What is Ethereum?*, available at https://ethdocs.org/en/latest/introduction/what-is-ethereum.html (last visited April 8, 2022).

[9] See *Id.*

However, it has been pointed out that public and unauthorized blockchains, like Ethereum, and the GDPR are incompatible at a conceptual level[10], even if they share the same objectives: empowering individuals[11]. This is due to the GDPR being drafted taking into account a centralized method for data collection and storage that cannot be reconciled with the decentralization typical of this type of blockchain[12]. Some authors even argued that blockchains and the GDPR cannot coexist[13]. This alleged incompatibility is going to be a problem also for those projects that, at present, do not deal with personal data. In fact, the European data protection law runs the risk of becoming "the law of everything": as our daily life is increasingly mediated by information technology, any data could be plausibly argued to be personal[14].

It is argued that the incompatibility issue is more problematic for public and permissionless blockchains than for permissioned ones[15]. This is mainly because, in permissioned blockchains, it is still possible to have a clear definition of roles among the subjects involved, thus facilitating the application of the GDPR. However, also public and unofficial blockchains can be characterized by power concentration, typically with regard to the software development process[16]. Furthermore,

[10] See Michèle Finck, *Blockchains and Data Protection in the European Union at 2*, 1, Max Planck Institute for Innovation and Competition Research Paper Series, 2018.

[11] See *Id*, see also Lokke Moerel, *Blockchain and Data Protection* in The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms at 217, 231 (Larry A DiMatteo, Michel Cannarsa and Cristina Poncibò eds., 2019); Nguyen Binh Truong and others, *GDPR-Compliant Personal Data Management: A Blockchain-Based Solution*, IEEE Transactions of Information Forensics and Security, 2019.

[12] See Finck, *Blockchains and Data Protection in the European Union* (cited in note 10).

[13] See The European Union Blockchain Observatory and Forum, *'Blockchain and the GDPR'* (2018), available at https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (last visited April 8, 2022).

[14] See Nadezhda Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, 10, Law, Innovation and Technology 40, 41, 2018.

[15] See *The European Union Blockchain Observatory and Forum, Blockchain and the GDPR*, 16 (2018); Anisha Mirchandani, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, 29, Fordham Intellectual Property, Media and Entertainment Law Journal, 2019.

[16] See Michele Finck, *Blockchain Regulation and Governance in Europe*, 19, Cambridge University Press, 2018.

the concrete governance of a specific project can be analyzed in order to identify responsibility roles[17]. Nevertheless, the identification of responsibility roles is only one of the tensions pointed out in the literature, which also include the difficulty of ensuring compliance with data processing principles and the possibility of guaranteeing data subjects an effective exercise of their rights.

This article analyses the Ethereum blockchain because it is the public blockchain with the greatest number of application and users[18], although the conclusions that will be drawn for features generally shared among this type of blockchains can be applied in different projects as well.

After providing an introductory definition of the GDPR and the blockchain technology, the conditions that have to be met for the GDPR to be applicable to the Ethereum blockchain will be assessed From Section 6 to 15, there will be an Ethereum-focused analysis of the major issues highlighted by the literature in the application of the GDPR to public permissionless blockchains.

2. *General Data Protection Regulation*

From 1995 to May 2018, Directive 95/46/EC was the main EU legal data protection instrument[19]. Even if it provided a high level of harmonization, Member States still had discretion in their national implementation and application. These differences could undermine the functioning of the single market and "distort competition"[20]. The adoption of a more coherent legal framework for the protection of personal data was also needed due to the new challenges brought by

[17] See Valeria Ferrari and Alexandra Giannopoulou, *Distributed Data Protection and Liability on Blockchains*, Internet Science (Svetlana S Bodrunova eds. 2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3316954 (last visited April 8, 2022).

[18] See The European Union Blockchain Observatory & Forum, March 2021 Trends Report (2021).

[19] See European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, 29, (2018).

[20] Recital 9 GDPR.

the rapid technological developments and by globalization, which increased the scale of the collection and sharing of personal data[21].

The GDPR was adopted in 2016 and became applicable from the 25th of May 2018[22], repealing Directive 95/46/EC. Under EU law, regulations are directly applicable and there is no need for national implementation, therefore the GDPR provides a single set of data protection rules across the EU. However, there still exist differences on its interpretation among national Data Protection Authorities (DPAs)[23].

In the regulatory text of the GDPR is stated that it has been made "technologically neutral"[24], meaning that it can be applied regardless of the characteristics of a given technology. an attempt has been made to structure it in such a way that it can be observed in a set of general overarching principles that have to be applied to the specific data processing operation[25].

The main objectives pursued by the Regulation are "the protection of natural persons with regard to the processing of personal data" and the "free movement of personal data"[26]. To fulfill the first objective, it establishes the role of the "controller" – the main responsibility role in the Regulation – a natural or legal person determining the purposes and means of the processing[27]; and the overarching principle of the controller's accountability. In this way, it ensures that the processing of personal data is carried out in a responsible way through the introduction of a number of obligations that vary in accordance with the types of personal data being processed and with the level of risk entailed by the processing. The 'data subject' is the natural living person whose personal data are being processed.

[21] See Recitals 6 and 7 GDPR.

[22] See GDPR Article 99.

[23] For an assessment of how the different approaches adopted by national DPAs is impairing competition in digital markets, *see* Damien Geradin, Theano Karanikioti, Dimitrios Katsifis, *GDPR Myopia: How a Well-Intended Regulation ended up Favoring Google in Ad Tech*, TILEC Discussion Paper, 2020.

[24] GDPR Recital 15.

[25] See Michele Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?*, 98, 2019.

[26] GDPR Article 1.

[27] GDPR Article 4 (7).

3. *Blockchain Technology*

Blockchain technology first appeared in 2008 in the Bitcoin White Paper by Satoshi Nakamoto, where he announced the creation of a peer-to-peer system that would allow individuals to securely transact with each other without the need of a trusted middleman[28]. On January the 3rd 2009, Nakamoto mined the genesis block of the Bitcoin blockchain, where he also included an encrypted message – "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks": the headline of The London Times issued that same day[29]. Among the Bitcoin community, this message is considered a further indication of the will of Nakamoto to create a completely new financial system, in which central institutions, like banks, would not be needed anymore[30]. Generally speaking, through blockchain, individuals are able to lower the uncertainties that arise when transacting with each other, not through trusted third parties, but through code[31].

As suggested by Primavera De Filippi[32], Nakamoto's creation seems to be the fulfillment of Timothy C. May's prophetic words describing "tamper-proof boxes" allowing people to interact with each other in a totally anonymous manner, escaping government control and all it entails[33]. Even if the original idea behind blockchain technology can thus be linked to the Crypto-anarchist movement[34], and

[28] See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 1 (2008), available at https://bitcoin.org/bitcoin.pdf (last visited April 8, 2022).

[29] See Jamie Redman, *A Deep Dive Into Satoshi's 11-Year Old Bitcoin Genesis Block* (January 3, 2020) available at https://news.bitcoin.com/a-deep-dive-into-satoshis-11-year-old-bitcoin-genesis-block/ (last visited April 8, 2022).

[30] See Giannopoulou and Ferrari, *Distributed Data Protection and Liability on Blockchains* (cited in note 17).

[31] See Michèle Finck, *Blockchains: Regulating the Unknown*, 19 German Law Journal 665, 669 (2018).

[32] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code, 2,* , Harvard Univ Pr, (2018).

[33] See Timothy C. May, *The Crypto Anarchist Manifesto* (1988).

[34] As stated by May in the Crypto Anarchist Manifesto "The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations

was mainly intended to empower individuals and to escape the law, today blockchain is widely used by those traditional intermediaries that it was meant to rule out – banks[35], financial intermediaries, companies[36], even governments[37]– and has increasingly been addressed by regulators.

The value of blockchain technology has been recognized by the European Commission as well[38], thus giving the European Union the possibility of adopting a pan-European regulatory sandbox to better understand how to regulate the use cases of this technology without hampering its development[39]. In fact, blockchain technology is seen as an opportunity for Europe to lead technological development in a way that is finally respectful of European values.

In simple terms, blockchain can be defined as a decentralized distributed database that allows a large number of actors to store synchronized copies of the same data[40]. Data are grouped in blocks, which are linked to one another through the hashing process[41].

This process consists in the creation of an alphanumeric code (so-called hash) that represents the data contained in each block, so that if these data are manipulated, the resulting hash will be different.

and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy".

[35] See Ryan Browne, *Big Banks Take Baby Steps Toward Commercializing Blockchain*, (November 20, 2020), available at https://www.cnbc.com/2020/11/20/big-banks-take-baby-steps-toward-commercializing-blockchain.html (last visited April 9, 2022).

[36] See Michael del Castillo, Blockchain 50 2021, (February 2, 2021) available at https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/?sh=4043e2fc231c (last visited April 8, 2022).

[37] See Kaspar Kojus, *Welcome to the Blockchain Nation*, (July 7, 2017), avalaible at https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b-46c06fd4 (last visited April 9, 2022).

[38] See European Commission, *Blockchain Technologies*, (2021) , avalaible at https://ec.europa.eu/digital-single-market/en/blockchain-technologies (last visited April 8, 2022).

[39] See European Commission, *Legal and Regulatory Framework for Blockchain*, (2021) https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain (last visited April 8, 2022).

[40] See *The European Union Blockchain Observatory and Forum, 'Blockchain and the GDPR'* (2018), 14.

[41] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 3 (cited in note 25).

Given that each block also contains the hash of the previous block, if the previous block is manipulated, then the resulting hash of all the following blocks will change as well, originating a new version of the chain that will not correspond to the version shared by all the other nodes in the network. Therefore, hash-chaining makes the blockchain temper-evident[42].

The mechanism through which the network agrees on which new block to add to the chain is called the consensus protocol. In reference to the Ethereum and the Bitcoin blockchains, it is used the "proof of work" protocol[43]: validating nodes compete to solve a mathematical problem; the first node to solve it, broadcasts the block to the rest of the nodes, which accept the block – only if all transactions in it are valid – by working on creating the next block in the chain, using the hash of the accepted block as the previous hash[44].

As illustrated in the table below, blockchains can be distinguished in public/private, permissionless/permissioned, according to their characteristics in terms of usage and validation. The distinction between public and private depends on whether some kind of authorization is needed in order to become a participating node[45], for instance when the administrator of the system has to grant access to the user. If no authorization is needed, and therefore anyone could access the information stored on a blockchain, the blockchain is said to be public[46]. The distinction between permissionless and permissioned refers to whether any authorization is needed in order to become a

[42] For more information on how it works, in-depth information is available at https://blockchain.regulatingbig.tech/#!/blockchain (last visited April 8, 2022).

[43] Ethereum will move to a Proof of Stake consensus in the future, meaning that users will need to stake a certain amount of ETH to become validators. Validators are randomly chosen to create blocks and are responsible for checking and confirming blocks created by others. A user stake can be lost if the user certifies malicious blocks. For more information on Proof of Stake, see *Proof-of-stake (PoS)* (April 16, 2021) available at https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (last visited April 8, 2022).

[44] See Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* at 3 (cited in note 29).

[45] A node is a computer that stores a local copy of the blockchain.

[46] See Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* at 14-15 (cited in note 29).

validating node, meaning, to be able to add data to the blockchain. If no authorization is needed, a blockchain is said to be permissionless[47].

In public permissionless blockchains, anyone can install the software and download a copy of the blockchain and become a full node that can participate in the storing and adding of data. No registration procedure is needed, no one owns the network[48]. The software is created and maintained by volunteers who, normally, change over time[49].

	Private	Public
Permissioned	Authorization is needed in order to access and add data to the blockchain	Authorization is needed only to add data to the blockchain, while data are publicly available
Permissionless	N/A	Anyone can access and add data to the blockchain

Table 1. Types of blockchain

The blockchain environment is multi-layered. Blockchains function on the Internet and TCP/IP protocol; blockchains provide an infrastructure for data management (layer 1), but also an infrastructure for the decentralized execution of software (layer 2)[50]. An example of this can be the Ethereum blockchain (layer 1) upon which smart contracts can be executed, as well as Ether transactions (layer 2).

[47] See *Id.*

[48] See *Id.*

[49] See *Id.*

[50] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 4 (cited in note 25).

4. *Territorial Scope of Application of the GDPR*

For the GDPR to be applicable, the Ethereum Blockchain has to fall within its territorial and material scope of application, therefore the single processing operation must be examined to understand if this is the case. As a matter of fact, not all processing activities, carried out by the same controller or processor, may fall within the scope of application of the GDPR[51].

Article 3 GDPR establishes two main criteria to be considered: the "establishment" criterion under Article 3(1) and the "targeting" criterion under Article 3(2)[52].

Firstly, it is important to consider any real and effective activity exercised through stable arrangements[53] to determine if there is an establishment in the EU, by departing from a formalistic approach whereby undertakings are established solely in the place where they are registered[54]. When it comes to the assessment of the 'stable arrangement' for the provision of services online, the threshold is quite low, as the presence of even only one representative could be deemed to be enough[55]. However, such an establishment cannot exist merely because the undertaking's website is accessible in the Union[56].

To assess if the establishment criterion can be used to apply the GDPR to the Ethereum blockchain, one should be able to single out who the controller is. In Section 6 and following, the controllership issue will be analyzed deeper. For now, it is enough to argue that it is impossible to identify a proper establishment in the European Union or a stable arrangement for the provision of the service, because there is no such thing as official Ethereum headquarters anywhere in the world[57], and, as we will see in Section 8, in most cases, natural persons

[51] See *European Data Protection Board, Guidelines 3/2018 on the Territorial Scope of the GDPR* (Article 3), 4, (2019).

[52] See *Id.*

[53] GDPR Recital 22.

[54] Case C-230/14 Weltimmo v NAIH, 2015 para 29.

[55] See *Id*, at 30.

[56] Case C-191/15 Verein für Konsumenteninformation v. Amazon EU Sarl, 2016 para 76.

[57] The Ethereum Foundation cannot be considered as an overarching responsible entity, since '*its role is not to control or lead Ethereum, nor are they the only organization that founds critical development of Ethereum-related technologies*', in About the Ethereum

will be identified as controllers, and relying on this criterion would make the application of the GDPR dependent on where these persons decide to reside. The absence of a central point of power in the Ethereum ecosystem is highlighted several times even in the home page of the website. Ethereum is regarded as a "community-run technology", and it is said that 'No government or company has control over Ethereum'[58]. Furthermore, it is rather difficult to know exactly where the individuals who can be appointed as controllers are effectively located.

Turning now to the targeting criterion, its applicability mainly depends on the presence of the data subject in the territory of the Union (I) at the moment of the offering of services or goods, or (ii) when the monitoring of the data subject's behavior takes place. In addition, it is necessary that the activity is intentionally offered to individuals in the Union[59] (services offered to individuals outside the Union, which are not withdrawn when such individuals enter the EU, will not be subject to the Regulation)[60].

The offering of services also includes the offering of information society services[61], regardless of whether a payment by the data subject is required in exchange[62]. The Ethereum blockchain can be considered an information society service as described by point (b) of Article 1(1) of Directive (EU) 2015/1535[63], which is referred to by Article 4 (25) GDPR. In fact, it is a service normally provided for remuneration,

Foundation (March 30, 2021) available at https://ethereum.org/en/foundation/ (last visited April 8, 2022).

[58] See https://ethereum.org/en/ (last visited April 8, 2022).

[59] See GDPR Recital 23.

[60] See European Data Protection Board, *Guidelines 3/2017 on the territorial scope of the GDPR (Article 3)* 15 (2019).

[61] Article 1(1) point (b) Directive (EU) 2015/1535: "any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

[62] See Case C-352/85 *Bond van Adverteerders and Others vs. The Netherlands State*, 1988 para 16; Case C-109/92 Wirth, 1993 para 15.

[63] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241.

without the parties being simultaneously present, through electronic means, and through the transmission of data on individual request[64].

The Ethereum service is intentionally offered to individuals in the European Union, since, as claimed in the Ethereum website, "it's open to everyone, wherever you are in the world – all you need is the internet"[65].

In conclusion, it is likely that the GDPR will apply to every public permissionless project under Article 3(2), since their aim is usually to offer a service accessible from all over the world.

5. *Material Scope of Application of the GDPR*

Article 2 GDPR defines the material scope of application of the Regulation, and it also provides a number of exemptions, such as the household exemption which will be examined later on[66].

The Ethereum blockchain falls within the material scope of the GDPR because it implies the processing of personal data by automated means. 'Processing' encompasses practically any activity involving personal data[67]. Automated data processing concerns any personal data processing carried out using a device (e.g., a computer)[68]. This broad interpretation of processing implies that the addition of personal data, its continued storage and any further operation on the blockchain constitute personal data processing[69]. Ethereum can be

[64] This reconstruction considers the user perspective who is using blockchain to broadcast a transaction to the network. The perspective of nodes and miners should not be considered because their activity on the blockchain constitutes part of the service itself.

[65] See *What is Ethereum?* available at https://ethereum.org/en/ (last visited April 9, 2022).

[66] GDPR Article 2(1) provides that "this Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".

[67] GDPR Article 4(2).

[68] See *European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law*, law, 99 (2018).

[69] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 10 (cited in note 25).

defined as an append-only ledger as it is almost impossible to delete data once they are stored on it. As a consequence, data is continuously stored on the blockchain for as long as it functions. Secondly, to validate transactions it is necessary to verify all the previous transactions and for this reason past data have to be continuously processed.

As for the household exemption, Article 2 (2) (c) provides that the GDPR does not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity, which is thus non-commercial/non-professional[70]. Accordingly, the Commission Nationale de l'Informatique et des Libertés (CNIL) stated that natural persons who use a blockchain for reasons unrelated to their profession or commercial activity do not assume the role of controllers, therefore "a natural person who buys or sells Bitcoin, on his or her own behalf, is not a data controller"[71]. However, the CJEU case law[72], as well as the Guidelines of Article 29 Working Party[73], require a further condition for the exemption to be applicable: the diffusion of personal data being restricted to a limited number of persons.

As for Ethereum blockchain, even individuals who use the blockchain for personal purposes are qualifiable as data controllers because data is accessible to an indefinite number of people. In fact, anyone can access the information stored in the blockchain, even without the need of downloading the software[74]. This is generally true for all public and permissionless blockchains[75]. Nonetheless, to support the CNIL point of view, it has been pointed out that making information publicly available in the blockchain is not like doing the same on a social

[70] GDPR Recital 18.

[71] See Commission Nationale de l'Informatique et des Libertés*, Solutions for a Responsible use of Blockchain in the context of Personal data*, 2 (2018).

[72] Case C-101/01 Lindqvist, 2003 para 47; Case C-73/07 Satakunnan Markkinapörssi and Satamedia, 2008 para 44; Case C-212/13 Ryne , 2014 para 31 and 33; Case C-345/17 Buivids*,* 2019 para 43; Case C-25/17 Jehovan todistajat, 2018 para 42.

[73] Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, 6 (12 June 2009).

[74] See https://etherscan.io/ (last visited April 9, 2022).

[75] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 12 (cited in note 25).

network. In fact, it would be much harder to single out a person only through on-chain data[76].

5.1. *Personal Data on the Blockchain*

The GDPR applies only to the processing of personal data: any activity involving data that does not fall within this category, such as anonymous data[77] , will not be regulated by the GDPR.

The concept of personal data[78] has to be interpreted broadly[79], in order to include any kind of statement about a living person, both objective and subjective, regardless of its correctness[80], and of the format or the medium on which it is contained[81].

Within this broad category, there are special categories of personal data which reveal sensitive information about an individual, such as political opinions or sexual orientation[82], to which the GDPR provides greater protection.

Even information that has undergone pseudonymization is still personal data[83]: pseudonymization is only a security measure that prevents the attribution of the personal data being processed to the data subject in the absence of additional information. For instance, in databases storing personal details of data subjects, names are replaced with numbers and the document containing the associations between names and numbers is stored elsewhere.

On the Ethereum blockchain there are two main types of data: accounts and transaction data, while there are two types of accounts:

[76] See Jörn Erbguth, *Five Ways to GDPR-Compliant Use of Blockchain*, 5 European Data Protection Law Review 427, 431(2019).

[77] Anonymous data refer to information relating to a person whose identification is irreversibly prevented.

[78] Article 4 (1) GDPR defines personal data as 'any information relating to an identified or identifiable natural person ('data subject')'

[79] Case C-434/16 Peter Nowak v Data Protection Commissioner, 2017 para 34.

[80] Article 29 Working Party, Opinio 4/2007 on the concept of personal data, 6 (June 20, 2017).

[81] See *Id*, at 7.

[82] GDPR Article 9 (1).

[83] GDPR Recital 26.

externally owned ones, and contract accounts, hereafter "contract"[84]. Externally owned accounts represent identities of external agents (such as human personas, mining nodes or automated agents), and use public-key cryptography to sign transactions[85]. Contracts have an associated code, whose execution is triggered by transactions launched from other externally owned accounts or contracts[86]. Contracts can serve different purposes, such as archiving data to the benefit of both other contracts or actors outside the blockchain for example, a contract can record membership in a particular organization. Moreover, they can serve as externally-owned account with a more complicated access policy that can manage "manage an ongoing contract or relationship between multiple users" or "provide functions to other contracts, essentially serving as a software library"[87].

Considering that transaction data consists in the data contained in a transaction, a transaction takes place between externally owned accounts and other accounts and consists of the transmission of a signed package of data[88]. There are three main categories of functions that transactions can complete: money transfer, contract creation and contract invocation[89]. Each transaction contains the recipient of the message, a signature identifying the sender, the amount of Wei[90] to transfer, an optional data field that can contain the message sent to a contract[91], the maximum number of computational steps the transaction execution is allowed to take, the fee the sender is willing to pay to have the transaction verified[92].

[84] See Ethereum Community, *Account Management*, available at https://ethdocs.org/en/latest/account-management.html?highlight=address#keyfiles (last visited April 9, 2022).

[85] See *Id.*

[86] See Ethereum Community, *Contracts and Transactions*, available at https://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#eoa-vs-contract-accounts (last visited April 9, 2022).

[87] See *Id.*

[88] See *Id.*

[89] See Jiajing Wu and others, *Analysis of Cryptocurrency Transactions from a Network Perspective: An Overview*, 3 (2020).

[90] The base unit of Ether, the currency used on Ethereum.

[91] The message is like a transaction, but it is produced by a contract and not by an account. Contracts can have relationships with other contracts through messages. MA message leads to the recipient account running its code.

[92] See Ethereum Community (cited in note 87).

Each block in the Ethereum blockchain collects several pieces of information, among which there is the address of the miner[93] who validates the transactions, to which the fees of each transaction are sent; as well as the list of validated transactions[94].

Clearly, when accounts are used by natural persons, the address and the public key can be qualified as personal data[95] because they are "online identifies"[96].

As for contracts, the only use cases in which they do not qualify as personal data are the ones in which they are used as software libraries or when they are used by non-natural persons.

Regarding transactional data, this type of data can certainly be considered personal data when concerning transactions between accounts belonging to natural persons, and when personal data are stored in the message added in the optional data field[97].

Furthermore, it has been proved that, in the Ethereum blockchain, the identification of natural persons is reasonably likely to be possible, not only through the linking of on-chain data to other pieces of information collected by other means[98], but also through analytic on-chain data examination alone. For instance, it has been argued that the "linkability" of the identity of a user to a cluster of addresses is

[93] Miners are validating nodes, meaning, nodes in the network that group the transactions into "blocks".

[94] See Gabin Wood, Ethereum: A secure Decentralised Generalised Transaction Ledger, 5, Petersburg Version 41c1837 (February 14, 2021).

[95] See Giannopoulou and Ferrari (cited in note 17). For the opposite conclusion, See Luis-Daniel Ibanez, Kieron O'Hara, Elena Simperl*, On Blockchains and the General Data Protection Regulation,* 6.

[96] GDPR Recital 30 provides that "*natural persons may be associated with online identifiers [...] which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*" Examples of online identifiers are cookies and IP addresses.

[97] For an example of message, see https://etherscan.io/tx/0xcdcc5e38b063bb-5b2007ec5106495cca1468ef2475d5adb2a680ba210e72a363, scroll the page and click on 'click to see more', under the invoice 'input data' click on the button 'view inputs as' and select 'UTF-8' (last visited April 9, 2022).

[98] See Matthias Berberich, Malgorzata Steiner, *Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers*, 2, European Data Protection Law Review, 2 422, 424 (2016); Also see Wu and others, *Account Management* at 10 (cited in note 84).

increased through the deployment of a smart contract's source code[99]. Moreover, since Ethereum is an account-based model[100], its users tend to use only a handful of addresses for their activities[101]. Address reuse has allowed the identification of a number of 'quasi-identifiers', such as time-of-day activity, transaction fee, transaction graph, leading to the profiling and deanonymization of Ethereum users[102]. In addition, law enforcement agencies have developed forensic chain analysis techniques to identify suspected criminals[103].

Finally, as the technological development that may take place during the processing must be considered to assess which means are reasonably likely to be used to identify a person, there is a general consensus on the qualification of public keys as personal data in public permissionless blockchains[104]. In fact, with regard to blockchain use cases built on the assumption that the infrastructure will serve as a perpetual record of transactions, as is the case for Ethereum, any data

[99] See Shlomi Linoy, Natalia Stakhanova, Alina Matyukhina, *Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution*, 15TH International Conference on Network and Service Management, (2019).

[100] "*In an account-based cryptocurrency, native transactions can only move funds between a single sender and a single receiver, hence in a payment transaction, the change remains at the sender account. Thus, a subsequent transaction necessarily uses the same address again to spend the remaining change amount. Therefore, the account-based model essentially relies on address-reuse on the protocol level*", in Ferenc Béres, Istvan A. Seres, Andras A. Benczur, Mikeah Quintyne-Collins, *Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users*, 1 (2020).

[101] See *Id.*

[102] See Béres, Seres, Benczur, Quintyne-Collins, *The European union Blockchain Observatory and Forum, Blockchain and the GDPR*, 20 (2018)); Béres, Seres, Benczùr, Quintyne-Collins, (cited in note 101); Wu and others, (cited in note 90, at 10).

[103] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 27 (cited in note 25).

[104] See Commision nationale de l'Informatique et des Libertés*, Solutions for a Responsible use of Blockchain in the context of Personal Data* (2018), The European Union Blockchain Observatory and Forum, Blockchain and the GDPR (2018; Jean Bacon and Others, *Blockchain Demystified*, Queen Mary School of Law Studies Research Paper No. 268/2017, 40 (2018) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218 (last visited April 9, 2022) also see Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?*, (cited in note 25).

has to be considered personal data since it cannot be reasonably assumed that identification will remain unlikely in the future[105].

6. *Controllers, Joint controllers and Processors*

One of the most controversial issues in the application of the GDPR to public permissionless blockchains is the attribution of controller and processor responsibility roles to the actors involved. As already explained, this is mainly due to the fact that, in these environments, no central authority exists, and the power is split among different categories of actors, who have different roles in the functioning of a blockchain. In order to understand to what extent, they can be identified as controllers or processors, we need to understand how these roles are regulated first.

The controller is the figure who is practically entrusted with ensuring that the system complies with data protection law[106] and for this reason it has been argued that the broader the controllership concept is interpreted the more data subjects will be safeguarded[107]. A controller autonomously determines the purposes and means of the processing, regardless of whether it has access to the data being processed[108].

A processor is a distinct entity from the controller and is set to process personal data on behalf of and under the directions of the

[105] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 24 (cited in note 25). For a quick overview of the potential of quantum computing, see MacKenzie Sigalos, Hacking bitcoin wallets with quantum computers could happen – but cryptographers are racing to build a workaround, (June 10, 2021) available at https://www.cnbc.com/2021/06/10/long-term-crypto-threat-quantum-computers-hacking-bitcoin-wallets.html (last visited April 9, 2022).

[106] See Finck, *Blockchain and the General Data Protection Regulatio*n at 37 (cited in note 25).

[107] EUCJ Google *Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12 (2014) at para 32; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16 (2018) at para 28; *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, C-40/17 (2019) at para 66.

[108] *Wirtschaftsakademie Schleswig-Holstein* at para 38 (cited in note 108).

controller[109]. Therefore, the processor cannot carry out the processing for its own purposes, thus going beyond the controller instructions, but it can determine the non-essential means for processing.

The notions of controller and processor are functional concepts: their objective is to allocate responsibilities according to the actual roles of the parties and not according to formal designations. This implies that the legal status of an actor, independently from the fact that it has been appointed as a "controller" or a "processor", must be determined on the basis of its actual activities in a specific situation[110].

It is important to establish which level of influence on the purposes and the means of processing should entail the qualification of the controller. Decisions on the purposes of the processing have to be always made by the controller[111]. Then, regarding the determination of the means, a distinction can be made between essential and non-essential means[112]. Essential means are reserved for the controller. Examples are decisions taken about "the type of personal data which are processed, the duration of the processing, the categories of data subjects"[113]. On the contrary, non-essential means can be left to the processor. They concern the practical aspect of processing, like the decision to use given hardware or software, or the adoption of detailed security measures[114].

When the decision-making power on the purposes and essential means of the same processing activities is exercised by several different entities at the same time, those entities qualify as joint controllers[115]. In this case, the processing would not be possible without the participation of all parties, since their processing activities are "inextricably linked"[116]. Even when they do not share the same purposes, joint controllership can be established if they pursue complementary

[109] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (September 2, 2020) at 24, available at https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controller-processor_en.pdf (last visited April 6, 2022).

[110] See *Id* at 7.

[111] See *Id* at 13.

[112] See *Id* at 14.

[113] See *Ibid.*

[114] See *Ibid.*

[115] See *Id* at 18.

[116] See *Ibid.*

or linked purposes. Such is the case when there is a mutual benefit arising from the same processing operation[117].

There is joint controllership also when one of the involved actors provides the means of the processing, such as a tool or other system, making them available to other entities. By deciding to use those means of processing for its own purposes, an entity will participate in the determination of the means of the processing[118]. However, the use of a common infrastructure will not always imply joint controllership. This would be the case when the processing 'could be performed by one party without the intervention from the other'; when the provider can be qualified as a processor because of the absence of any purpose of his own[119]; when each actor determines its own purposes[120].

Article 26 (1) GDPR requires joint controllers to determine, following a factual-based approach[121] and by means of an arrangement between them, the respective responsibilities for compliance with the obligations under the GDPR. However, Article 26 (3) establishes that data subjects may exercise their rights in respect of, and against each of the controllers, irrespective of any such arrangement. The fact that one party does not have access to the data processed would not be enough to exclude joint controllership[122].

7. *Ethereum Governance and Stakeholders*

In order to identify controllers and processors in the Ethereum blockchain, it is important to understand how stakeholders exercise

[117] See *Id* at 19; *Fashion ID at* para 80 (cited in note 108).

[118] In case C-210/16 the Court of Justice held that the administrator of a Facebook fan page takes part in the definition of the means of the processing of personal data related to the visitors of its fan page, by defining parameters based on its target audience.

[119] See European Data Protection Board, *Guidelines 07/2020* at 20 (cited in note 110).

[120] See *Id* at 23.

[121] See *Wirtschaftsakademie Schleswig-Holstein at* para 43 (cited in note 108).

[122] See *Id* at 38; *Jehovan todistajat* at para 69 (cited in note 73).

their decision-making power[123], as each group has different roles, incentives, interests and means of participation[124].

In general, there are two types of governance in the blockchain environment: on-chain or off-chain. In the Ethereum blockchain, governance relies on off-chain mechanisms. On-chain governance refers to rules and decision-making processes that have been encoded into the infrastructure of a blockchain[125], defining the interactions between participants within the infrastructure, through the infrastructure itself[126]. Off-chain governance means that 'the rules of governance are not written into the core blockchain protocol itself and must instead be dealt with at the social layer, i.e., humans talking to other humans'[127]. Off-chain governance allows for interventions into the blockchain protocol that are not prescribed by the protocol itself[128].

As for the governance in Ethereum, miners, developers and users signal their approval or disapproval of a protocol improvement proposal through private and community discourse[129]. Stakeholders' consensus cannot be obtained through on-chain voting[130]. This is to avoid favoring those with more Ethereum tokens[131], whom could be given more vote power. In this case, there are two scenarios that can occur: (i) if all stakeholders agree, the code changes are made smoothly; (ii) if they disagree, stakeholders can either try and convince other stakeholders to act in favor of their side, or, if consensus cannot be reached,

[123] See *Giannopoulou and Ferrari* (cited in note 17).

[124] See Finck, *Blockchain Regulation and Governance in Europe* at 198 (cited in note 16).

[125] See Wessel Reijers et al, *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*, 37 TOPOI: International Review of Philosophy 17, 2 (2018).

[126] See *Ibid.*

[127] See *Ethereumbook* (May 9, 2018), available at https://github.com/lrettig/ethereumbook/blob/governance/contrib/governance.asciidoc (last visited April 8, 2022).

[128] See Reijers et al, *Now the Code Runs Itself* at 3 (cited in note 125).

[129] See EhtHub, *Ethereum Basics*, available at https://docs.ethhub.io/ethereum-basics/governance/ (last visited April 6, 2022).

[130] See Bogdan Rancea, *What is Ethereum Governance? Complete Beginner's Guide* (Unblock, 7 January 2019) https://unblock.net/what-is-ethereum-governance/ (last visited April 6, 2022); also see The European Union Blockchain Observatory and Forum, Governance of and with Blockchains13 (2020).

[131] See Rancea, *What is Ethereum Governance?* (cited in note 131).

they have the ability to hard fork the protocol and keep or change features they think are necessary[132]. In the latter case, there will be two blockchains that will have to "compete for brand, users, developer mindshare, and hash power"[133].

With regard to the various actors involved in the functioning and use of the Ethereum blockchain, first of all, there are core developers who work on the software that implements the protocol[134]. They are responsible for "fixing bugs, responding to technical issues, and coordination ongoing protocol updates"[135]. They can suggest software changes (as anyone with a Github account can do)[136], but they cannot impose such changes unilaterally.

Node operators, who are "the owners and managers of nodes that run the protocol"[137], participate in the network by storing a full or light copy of the ledger, decide whether to update protocol changes, and can send transactions to the network.

Miners are validating nodes, meaning, nodes in the network that group the transactions into "blocks and compete with one another for their block to be the next one to be added to the blockchain"[138]. They can determine the success of a protocol update by installing the software modifications[139].

Application developers build applications of arbitrary complexity that run on the blockchain[140].

[132] See EthHub, *Ethereum Basics* (cited in note 130).

[133] See *Ibid.*

[134] See *Ibid.*

[135] See Retting, *Ethereumbook* (cited in note 128).

[136] See *Ibid.*

[137] See EthHub, *Ethereum Basics* (cited in note 130).

[138] See Ethereum Community, W*hat is Ethereum?*, available at https://ethdocs.org/en/latest/introduction/what-is-ethereum.html#how-does-ethereum-work (last visited April 6, 2022). As said before, this is likely to change in the future, since a Proof of Stake consensus is going to be adopted, in which validating nodes will be chosen randomly.

[139] See Finck, *Blockchain Regulation and Governance in Europe* (cited in note 16).

[140] See Retting, *Ethereumbook* (cited in note 128).

8. *Controllers and Processors in Ethereum*

Given that responsibility roles have to be identified with respect to the single processing operation, it is important to understand which processing operations take place on Ethereum. The participation of a variety of actors in the functioning of this blockchain means that an actor, or a group of actors, can qualify as data controller for a specific operation, and as processor for others. Furthermore, the multi-layered infrastructure of blockchain-based systems implies the presence of different controllers for different layers[141].

It has been argued that trying to find a controller at the infrastructure layer[142] is like assessing 'who the controller is with respect to the entirety of data processing via the Internet or via email functionality' since blockchain, like the Internet, is a general-purpose technology[143]. However, even if it is true that the Ethereum blockchain is a general-purpose technology, because anyone can send transactions for their own purposes and build applications on top of it, there is still an underlying interest that is relevant at the infrastructure layer – ensure the reliability and the functioning of the blockchain – which is realized through the processing of personal data, and which is not comparable to the way the Internet functions.

The processing operations carried out to achieve this interest consist of the fact that each node, in order to participate in the network, has to download the (full or partial) history of transactions, and in the fact that transactions can be added only through the creation of new blocks. The means through which this processing is carried out consist of the core software of Ethereum and the hardware provided by nodes and miners. This interest, and the means to achieve it, were established by the founders of Ethereum when they developed the infrastructure itself. Nowadays, core developers take care of the core software of Ethereum but, even if their opinions may be highly

[141] See Finck, *Blockchain and the General Data Protection Regulation* at 4 (cited in note 25).

[142] As a recall, the infrastructure layer in this work is considered to encompass the 'consensus layer', the 'network layer' and the 'data layer', as illustrated in Figure 1 at page 8. Practically speaking, it is where data are stored, where transactions are implemented and the security of the network ensured.

[143] See Moerel, *Blockchain and Data Protection* at 217 (cited in note 11).

influential on the community[144], the actual implementation of the changes is left to nodes and miners[145]. With regard to nodes and miners, by downloading the software and participating in the functioning of the network, they share the interest in keeping the blockchain functioning, and in ensuring its reliability. They continue to exercise such decision-making power by choosing which version of the software to implement. Therefore, at the infrastructural level, nodes and miners can be qualified as joint controllers[146] with respect to the processing operations needed to keep the network functioning and reliable[147].

As regards the allocation of responsibility concerning the single transaction, some authors argued that nodes can be qualified as controllers[148], because they are not "subject to external instructions, autonomously decide whether to join the chain and pursue their own objectives"[149], and they can order, store and freely use data[150]. However, this interpretation cannot be considered accurate because it does not take into account the hypothesis in which nodes chose to passively run the software to facilitate the processing of transactions on behalf of users – a hypothesis in which they would qualify as processors,

[144] See Michele Benedetto Neitz, *Ethical Considerations of Blockchain: Do We Need a Blockchain Code of Conduct?* (The FinReg Blog, January 21, 2020), available at https://sites.law.duke.edu/thefinregblog/2020/01/21/ethical-considerations-of-blockchain-do-we-need-a-blockchain-code-of-conduct/ (last visited April 6, 2022).

[145] See Giannopoulou and Ferrari, *Distributed Data Protection and Liability on Blockchains* (cited in note 17).

[146] The opposite conclusion is reached in The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR* at 18 (cited in note 15), in which it is argued that "*nodes do not determine the purpose and means of processing. They are running the protocol in the hope of winning a reward, or in order to contribute to the stability of the network, and/or as a way to access the data that is relevant to them without relying on third-party intermediaries*".

[147] For an analogous line of reasoning with respect to Bitcoin, see Bacon et al *Blockchain Demystified* (cited in note 104).

[148] See Berberich and Steiner, *Blockchain Technology and the GDPR* at 424 (cited in note 98).

[149] See Finck, *Blockchain Regulation and Governance in Europe* at 100 (cited in note 16).

[150] See Finck, *Blockchain and the General Data Protection Regulation* at 47 (cited in note 25); under reference to Mario Martini, Quirin Weinzierl, *Die Blockchain-Technologie und das Recht auf Vergessenwerden*, 36 NVWz 1251 (2017).

rather than controllers[151]. Miners are generally qualified as processors, due to the fact that , even if they have influence over the means of the processing, they have no decision-making power over the purposes underlying the single transaction[152]. Finally, users are generally identified as data controllers with respect to the transaction they sign and broadcast to the network[153]. This is because they pursue their own purposes and decide the means by choosing to rely on the blockchain. This conclusion is also in line with the opinion on the Article 29 Working Party, which allows the user of a social media to be a controller[154]. However, it may be criticized that this allocation of accountability has the result of shifting the responsibility for the technology design from the actual designers to users[155], who are generally not aware of such legal implications. It is also difficult to determine how fines will be calculated in case a controller, in the Ethereum blockchain, failed to comply with the GDPR – given that Article 83 GDPR refers to the "annual worldwide turnover" – or even how an ordinary person could ever be able to pay the heavy fines the GDPR allows to impose[156].

For what concerns smart contracts, the developer could be qualified as controller or as processor according to his/her role in determining

[151] See Bacon et al , *Blockchain Demystified* at 45 (cited in note 104); The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR* at 18 (cited in note 15).

[152] See Commission National de l'Informatique et des Libertés, *Solutions for a responsible use of Blockchain in the context of personal data* at 2 (cited in note 72); The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR* at 18 (cited in note 15).

[153] See Finck, *Blockchain and the General Data Protection Regulation* at 47 (cited in note 25); Commission National de l'Informatique et des Libertés, *Solutions for a responsible use of Blockchain in the context of personal data* at 2 (cited in note 72); The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR* at 18 (cited in note 15); Finck, *Blockchain Regulation and Governance in Europe* at 101 (cited in note 16); Bacon et al, *Blockchain Demystified* at 44 (cited in note 104); Erbguth, *Five Ways to GDPR-Compliant Use of Blockchain* at 433 (cited in note 77); Giannopoulou and Ferrari, *Distributed Data Protection and Liability on Blockchains* (cited in note 17).

[154] Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking* (2009) at 6.

[155] See Finck *Blockchain and the General Data Protection Regulation* at 48 (cited in note 25).

[156] See Finck, *Blockchains and Data Protection in the European Union* at 17-18 (cited in note 10).

the purpose of the processing[157]. For instance, if the software is developed by one of the parties deploying the smart contract, then the developer, as well as the other party, will qualify as controllers due to the influence on the determination of the purposes of processing. Whereas, if the software is developed by a third party and deployed by different actors for their own purposes, then the developer will rather qualify as processor and the parties as controllers.

As for blockchain-based applications (i.e. cases in which users will not interact with the infrastructure layer of the blockchain, but with a user-friendly interface)[158], the entity which developed, or is responsible for the application will act as an intermediary – meaning that it will add data to the blockchain on behalf of their users[159] – and will qualify as data controller, since it determines the means and the purposes of the processing[160].

From the analysis above, it is clear that there could be situations in which data controllers may be unable to comply with the GDPR requirements due to their insufficient control over data[161] (the implications deriving from such allocation of responsibilities will be analyzed deeper in Section 12). Taken alone, nodes, miners and users have very limited influence over the respective means of the processing: a single node would not be able to change the protocol or the history of transactions stored on the blockchain on its own; nodes or users could not bind miners, in quality of their relationship controllers-processors, through a contract ensuring compliance with GDPR requirements; single users would not be able to erase data to comply with an erasure request forwarded by the other party in the transaction, in quality of their relationship controller-data subject.

[157] See Commission National de l'Informatique et des Libertés, *Solutions for a responsible use of Blockchain in the context of personal data* at 2 (cited in note 72).

[158] Also tokens and smart contracts fall under the definition of application. However, in this paper an 'application' is considered to be something which closely resembles a 'regular' application, to which users generally think about when talking about applications.

[159] See The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR* at 17 (cited in note 15).

[160] See Erbguth, *Five Ways to GDPR-Compliant Use of Blockchain* at 433 (cited in note 77).

[161] See Finck, *Blockchain and the General Data Protection Regulation* at 52 (cited in note 25).

As Advocate General highlighted in his Opinion in *FashionID* case, law, and its interpretation, should never reach the result of imposing an obligation on addressees who cannot actually comply with them[162]. There should always be "a reasonable correlation between power, control, and responsibility"[163].

9. *Lawfulness of Processing*

The processing of personal data must be carried out in a lawful way, according to Article 5(1)(a) GDPR, meaning that the processing has to be justified by one of the legal grounds provided by Article 6(1) GDPR[164].

Consent[165] can be an appropriate basis for processing only when the data subject has control and can deny consent without detriment[166]. This will never be the case with respect to data processing on blockchain: first, by declining the storing of data on the blockchain, the processing operation could not take place at all; second, the data subject cannot be granted an effective choice and control over data once it is inserted in the system. Furthermore, the data subject could withdraw consent at any time[167], and in the case it does, data has to be erased, if there is no other purpose justifying the continued processing[168]. As it will be explained further on, deletion of data is not possible on Ethereum blockchain and the interest in keeping the

[162] See Opinion of AG Bobek, *Fashion ID & Co. KG v Verbraucherzentrale NRW e.V*, C-40/17, December 19, 2018 at para 93.

[163] See *Id.* at 91.

[164] Which are: a) consent of the data subject; b) performance of a contract; c) compliance with a legal obligation to which the controller is subject; d) protection of the vital interests of the data subject or of another natural person; e) carrying out a task in the public interest; f) legitimate interest of the controller.

[165] GDPR Article 4(11) defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

[166] See European Data Protection Board, *Guidelines 05/2020 on Consent Under Regulation 2016/679*, para 3 (2020).

[167] GDPR Article 7(3).

[168] GDPR Article 17(1)(b).

network working and reliable might justify the further processing of data under the legal basis of the legitimate interest – thus "avoiding" the issue of erasing data – consent should never be used as a legal ground for the processing.

The same applies to the "explicit consent" required by Article 9 (2) (a) for the processing of special categories of personal data, with the difference that in this case, the legitimate interest in preserving the network will not be a legal ground justifying the further processing of data in the case consent has been withdrawn.

The legal grounds listed in Article 6 (1) letters (c) compliance with a legal obligation to which the controller is subject, (d) protecting the vital interests of the data subject or of another natural person, (e) carrying out a task in the public interest, could be relied upon in very specific cases in which the Ethereum blockchain would be used, for example, as a means for voting in elections, or for the storage of healthcare data, or for banks to comply with AML obligations. However, at the moment these uses are taking place at a rather negligible level and, consequently, are of no relevance in this work. Therefore, my analysis will focus on the legal grounds provided in Article 6 (1) letter (b) performance of a contract, and (f) legitimate interest, which are the ones on which most of Ethereum blockchain processing operations could be relied on.

The same goes for the processing of special categories of data, for which the only legal ground that is worth discussing is provided in Article 9 (2) (e), which refers to processing of personal data which are manifestly made public by the data subject.

9.1. *Performance of a Contract*

For Article 6 (1) (b)[169] to be applicable, the controller should be capable of demonstrating (i) the existence of a contract, (ii) its validity

[169] GDPR Article 6 (1) (b) provides that "*Processing shall be lawful only if and to the extent that at least one of the following applies: b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*".

under the applicable contract law and that (iii) the processing is objectively needed to perform it[170].

To assess if the processing is necessary to perform the contract, one has to identify the specific purpose that is going to be achieved through the processing itself, so that if less intrusive alternatives are available, the processing cannot be considered as "necessary"[171]. The 'necessity' has to be assessed also from the perspective of 'an average data subject', therefore the data controller has to ensure that the processing constitute a reasonable expectation of the data subject when entering into the contract[172]. For instance, when ordering a product online, it is reasonable to ask for the customer's address only if home delivery has been required.

When users transact on Ethereum, it is reasonable to assume that in most cases the transaction is linked to a previous agreement between the parties. However, whether the transaction is qualifiable as a contract is something that depends on the circumstances of the specific transaction and on the (local) applicable contract law[173]. Whereas the "necessity" requirement is satisfied that, currently, knowledge of the recipient's address is the minimum condition for the transaction to take place.

At the application level, this legal basis may be invoked to the extent that the registration of data on the blockchain is necessary to perform the service requested by the user. However, the 'average data subject' may not be aware of the fact that data is going to be permanently stored on the blockchain.

When relying on this legal basis, processing should terminate when the contract is entirely performed[174], unless it is carried out for other purposes, authorised under other legal grounds and clearly

[170] See European Data Protection Board, *Guidelines 2/2019 on the processing of Personal Data Under Article 6 (1)(B) GDPR in the context of the provision of Online Services to Data Subjects*, para 27 (2019).

[171] See *Id*, at 24-25.

[172] See *Id*, at 32.

[173] For an overview of the legal status of smart contracts, *See* Nataliia Filatova, *Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies*, 28, International Journal of Law and Information Technology 217, 242, 2020.

[174] GDPR Article 17 (1) (a).

communicated at the beginning of processing[175]. In this case, as explained in the following section, the legitimate interest in preserving the network could be a viable legal ground to justify the further processing of data once the contract is terminated.

The necessity to perform a contract is not among the exceptions listed in Article 9 (2) for the processing of special categories of personal data for which the explicit consent of the data subject would be required. As a result, services demanding the processing of such data on Ethereum will not be compliant with the GDPR, mainly because the conditions for valid consent, and the erasure of data after the withdrawal of it, cannot be

To conclude, the possible application of Article 6 (1) (b) will depend on the context of the specific transaction and application, but there are some reasons to argue that processing could rely upon this legal ground.

9.2. *Legitimate Interest*

For Article 6 (1) (f)[176] to be applicable, the following three cumulative conditions must be met: (i) the interest pursued must be legitimate, (ii) the processing must be necessary for the purpose, (iii) the fundamental rights and freedoms of the data subject do not override the legitimate interest pursued.[177] Furthermore, this legal basis can be relied upon only after an assessment of the interest of the data controller and the rights and interests of the data subject has been carried out[178], so to avoid a disproportionate impact on the latter[179].

[175] See European Data Protection Board, *Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(B) GDPR in the context of the provision of Online Services to Data Subjects*, para 44 (2019).

[176] GDPR Article 6 (1) (f) provides that "*Processing shall be lawful only if and to the extent that at least one of the following applies: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*".

[177] Case C-13/16 R gas satiksme, 2017 para 28.

[178] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, 9 (9 April 2014).

[179] See *Id*, at 41.

In order to be considered as 'legitimate', the interest of the controller has to be sufficiently specific, related to concrete and actual circumstances[180], and in accordance with the law[181].

Concerning the assessment of the impact of the processing on the data subject, consideration should be given to, *inter alia*, on one hand, whether the legitimate interest can be linked to the exercise of the controller's fundamental rights[182], or if it represents a public interest or an interest shared by the wider community[183], or if it is legally or culturally recognized[184], and on the other hand, the positive and negative consequences of the operation on the data subject, the nature of the data processed and whether it is publicly available, the reasonable expectation of the data subject regarding the use and disclosure of data, the status of the data subject and of the data controller[185].

According to Recital 49, the processing of personal data to the extent that is strictly necessary and proportionate to ensure the security of the network is a legitimate interest of the data controller. In this case, ensuring the reliability of the network has to be equated to ensuring its security, given that by storing a copy of the transactions history, each node prevents the unilateral modification of it by other malicious actors, and guarantees that only one version of the ledger exists, without the need of relying on a single central authority. Otherwise, nodes will not have any means to ensure that a sole version of the ledger exists.

This processing operation is proportional, given that nodes can decide whether to store a full, a light or an archive node, where only the

[180] See *Id*, at 24; Case C-708/18 Asocia ia de Proprietari bloc M5A-ScaraA, 2019 para 44.

[181] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, 25 (9 April 2014).

[182] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, 34 (9 April 2014).

[183] See *Id*, at 35.

[184] See *Id*, at 36.

[185] See *Id*, at 37-39.

latter stores a complete archive of historical states, while the others will result in pruned blockchain data[186].

The interest in ensuring the reliability and functioning of the network is specific enough to allow the balancing test to be carried out, and represent a concrete and actual interest, given that, at the moment of writing, Ethereum has around 2 million active nodes[187], and one Ether is worth 2.700 €[188].

Not only is the interest at stake shared by those who have invested in Ether, but it is also shared by a community of users and developers, and, finally, by society given that Ethereum has a high potential to render blockchain more user friendly for a variety of use cases.

Regarding the nature of the data being processed, in simple terms, data on Ethereum consists of public keys and transactions which will hardly be recognized as personal data by users themselves. As previously explained, messages added in transactions could store personal data, and the combination of on-chain data with off-chain data, or a deep and careful analysis of the blockchain itself, could increase the possibility of users' identification and, consequently, of their surveillance. However, in most cases, carrying out such a study will require a deep knowledge of the network, as well as a high level of IT skills. Furthermore, users may not be aware that transactions will be stored forever, or that there is the possibility that their identity could be discovered. In particular, the inability to delete data from the ledger constitutes a rather heavy impact on the data subject's rights and interests.

In conclusion, storing transaction history to ensure the reliability and the functioning of the network is a processing operation that should be justified under Article 6 (1) (f) because the interests and rights of data subjects are not likely to override the legitimate interest of the controllers. However, this could change depending on a data subject's specific situation.

[186] See *Nodes and Clients* (April 2, 2021), available at https://ethereum.org/en/developers/docs/nodes-and-clients/ (last visited April 9, 2022).

[187] See https://etherscan.io/nodetracker/nodes (last visited April 10, 2022).

[188] See https://www.tradingview.com/symbols/ETHEUR/ (last visited April 10, 2022).

9.3. *Special Categories of Data Manifestly Made Public by the Data Subject*

Article 9 (2) (e) provides that the processing of special categories of data shall be permitted if data is made manifestly public by the data subject. Being it an exception to the general prohibition to process special categories of data, it has to be interpreted strictly and 'as requiring the data subject to deliberately make his or her personal data public'[189]. Furthermore, it would be incorrect to assume that in these cases the public availability of data is a sufficient condition to allow any type of data processing[190]. Rather, Article 6 has to be applied cumulatively with Article 9 to ensure that all relevant safeguards are satisfied, and that the processing of special categories of data is not granted a lower protection than personal data in general[191].

As far as Ethereum blockchain is concerned, it is unlikely that sensitive data can be considered as deliberately made public by the data subject. In fact, the user is likely to believe that their identity will remain unknown. Therefore, if an address were linked to a person's identity, and the transactions made were sufficient to reveal, for instance, their political opinions, further processing of data would be unlawful.

10. *Transparency*

In the following sections, the extent to which Ethereum's blockchain uses can ensure compliance with those data processing principles listed in Article 5 of the GDPR that are claimed to be 'incompatible' with public permissionless blockchains, such as transparency, data minimization and accountability will be discussed. A regulatory overview will be provided for each section, which will then be applied to Ethereum. According to Recital 39 GDPR, the transparency

[189] See European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, 162 (2018).

[190] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, 15 (9 April 2014).

[191] See *Id.*

principle requires that any information related to the processing of personal data must be easily accessible and easy to understand for the data subject. In particular, information should be given about the identity of the controller, the purposes of processing, the risks, rules, safeguards and rights linked to the processing and how to exercise them. This requirement is established also by Articles 13 and 14 of the GDPR.

The transparency principle is more easily complied with at the application layer, where is easier to single out an intermediary[192], rather than at the infrastructure or transaction layer, where it raises again the question of the connection between accountability and control[193]. Indeed, the information that the controller is required to make available to data subjects, according to Articles 13 – 14 GDPR, could be unreasonably burdensome to be provided in some cases. For instance, at the infrastructure level, as each node qualifies as a data controller, the identity and contact details of all of them should be made available to all users. At the transaction level, the parties involved often do not know each other, and since both parties qualify as controllers, requiring them to disclose their identities would imply a higher risk for the privacy of users, rather than a privacy improvement.

The GDPR lays down some exceptions to the obligation to provide information to the data subject, which differs according to whether the data have been collected directly from the data subject or not. In the former case, the only exception applies when the data subject already has the information[194]. In the latter case, the data controller is exempted from the obligation to give information when it is impossible, or it 'would involve a disproportionate effort', or when it is likely to 'seriously impair the achievement of that processing'[195]. In such cases, the controller shall take appropriate measures to protect the data subject's rights and interests, including making the information publicly available.

[192] See Ibáñez, O'Hara, Simperl, *On Blockchains and the General Data Protection Regulation* at 10 (cited in note 95).

[193] See Finck, *Blockchain and the General Data Protection Regulation* at 64 (cited in note 25).

[194] GDPR Article 13 (4).

[195] GDPR Article 14 (5) (b).

The 'impossibility' or the 'disproportionate effort' must be connected to the fact that personal data were not obtained directly from data subjects[196]. In addition, the 'disproportionate effort' exception cannot be routinely relied upon if controllers do not process data for archiving or statistical purposes[197].

The exception of the "serious impairment of objectives" can be if controllers are able to demonstrate that the provision of information alone would nullify the purpose of the processing[198].

While at the transaction level, the parties involved should disclose their identity to each other as personal data are collected directly from the data subject, at the infrastructure level, it could be argued that by downloading the history of transactions, nodes do not enter in direct contact with each user and that data are not collected directly from them. However, none of the exceptions provided by Article 14 (5) (b) apply. Requiring nodes to disclose their identity is not impossible, even if burdensome. Given that the processing is not taking place for archiving or statistical purposes, it would be irrelevant whether the provision of the information would imply a disproportionate effort. Finally, the disclosure of identities will not (directly) impair the objective of ensuring the reliability and the functioning of the network. However, it is questionable whether the network will have the same rate of active nodes in case they were required to disclose their identities.

In conclusion, in theory, it is possible to achieve compliance with the transparency principle in the Ethereum blockchain. In practice, this is unlikely to happen and, in any case, a reasonable interpretation of this principle should be adopted, so that individuals are not required to disclose more personal data than necessary.

[196] Article 29 Data Protection Working Party, Guidelines on Transparency Under Regulation 2016/679, para 62 (11 April 2018).

[197] See *Id,* at 61.

[198] See *Id,* at 65.

11. *Data Minimization and Storage Limitation*

The principle of data minimization requires that the controller processes only the data which are necessary and adequate for the purpose of the processing. Given that the data minimization principle requires the controller to process personal data only if they are sufficient to fulfilll the specified purpose, even the processing carried out on insufficient data will be in violation of the GDPR[199]. Also, from the case-law of the CJEU it is possible to conclude that the assessment of compliance with the data minimization principle has to be carried out considering whether all possible reasons that could justify the processing of fewer data were taken into account when delimiting the scope of a processing operation[200].

As to the principle of storage limitation, Article 5 (1) (e) requires that personal data must be deleted or anonymized when they are no longer necessary[201]. This principle is important to ensure that personal data are erased or anonymized when the controller does not need it anymore[202]. Data controllers should always take a proportionate approach, balancing their needs with the impact of retention on individuals' privacy[203].

[199] See Information Commissioner's Office, *Principle (c): Data minimisation*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ (last visited April 10, 2022).

[200] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd and Kärntner Landesregierung, 2014 paras 57-58, 69. The CJEU found that the generalised way in which the Data Retention Directive (Directive 2006/24/EC) covered "*all individuals and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*", was in breach of the proportionality principle.

[201] See European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, 129, (2018).

[202] See Information Commissioner's Office, Principle (e): Storage limitation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (last visited April 10, 2022).

[203] See *Id.*

Data minimization and storage limitation are said to be at odds with the 'perpetual distributed storage'[204] of data, being blockchains append-only, ever-growing databases[205]. However, a deeper analysis reveals that, contrary to what is generally assumed, this is not the case: compliance with these principles has to be assessed in consideration of the purposes of the processing. As a matter of fact, the perpetual storage of data and the distributed nature of the ledger are necessary for ensuring the reliance and the functioning of the network. Therefore, data stored on blockchain will always remain necessary because they ensure that the state of the system is reliable and verifiable. The processing of users' public addresses is necessary for the proper functioning of the blockchain and is not possible to further minimise them[206]. However, there is room to argue that at the transaction level, as well as at the application layer, unnecessary data could be inserted in the transaction, but this will only render the transaction GDPR-incompliant, whereas it would not render the transaction or the blockchain GDPR-incompatible.

12. *Accountability*

Article 5 (2) introduces the principle of accountability, which requires controllers to safeguard data protection in their processing activities, and establishes their responsibility for ensuring and demonstrating that the processing operations they carried out are in compliance with the law[207].

The principle of accountability is clearly linked to the controller responsibility role. As highlighted in Section 8, the allocation of responsibilities deriving from the application of the GDPR to Ethereum blockchain leads to situations in which data controllers may be

[204] See Berberich and Steiner, *Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers* at 425, (cited in note 98).

[205] See Lokke Moerel, *Blockchain & Data Protection... and Why They Are Not on a Collision Course*, 6, European Review of Private Law 825, 847-848 (2019).

[206] See Commission Nationale de l'Informatique et des Libertes, *Solutions for a Responsible Use of Blockchain in the Context of Personal Data*, 7 (2018).

[207] See European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law 134, (2018).

unable to comply with the GDPR requirements due to their insufficient control over the data. The major obstacle is that single nodes, or users, would not be able to delete, modify or access data. Because of the structure of the network, they would not be able to choose processors and to bind them to the adoption of proper safeguards in the processing of data.

The resulting dissociation between control and responsibility clashes with the main objective pursued by both the accountability principle and the controller as a responsibility role, namely, to improve the effective application of data protection law[208], and to "ensure that responsibility is allocated in such a way that compliance with data protection rules will be sufficiently ensured in practice"[209].

The ever-growing complexity of data processing, which is ever more likely to comprise several different processes and to involve numerous parties holding differing degrees of control, increases the risk of accountability gaps. However, these gaps should not be filled by assigning responsibility to those who do not exercise any factual power[210].

In *Google Spain*, the CJEU held that the data controller has to ensure compliance with data protection law "within the framework of its responsibilities, powers and capabilities"[211]. Therefore, even if, at first glance, Ethereum blockchain may seem incompatible with the accountability principle, there is room to argue that, it will be reasonable to adopt a more flexible and realistic interpretation of the requirements leading to the qualification of controller, in cases where the actors qualifiable as controllers cannot comply with GDPR obligations. It has not the effect of allocating responsibility to subjects who are materially incapable of doing anything to avoid it, and it actually mirrors the extent of control held by actors involved in the processing operation.

[208] Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability (July 13, 2010).

[209] Article 29 Working Party, Opinion 1/2010 on the Concepts of "controller" and "processor", 1, (2010).

[210] Case C-40/17 Fashion ID, Opinion of AG Bobek, 2019 para 71.

[211] Case C 131/12 Google Spain, 2014 para 38.

13. *Right of Access*

Chapter III of GDPR is dedicated to the rights of the data subject. In the following sections, I will analyze only the most problematic ones to exercise in public permissionless blockchains, namely, the right of access, right to rectification, right to erasure.

Article 15 GDPR grants data subjects the right to obtain confirmation from the controller as to whether their personal data are being processed, and, consequently, access to personal data and to information, such as, *inter alia*, the purposes of processing, the categories of data processed, the recipients to whom data have been or will be disclosed. The boundaries defining the scope of application of the right of access have to be determined considering its objective[212], meaning, to allow the data subject to become aware of which data are being processed, and to check that they are accurate and processed in compliance with the law[213].

It is not possible for data subjects to be entitled to the right to obtain a copy of the original file in which their personal data appear as a consequence of their right of access. Data can be communicated through means other than the original file, for instance in order to safeguard the rights of other individuals if the original document also contains personal data related to them[214]. Indeed, the right of access cannot be exercised in a way which it adversely affects the rights and freedoms of others[215].

For the same reason, a controller can legitimately refuse access to data if it can be demonstrated that the data subject is not identifiable.[216]. In particular, granting access to information that is only linked to a non-obvious identifier, rather than against other information more clearly related to a person, represents a 'major privacy risk' due to the controller not being able to determine whether the information

[212] Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v M and S.*, 2014 para 46.

[213] See *Id,* at 59.

[214] See *Id.*

[215] GDPR Article 15 (4); GDPR Recital 63.

[216] GDPR Article 11 (2).

requested is exclusively about the person making the request[217]. For example, a data controller may reject access requests based only on IP addresses, as this online identifier is linked to the device, which could be used by more than one individual.

The fulfillment of the data subject request in the Ethereum blockchain environment becomes problematic at the infrastructure level, where all nodes, including miners, can be qualified as joint data controllers. Consequently, a data subject could address any of them in order to request access to his/her personal data. However, nodes would not be able to satisfy the request because they only see encrypted and hashed data[218]. At the same time, it has to be pointed out that none of them could reasonably be able to ascertain whether information, to which access is requested, can be linked back to the individual making the request. Being data encrypted and not having the key to decrypt it, granting access would mean cracking the encryption used by others to protect their data. This could be a reason for data controllers to lawfully refuse access.

14. *Right to Rectification*

Article 16 GDPR states that the data subject has the right to obtain from the data controller the rectification of inaccurate personal data concerning him or her, in the light of the purpose for which data was collected[219]. Therefore, the data subject can obtain the rectification including by means of providing a supplementary statement, where appropriate.

[217] See Information Commissioner's Office, *Personal Information Online Code of Practise*, 32, (2010).

[218] See Finck, *Blockchain and the General Data Protection Regulation* at 10 (cited in note 25). Also see The European Union Blockchain Observatory and Forum, Blockchain and the GDP, 25 (2018). It has to be kept in mind that if a data subject wanted to know the transactions linked to his/her account, or to read data added in plain text, he/she would be able to check that information on his/her own, without the need to file an access request.

[219] Case C-434/16 Peter Nowak v Data Protection Commissioner, 2017 para 53.

Article 29 Working party considers that only factual information can be inaccurate, not opinions[220]. Concerning the latter, opinions diverged as to whether the principle of accuracy applies: according to some, non-factual data *per se* cannot be accurate, while others argue that accuracy applies as they fall within the scope of application of data protection legislation[221].

It has been highlighted that, even when data is factually correct, there are other aspects that could offer a misleading impression of an individual, for instance when data are presented in a way that can lead to misinterpretation[222].

Given the immutability of transactions on Ethereum[223], it would be practically impossible to comply with data subjects' requests by substituting erroneous data with correct data. Single nodes could modify their version of the ledger; however, this would only mean that *their* version would be different from the *actual* version of the blockchain, which would be the version shared by, at least, 51% of nodes in the network. Furthermore, a hard fork[224] would be necessary in order to change data stored in past blocks, and to make the change effective for the majority of nodes,. However, a 'old' version of the chain, which contains the erroneous data, will continue to exist and, potentially,

[220] Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, 15 (November 26, 2014).

[221] See Diana Dimitrova, *The Rise of the Personal Data Quality Principle. Is it Legal and Does it Have an Impact on the Right to Rectification?*, 4 (2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790602 (last visited April 10, 2022).

[222] See *Id*, at 11. This conclusion can be inferred from the CJEU preliminary ruling in the case U v Stadt Karlsruhe (Case C-101/13 U. v Stadt Karlsruhe, 2014) in which, although the personal data of the applicant were factually correct, they were presented in a misleading format which led to their misinterpretation.

[223] See *Is Ethereum Immutable?* https://docs.ethhub.io/questions-about-ethereum/is-ethereum-immutable/#immutability-and-the-dao-hard-fork (last visited April 10, 2022); Also see Ibáñez, O'Hara, Simperl, *On Blockchains and the General Data Protection Regulation* at 7 (cited in note 95).

[224] 'A hard fork refers to a radical change to the protocol of a blockchain network that effectively results in two branches, one that follows the previous protocol and one that follows the new version' from Jake Frankenfield, Hard Fork (Blockchain) (4 March, 2021), available at https://www.investopedia.com/terms/h/hard-fork.asp (last visited April 10, 2022).

other miners and users who disagree with the hard fork, could continue using it[225], as shown in the figure below. Therefore, it is incorrect to assume that compliance with these requests could potentially be achieved by a periodical fork of the blockchain, as suggested by some scholars[226], because erroneous data could still continue to be processed in the old version of the blockchain.

Blocks from non-upgraded nodes	Follows old rules	↦	Follows old rules	↦	Follows old rules	↦	Follows old rules	↦	Follows old rules
Blocks from upgraded nodes	Follows old rules	↦	Follows old rules	↦	Follows new rules	↦	Follows new rules	↦	Follows new rules

Table 2. Representation of a hard fork

It is worth pointing out that requests of rectification, where the addition of supplementary information would be sufficient to rectify the data, could be complied with by any node, or even by the data subject on its own, through the broadcasting of new transactions to the network. However, rectification through the substitution of erroneous data will remain problematic due to the difficulties in changing the blockchain history.

15. *Right to Erasure*

Article 17 GDPR confers to data subjects the right to obtain from the controller the erasure of personal data concerning them if at least one of the conditions required is met[227].

[225] See *Is Ethereum Immutable?*, available at https://docs.ethhub.io/questions-about-ethereum/is-ethereum-immutable/#immutability-and-the-dao-hard-fork (last visited April 10, 2022).

[226] See Bacon and Others, *Blockchain Demystified* at 48 (cited in note 104); Also see Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 73 (cited in note 25).

[227] These are: the personal data are no longer necessary in relation to the purposes for which they were collected or processed; the data subject withdraws consent on which the processing was based; the personal data have been unlawfully processed; the erasure is needed to comply with a legal obligation; personal data have been

The right to erasure is not absolute[228]. As a matter of fact Article 17 (3) provides a number of cases where the erasure can be lawfully denied. The CJEU stressed the need to adopt a case-by-case approach when balancing clashing interests, taking into account the nature and the sensitivity of the information in question, and the interest of the public in accessing it[229].

As pointed out by Finck, the exact meaning of the term 'erasure'[230] has not been clarified yet. In *Google Spain*, the delisting from search results was considered to equal erasure, while in *Nowak*, the CJEU considered 'erasure' to mean 'destruction' of data[231]. However, the latter case was not about the right to erasure and the 'destruction' of data was the most straightforward means to achieve erasure[232]. The case-by-case approach, and the uncertainty about the real implication of the expression 'erasure' may be taken as indications that controllers should do all they can to obtain a result as close as possible to the destruction of data, within the limits of their own possibilities[233].

In the case of Ethereum blockchain, the major problem will derive from the immutability of the blockchain.

Therefore, alternative means for the destruction of data have been considered. In particular, the CNIL deemed the inaccessibility of data to be close enough to erasure[234]. However, inaccessibility could be achieved only through encryption and deletion of the private key, while if data were stored in plain text, the request of erasure would never be complied with. Furthermore, it was suggested, by analogy

collected in relation to the offer of information society services to a minor of 16 (or 13) years old, in the absence of consent given by the holder of parental responsibility.

[228] In Case C 398/15 Manni, 2017, the CJEU found the interference with the right to privacy of the plaintiff was not disproportionate and did not grant the exercise of the right to erasure.

[229] Case C 131/12 Google Spain, 2014 para 81.

[230] See The European Union Blockchain Observatory and Forum, *Blockchain and the GDPR*, 25 (2018); Also see Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 75 (cited in note 25).

[231] Case C-434/16 Peter Nowak v Data Protection Commissioner, 2017 para 55.

[232] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 76 (cited in note 25).

[233] See *Id.*

[234] See Commission Nationale de l'Informatique et des Libertés, *Solutions for a Responsible Use of Blockchain in the Context of Personal Data*, 8 (2018).

with *Google Spain*, that it would be likely for users to address their requests to intermediaries like block explorers to obtain the removal of data from their indexes[235].

When no alternative means are available to comply with an erasure request, the only solution would be taking down the entire blockchain, at least in Europe, and implementing measures to prevent people residing in the EU from downloading the ledger again. However, the adoption of this measure would be rather drastic. It should follow from the balancing of a number of different interests. As a matter of fact, being Ethereum a general-purpose technology, it can be also used for many laudable scopes, such as the escaping of censorship by people living in authoritarian countries[236].

In conclusion, at the application layer, intermediaries could store encrypted data on the blockchain, so that the deletion of the private key could be enough to comply with an erasure request. Nevertheless, when data are stored in plain text or are publicly accessible, there would be no way to comply with an erasure request without taking down the entire blockchain, or without turning it into a permissioned one. However, data stored on a blockchain are not as easy to find as it would be in regular databases, since one should already have a hint of what to search for, or where to search it, and no "general" search can be carried out, for example through keywords[237]. In *Google* Spain, the CJEU considered the harm to an individual's right to privacy to be particularly serious "when the search by means of that engine is carried out on the basis of an individual's name. In fact, that processing enables any internet user to obtain through the list of results a

[235] See Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European Data Protection Law?* at 76 (cited in note 25).

[236] See Nir Kshetri, *Chinese Internet Users Turn to the Blockchain to Fight Against government Censorship* (February 25, 2019), available at https://theconversation.com/chinese-internet-users-turn-to-the-blockchain-to-fight-against-government-censorship-111795 (last visited April 10, 2022). Also see Roger Huang, *Chinese Netizens Use Ethereum To Avoid China's COVID-19 Censorship* (March 31, 2020), available at https://www.forbes.com/sites/rogerhuang/2020/03/31/chinese-netizens-use-ethereum-to-avoid-chinas-covid-19-censorship/ (last visited April 10, 2022).

[237] For instance, to carry out a research using https://www.blockchain.com/explorer/?utm_campaign=dcomnav_explorer, the research can only be based on 'transaction', 'address' or 'block'. Therefore, at least one of these elements should be known at the moment of starting the research (last visited April 10, 2022).

structured overview of the information relating to that individual that can be found on the internet"[238]. The way in which information can be searched for in the blockchain could decrease the negative impact on the data subject whose data should be erased, making the taking down of the entire blockchain an even more disproportionate measure.

16. *Conclusion*

The alleged incompatibility between public permissionless blockchains and the GDPR and the growing relevance of Ethereum blockchain with respect to use cases suitable for addressing current problems of our society, has conveyed relevance to the issue of its compatibility with the GDPR.

From the analysis carried out, it has emerged that the GDPR applies to the Ethereum blockchain because it falls within its territorial and material scope of application. Moreover, Ethereum blockchain is a service unequivocally addressed also to people residing in the EU and it implies the processing of personal data through electronic means, due to the fact that accounts and transaction data can be considered personal data when related to a natural living person.

The issues highlighted by the literature, which give rise to the incompatibility between public permissionless blockchains and the GDPR, relate to three major areas: controllership, principles of processing, data subject rights.

Concerning the allocation of responsibility roles, even if it is possible to single out the categories of actors who qualify as controllers or processors for given processing activities, it has emerged the lack of correspondence between control and responsibility: those who are held responsible do not have enough control over data to ensure compliance with the law. This mismatch makes the possibility to comply with the principle of accountability a problematic topic

Compliance with the data subject's right of access would be possible only at the application and at the transaction layers; while at the infrastructure level, nodes could legitimately deny access to data due to the impossibility to ensure that data to which access is sought are

[238] Case C 131/12 Google Spain, 2014 para 80.

actually linked to the subject making the request. The right to rectification and the right to erasure are not compatible with the immutability of Ethereum blockchain. However, there is room to argue that they could be respected if a given interpretation of the law is adopted, as long as it ensures sufficient protection of the data subject.

In conclusion, Ethereum blockchain and the GDPR are not incompatible. The major "compatibility" issue derives from the mismatch between responsibility and actual control over data, which could be overcome as blockchain use cases become more user-friendly. As a matter of fact, it is easier to reconcile control and responsibility in the entity which offers the service through an application, when users do not interact with the blockchain directly, but through the application.