universität wien

MASTER'S THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Smart Contracts Under the Light of Article 22 of the GDPR: Can Data Subject Rights be Enforced Successfully on a Blockchain?"

verfasst von / submitted by

Nick Nicklas Alexander Kosloff

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Vienna 2019/ Wien 2019

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Dr. Lukas Feiler

Abstract

In 2016, the European Union adopted the General Data Protection Regulation to unify the EU Member States' data protection laws. As such, the GDPR raised a new benchmark of data protection that gave natural persons more control over their personal data than ever before. The GDPR regulates the enforcement and protection of data subjects' rights and legitimate interests by designating clear entities and procedures for data systems that process personal data. The GDPR's core element is tech-neutrality, i.e., its provisions can be applied to all data systems. Recently, it has been discovered that blockchains can face severe compliance risks under the GDPR, because a number of the general principles are in conflict with those of the GDPR. For example, blockchain is an append-only system, whereas the GDPR gives the data subject the right to have his or her data corrected or removed completely. Blockchain operates on the basis of a peer-to-peer mechanism that aims to eliminate central validating parties, whereas the GDPR explicitly requires the designation of actors that fulfil the obligations of data controllers and processors. This raises question as to whether the rights can be enforced successfully on a blockchain at all. It is also unclear who shall enforce the rights on a blockchain because the actors are hard to identify on blockchain. Smart contracts have become increasingly popular with the spread of blockchain as the platform allows for a seamless execution and storage of their transactional data. However, the GDPR prohibits solely automated data processing under Art. 22(1) and it is likely that the smart contract comes under the prohibition. Technical solutions provide a promising future, provided that the developer community and the EU legislators cooperate to create not only blockchain-specific legislation, but also GDPR-compliant blockchain designs. This thesis concludes that data subject rights are currently only enforceable on private permissioned blockchains if external data silos and proper pseudonymisation techniques are used to protect the privacy of on-chain personal data.

Im Jahr 2016 hat die Europäische Union die Allgemeine Datenschutzverordnung (DSGVO) verabschiedet, um die Datenschutzgesetze der EU-Mitgliedstaaten zu vereinheitlichen. Als solches setzt die DSGVO einen neuen Maßstab für den Datenschutz, der natürlichen Personen mehr Kontrolle über ihre persönlichen Daten gibt als jemals zuvor. Die DSGVO regelt die Durchsetzung und den Schutz der Rechte und berechtigten Interessen der betroffenen Personen durch die Benennung klarer Stellen und Verfahren. Das Kernelement der DSGVO ist die Technologieneutralität, deren Bestimmungen auf alle Datensysteme anwendbar sind. Kürzlich wurde entdeckt, dass Blockchains unter der DSGVO aufgrund der allgemeinen Prinzipien, die im Widerspruch zu denen der DSGVO stehen, grob kompromittiert werden können. Beispielsweise ist die Blockchain ein System, das nur Anhänge enthält, während die DSGVO der betroffenen Person das Recht einräumt, ihre Daten zu korrigieren oder vollständig zu entfernen. Blockchains arbeiten auf der Grundlage eines Peer-to-Peer-Mechanismus, welche der DSGVO die Verpflichtung von Datenverantwortlichkeit und -verarbeitung auferlegt. Dies liegt daran, dass nicht klar ist, ob das Gesetz für eine Blockchain durchgesetzt wird, da die Akteure in der Blockchain schwer zu identifizieren sind. Smart Contracts sind mit der Verbreitung der Blockchain immer beliebter geworden, da die Plattform eine sichere Ausführung und Speicherung ihrer Transaktionsdaten ermöglicht. Die DSGVO unterliegt allerdings einer automatisierten Datenverarbeitung gemäß Art. 22 Abs. 1 und es ist wahrscheinlich, dass der Smart Contract unter das Verbot fällt. Technische Lösungen bieten eine vielversprechende Zukunft, vorausgesetzt, dass die Entwicklergemeinde und die EU-Gesetzgeber zusammenarbeiten, um nicht nur Blockchain-spezifische Gesetze, sondern auch DSGVO-konforme Blockchain-Designs zu erstellen. Diese Arbeit kommt zu dem Schluss, dass die Rechte der betroffenen Personen derzeit nur für private, genehmigte Blockchains durchsetzbar sind, wenn externe Datensilos und geeignete Pseudonymisierungstechniken zum Schutz der Privatsphäre von personenbezogenen Daten in der Kette verwendet werden.

Acknowledgements

I would like to thank my supervisor, Professor Lukas Feiler for his helpful guidance during the process of writing this thesis. I would also like to express my most sincere gratitude to my mother, father and sister for their unconditional love and support during my studies.

I would also like to express my gratitude to Graduate Recruitment at DLA Piper for offering me a training contract.

Helsinki, 6 August 2019

List of Abbreviations

DLT	Distributed Ledger Technology
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
EU	The European Union
GDPR	General Data Protection Regulation

Table of Contents

1 Introduction

I. Background

The GDPR was designed to be technology-neutral.[1] The actors responsible for the duties, and the addressees of rights are clearly identifiable on traditional centralized data systems. However, issues arise in relation to distributed ledger technology (DLT) because its general principles are inconsistent with those of the GDPR and centralized data systems.

Data subject rights under the GDPR, such as the right to erasure and the right to be forgotten, conflict with blockchain technology. The issues arise due to the immutable nature of the platform, which makes enforcing the rights impossible, or difficult to say the least. As such, the current consensus seems to be that in order to avoid compliance issues with the GDPR, each blockchain should be assessed and designed individually around the arising issues.[2] Blockchains should be combined with traditional centralised data systems until the application of the legislation regarding distributed information platforms is clear.

II. Aim

The aim of this thesis is to review and examine the legal compliance of blockchain technology under the General Data Protection Regulation (GDPR), and in particular, the compliance of blockchain-based smart contracts. With smart contracts and distributed ledger technologies (DLT) being implemented in the hopes of efficiency gains come issues of legal compliance: specifically how data subject rights can be enforced on a blockchain; who should enforce them under specific circumstances and whether or not the execution of a smart contract is prohibited under the GDPR. Can fundamental data processing principles of the GDPR, in particular data minimisation and data accuracy, be followed successfully in the

[1] European Commission, 'The GDPR: new opportunities, new obligations' < https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf> accessed 14 May 2019.
[2] Valeria Ferrari, 'EU Block chain Observatory and Forum Workshop on GDPR, Data Policy and Compliance', Institute for Information Law Research Paper No. 2018-04, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247494> accessed 3 April 2019.

execution of smart contracts? If yes, to what extent? If fundamental data subject rights can be exercised on a blockchain, who is responsible for enforcing them and how can the data subject's interests be protected?

III. Delimitations

According to academic and professional commentary, the most severe issues with respect to GDPR-compliance of the blockchain are (1) the identity of the on-chain data controller, (2) the right to erasure, (3) the right to be forgotten and (4) whether or not a blockchain-based smart contract is prohibited under Art. 22(1). The identity of the controller is unclear because attempting to designate a sole controller on a blockchain is like attempting to set a governing hierarchy on a system that was specifically designed not to include one. Moreover, the identity also depends on the nature of the specific blockchain design. With that in mind, it may be possible to create a GDPR-compliant blockchain.

The data subject rights are difficult to enforce because blockchain is censorship resistant. Data cannot be removed or changed, except under extreme circumstances where a large number of nodes cooperate under full consensus. If the smart contract is a form of prohibited data processing under Art. 22(1), there may still be technical workarounds that rely on the consent of the data subject as the legal basis, thus rendering its execution compliant. Lastly, every blockchain has to be designed as GDPR-compliant from the ground-up under Art. 25 privacy by design. This involves executing Data Protection Impact Assessments that assess the risks posed to the data subjects' rights and legitimate interests.

IV. Method and Materials

This thesis follows a legal dogmatic method for examining the relevant ledger technologies and their compliance under the GDPR. The method is used to describe the relevant provisions of the Regulation and their application to blockchain technology. This method has been chosen in order to supplement the aim of the thesis, which is to examine the compliance and applicability of distributed ledger technology (DLT) and the GDPR, in particular the identity of the data controller and whether the execution of the smart contracts comes under the qualified prohibition of solely automated data processing under Art. 22. It must be kept in

mind that there are no case judgements in this area of law so far. Therefore, legal analysis is restricted to the legislative provisions, guidance documents provided by EU institutions and academic as well as professional commentary. For instance, sources, such as the Journal of Institutional Economics, Computer Law Review International and European Data Protection Law Review have been referred to. Dr Lukas Feiler's commentary is also referred to, as well as Paul Voigt's guide on the implementation of the GDPR.

V. Disposition

Before the main legal analysis on data subject rights and the data controller, the thesis sets out with an introduction of the distributed ledger technology and its basic principles. An overview of the main inconsistencies between DLT and the GDPR is provided, e.g., the append-only nature of blockchain and its unsuitability with respect to general principles of data processing. This section will also look at whether blockchain comes under the material scope of the GDPR and whether on-chain data is personal data. Afterwards, the enforcement of data subject rights on blockchain will be analysed. This entails examining the individual difficulties each right poses in respect of blockchain and evaluating compliant solutions. This is followed by a detailed discussion on the right not to be subject to decisions based on solely automated data processing under Art. 22, which requires examining intricate concepts such as the definition of a decision, how human intervention can exist in smart contracts and what constitutes a solely automated decision. Next, the thesis sets out a detailed evaluation on the identity of the data controller on blockchain. This will cover a variety of on-chain actors on public permissionless blockchains and establishes the most reasonable interpretation as to who is the data controller thereof. Finally, the thesis looks at privacy by design under Art. 25 and examines GDPR-compliance of blockchain designs in more detail, followed by a final conclusion.

2 Distributed Ledger Technology

2.1 Introduction

The distributed ledger is a decentralised database which exists in multiple different locations, or amongst numerous participants. The ledger lacks an intermediary that authorises data exchanges. DLT operates via an authentication process that uses asymmetric encryption.[3] A user is represented through the use of a 'public key' that is a username on the platform.[4] Each public key corresponds with a private key that functions as a private password. The combination of these keys functions as a mathematical equation that reveals private encrypted data.[5] The public key can be used to reveal the identity of the user.

2.1.1 Blockchain

Blockchain is an add-only decentralized database that functions on an algorithmic basis and is located on nodes which are peer-operated computers. It is a type of a distributed ledger. All entries of data are confirmed and encrypted. The fundamental feature of blockchain technology and its most famous use-case, Bitcoin, is that it allows mutually distrusting parties to execute contractual obligations without the use of a central third party while also using a decentralized database that has a high level of integrity.[6] The benefits of blockchain technology include its transparent nature and portability of data. This means that anyone can access the data of a public blockchain by setting up a node, which is an independent computer operated by software that accesses and contributes to the network. This opens up opportunities for new technological business ventures and avoids fully centralized data systems that are more vulnerable to hacking. There are different types of blockchains: (1) public permissionless blockchains; (2) public permissioned blockchains; and (3) private permissioned blockchains.

[3] Michèle Finck, 'Blockchains and Data Protection in the European Union' (1/2018), European Data Protection Law Review, 17-35. < https://doi.org/10.21552/edpl/2018/1/6> accessed 22 April 2019.
[4] The 'public key' is a complex order of letters and numbers that indicate the user's identity.
[5] Finck (n 3) 19.
[6] Satoshi Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' (2009) <https://bitcoin.org/bitcoin.pdf> accessed 18 April 2019.

By virtue of its immutable and secure data storage, blockchain has gained popularity in many different industries, such as supply-chain management, healthcare, royalty distribution and cloud storage amongst many other applications.[7] The governance protocol of a blockchain depends on the exercise of free will of all facilitating actors. Every blockchain is based on individual configurations of each participant's software and hardware. Consequently, the functioning depends on the principles and rules created by the community of peers, nodes and miners. Each individual action of data-processing takes place in every node which contains a copy of the ledger. Consequently, peers have a financial incentive to deny false transactions, because obeying the rules of the protocol rewards the miners with more cryptocurrency, i.e., this ought to be more profitable than going against the system.[8] This is how a decentralised consensus exists on blockchain.

Public permissionless blockchains, such as Bitcoin and Ethereum, function on an open and decentralized basis.[9] Anyone can join and exit the network as a reader or a writer.[10] There is no central entity that validates memberships or refuses entry to readers and writers. Therefore, all the on-chain content becomes available to anyone. Private permissioned blockchains are different because only a limited number of peers are allowed to join. A third party validates the memberships of other peers and gives rights to reading and writing to other members. For the purposes of the GDPR, a private permissioned blockchain is easier to implement because the roles of the parties are clearer. For instance, the data subject and the data controller are easier to identify because a controlling undertaking can set a specific governing body for the blockchain.

Private information on blockchains is hidden using cryptography. This is made possible by virtue of a technique called 'hashing' that replaces the attributes of on-chain data with a hash function. The hash function represents any individual element of data with a numerical

[7] Karl Wüst, Arthur Gervais, 'Do you need a Blockchain?' (2017) <https://eprint.iacr.org/2017/375.pdf> accessed 18 April 2019.
[8] Nakamoto (n 6) 4.
[9] Finck (n 3); Gavin Wood, 'Ethereum: A secure decentralized generalised transaction ledger' Ethereum Project Yellow Paper (2014) 151 <https://gavwood.com/paper.pdf> accessed 19 April 2019.
[10] The *reader* is an individual or some other entity who does not add to the blockchain. This individual is only participating in transactions, reading the ledger or auditing the chain. The *writer* extends the blockchain or validates the chain.

identity.[11] For the layman, this can be understood as a *fingerprint* of any individual data. When data is being processed on a blockchain, a hash is created for that specific data. The corresponding hash is then stored on the blockchain network while the data unit instead may be stored on an external database.[12] Information is stored chronologically by hashing the data onto the blocks. If a user alters the on-chain data, a trace is left on all the blocks. This is how immutability on a blockchain works in practice.[13]

2.1.2 Smart Contracts

Independently executing code can be traced back to 1994 and Nick Szabo's description of smart contracts as 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises'.[14] Nick Szabo is an American computer scientist who is credited as the inventor of the smart contract and a respected contibutor to the science of cryptography.[15] Szabo was fascinated by the idea of computer software that had similarities with contractual clauses and could be embedded on data systems with the purpose of discouraging the parties from breaching their side of the contract.[16]

Smart contracts operate as independently executing digital code that automatically interprets its input values when the code is triggered by a particular pre-disposed event. Smart contracts are a method of automated data processing that is advantageous due to its efficiency benefits and suitability for modern technological markets and ventures.

A smart contract can provide exceptional contractual certainty due to the decentralized nature of blockchain technology. If one or more nodes do not function, the code will execute on other available nodes. This is because the platform's functioning is dependent on a large number of independent nodes. This highlights the advantages of decentralisation in the

[11] Grant Thornton, *GDPR & Blockchain, Blockchain solution to General Data Protection Regulation*, <https://www.grantthornton.global/globalassets/___spain___/links-ciegos/otros/gdpr--blockchain.pdf> accessed 10 April 2018.
[12] ibid.
[13] See further, Conte de Leon et al, 'Blockchain: Properties and Misconceptions' (2017) 11 Asia Pacific Journal of Innovation and Entrepreneurship https://www.emeraldinsight.com/doi/full/10.1108/APJIE-12-2017-034 accessed 16 May 2019.
[14] Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 11 March 2019.
[15] Nathan Reif, 'Who is Nick Szabo, and is he Satoshi Nakamoto?' (2018) < https://www.investopedia.com/news/who-nick-szabo-and-he-satoshi-nakamoto/> accessed 4 June 2019.
[16] ibid.

execution of digital contracts. Small systematic failures do not have a drastic impact on the overall result of the data processing.

It is important to remember that smart contracts often require a human counterpart, a group of people or even an independent digital programme that uses natural language to type in the input values. This is because the computer-programmed nature of smart contracts executes after a certain event is completed, for example a monetary payment or a digitally confirmed physical possession of a good.[17] However, smart contracts are capable of more than this; smart contracts are being engineered to provide intellectual property licenses and manage organizational coordination.[18]

[17] However, this is dependent on the nature of the blockchain algorithm itself.
[18] Davidson S., De Filippi P. and Potts J., 'Blockchains and the economic institutions of capitalism' (2018) Journal of Institutional Economics 14(4), 639-658 <doi:10.1017/S1744137417000200> accessed 17 April 2019.

3 The Scope and General Principles of the General Data Protection Regulation

3.1 Introduction

In 2016, the European Union adopted the GDPR to unify its privacy and data protection laws. The GDPR supersedes the EU's Data Protection Directive (DPD)[19] and enhances the privacy rights that EU citizens can enforce against undertakings that collect and use their personal data.[20] The biggest change is the unification of data protection laws across EU countries.[21] With its tough requirements for undertakings and sanctions for violations, the GDPR has set a high standard for data protection laws. Undertakings may now risk administrative fines of up to four percent of annual worldwide turnover, or EUR 20,000,000 whichever is higher, for violating the protected rights.[22] A distinct feature of the GDPR is also its territorial scope which extends beyond the geographical limits of the EU, provided the processed data relates to a data subject resident in the European Union.[23] For example, an Indian company that processes the personal data of EU nationals will be subject to the GDPR.

3.2 Scope of the GDPR

The GDPR applies to the processing of personal data by automated systems, and sometimes to manual processing of personal data.[24] Processing means any operation that is performed on personal data, regardless of automation, such as collection, storage, organisation or

[19] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter DPD].
[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, [hereinafter GDPR].
[21] Recital 7 GDPR.
[22] Art. 83(4)-(5); GDPR DLA Piper, 'A guide to the General Data Protection Regulation' (2018), https://www.dlapiper.com/en/uk/insights/publications/2016/12/a-guide-to-the-general-data-protection-regulation/, (accessed 4 March 2019).
[23] Art. 3 GDPR.
[24] Art. 2(1) GDPR '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. '

alteration.[25] The GDPR applies to personal data processing which is linked to the EU.[26] This happens when an entity that processes personal data is established in the EU, or when the entity is located outside of the EU but offers goods and services to the people within the EU.[27] The GDPR applies to various undertakings, such as companies, associations and organisations. However, there are exemptions. The GDPR does not apply to data processing conducted for the purposes of a purely 'personal or household activity'.[28] This means that if the processing has no connection to a professional or commercial activity it is exempt from the GDPR's scope. [29] This includes correspondence of addresses, social networking or private bank account management.[30]

3.3 Personal Data and Pseudonymization

Personal data is any information that relates to an identified or an identifiable individual.[31] An identifiable individual can be identified directly or indirectly by referring to an identifier such as, a name, location data or other personal factor.[32] Encrypted data and other electronic identities are also considered personal data.[33] Information which has been pseudonymised but can be related to a natural person with the use of additional data also constitutes personal data.[34]

The GDPR introduces the category of pseudonymised data.[35] Pseudonymisation separates data from direct identifiers, which makes identifying a natural person impossible without ancillary information. The definition of pseudonymisation comes from Art. 4(5) of the GDPR:

> '"[P]seudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data

[25] Art. 4(2) GDPR.
[26] See Arts. 1-2 GDPR.
[27] Art. 3 GDPR.
[28] Art. 2(2)(c) GDPR.
[29] Recital 18 GDPR.
[30] ibid.
[31] Art. 4(1) GDPR.
[32] ibid.
[33] The Swedish Data Protection Authority, Datainspektionen, 'The purposes and scope of the General Data Protection Regulation' < https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/the-purposes-and-scope-of-the-general-data-protection-regulation/> accessed 7 June 2019.
[34] Art. 4(1) GDPR.
[35] Art. 4(5) GDPR.

> subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'

Whether pseudonymised data can be classified as personal data depends on whose information and skills are taken into consideration.[36] At least the controller and processor must be considered because they have access to the personal data.[37] If one entity or a person is able to identify a natural person by means that are *reasonably likely* to be used then the natural person is identifiable.[38]

This is arguably an objective test. Factors, such as the costs of measures and time required for identification in respect of available technological measures must be taken into consideration.[39] However, the scope of personal data can also change retrospectively because the test takes into account future technological developments.[40] Therefore, pseudodymised data may become anonymised data in the future, and vice versa.

Lastly, anonymous data escapes the scope of the GDPR completely.[41] This refers to information that does not relate to an identified or an identifiable person, or to personal data which has been rendered irreversibly anonymous to an extent that the data subject is not, or no longer identifiable.

3.4 General Principles of Data Processing

The GDPR contains fundamental principles that must be followed during any form of data processing. These apply to all types of processing and are outlined below.

[36] Paulina Jo Pesch, Christian Sillaber, 'Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements' (6/2017) Computer Law Review International,167-172, <https://ssrn.com/abstract=3210499> accessed 22 April 2019.
[37] GDPR Recital 26.
[38] ibid.
[39] Ibid.
[40] Lukas Feiler, The EU General Data Protection Regulation (GDPR -) A Commentary (German Law Publishers 2018) 61.
[41] Recital 26 GDPR.

3.4.1 Lawfulness

All processing of personal data must be lawful, fair and transparent.[42] This means there must be lawful grounds to process the data. Other relevant national legislation must also be complied with.

3.4.2 Purpose Limitation

Under Art. 5(1)(b) of the GDPR personal data must be collected for a 'specific, explicit and legitimate' purpose.[43] These purposes must be decided before the processing. Personal data cannot be 'processed' in a way that is 'incompatible' with the original purpose.[44] The purposes will only be *explicit* if they are documented in a manner that makes them not only understood by the controller and the processor, but also by the supervisory authority and the data subject.[45] The undertaking cannot enforce 'checks' as the purpose of surveillance without also stating the purpose for the checks.[46] The purposes must also be legitimate, i.e., have a lawful basis under the GDPR and other applicable data protection legislation.[47] Furthermore, the data subjects also have the right to know why their personal data is being processed.

3.4.3 Data Minimization

Personal data that is collected must never be too extensive with respect to the purpose of its processing.[48] An undertaking can never process more data than is necessary, and the collected data must be clearly connected to the purpose of the processing.[49]

[42] Art. 5(1)(a) GDPR
[43] GDPR Art. 5(1)(b).
[44] ibid.
[45] Lukas Feiler (n 40) 75.
[46] Datainspektionen (n 33).
[47] ibid.
[48] Art. 5(1)(c) GDPR.
[49] Datainspektionen (n 33).

3.4.4 Accuracy

Undertakings must take all reasonable steps to ensure that the personal data is kept up-to-date, and to ensure that data that are inaccurate, are erased or rectified without delay.[50] This principle makes it essential to have in place procedures that rectify and remove inaccurate personal data, in the event of a data subject request.

3.4.5 Storage Limitation

Personal data can only be stored for as long as it is needed for the specific purpose of the processing.[51] When the data is no longer needed, it must be erased or anonymised. Certain procedures should be in place that undertake regular checks for the purposes of erasure after certain periods of time.[52]

3.5 Is On-chain Data Personal Data?

3.5.1 Interpreting the GDPR

Currently, there is little case law that assists in understanding the precise meaning of GDPR provisions with regards to its application on a blockchain. Therefore, the general provisional background and other soft law instruments shall be used throughout this thesis as interpretative tools in order to apply the law. These include the Recitals of the GDPR. However, it should be noted that the CJEU has interpreted preambles restrictively in its past practice.[53] A Community Act does not have binding legal force and cannot be relied on as a ground for derogating from the true wording of a provision.[54] As a result, Recitals cannot have independent legal effect themselves.

In addition, the Article 29 Working Party Guidelines are important for the purposes of interpreting the GDPR as they provide examples and clarify many of the ambiguous

[50] Art. 5(1)(d) GDPR.
[51] Art. 5(1)(e) GDPR.
[52] Datainspektionen (n 33).
[53] Directive 2000/78/EC is an example, which includes 'normative' recitals without corresponding provisions in the binding parts of the Directive. The CJEU follows the wording of the Recitals, but does not give much credit to the preamble. (Case C-267/06 *Tadao Maruko* [2008] ECLI:EU:C:2008:179, paras. 49-60).
[54] Case C-162/97, *Nilsson*, [1998] ECLI:EU:C:1998:554, para. 54

terminology regarding profiling and automated decision-making, as well as other provisions.[55]

3.5.2 Applying the GDPR on a Blockchain

The basic principles of data processing and the scope of personal data have been identified in the previous section. In order to examine whether data subject rights can be enforced, or must be enforced on a blockchain, the data system must come under the material and territorial scope of the GDPR. Hence, the GDPR applies to a blockchain if the processed and stored on-chain data can be considered personal data. There are two primary categories of data that must be examined: (1) transactional data and (2) public keys.

The transactional data contains data which relate to specific transactions. This can be stored (1) in plain text; (2) in encrypted form; or (3) in hashed form. It must be examined whether encryption or hashing can render data anonymous, i.e., such form that identification of the data subject is irreversibly prevented and the scope of GDPR is avoided.[56]

On-chain personal data in the form of text remains personal data for the purposes of the GDPR by virtue of it containing information which can be *prima facie* linked to natural persons. Encrypted data on the other hand can be accessed with the use of the correct private key and therefore cannot be considered prima facie *irreversibly* anonymized. Encryption techniques are also considered forms of pseudonymisation by Article 29 Working Party in the Guidelines on Anonymisation[57]. Consequently, encrypted transactional data is personal data for the purposes of the GDPR.

Hashed data also qualifies as personal data. Regardless of the fact that hashing can serve as a method for high-level privacy protection, it cannot avoid being qualified as personal data under the GDPR. The WP29 Guidelines on Anonymisation have decided that hashing is a

[55] Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679,* WP 251 (3 October 2017, revised 6 February 2018) [hereinafter: WP29 Guidelines on Automated Decision-Making].
[56] Article 29 Working Party, 'Opinion 04/2014 on Anonymisation Techniques' (2014) 0829/14/EN, 20 hereafter: WP29 Guidelines on Anonymisation).
[57] ibid.

technique of pseudoymisation, not anonymisation.[58] Consequently, hashed data is also personal data.

In respect of the test of pseudonymisation, encrypted data can escape the scope of the GDPR in the future if cryptographic techniques develop enough to render data anonymous. Vitalik Buterin, the founder of the Ethereum Blockchain, has also claimed that cryptographic obfuscation can serve as a useful technique of anonymisation but it is not developed enough yet.[59] Furthermore, blockchains that store their on-chain transactional data set on a secure private storage can be used. They leave the hash pointer of the data on the chain itself for the purposes of validating the transaction. However, the meta-hash and the public key have to be treated according to the GDPR rules because they can still remain under the scope of the Regulation.[60] It is concluded that on-chain transactional data remains personal data for the purposes of the GDPR. This leaves the examination of the public key.

The public keys on a blockchain are complex combinations of numbers and letters. They function as the alternative identities of legal and natural persons that access the blockchain for various purposes. Based on the above-mentioned discussion on pseudoymisation for the purposes of the GDPR[61], the public key cannot be attributed to a data subject unless the key is linked to 'additional information' such as a name or address. Hence, it must be examined whether the public key can be categorised as anonymised data, and escape the scope of the GDPR.

Despite the asymmetric encryption of the blockchain, identifying the natural person behind a public key is possible. This is often achieved by virtue of voluntary sharing of the public key on websites, such as blogs and crowd-funding sites.[62] There are also agencies which have developed forensic analysis methods that identify individuals by tracking the public key and its relevant transaction history.[63] The public key can even be traced back to an IP address in

[58] ibid.
[59] Vitalik Buterin, 'Privacy on the Blockchain (Ethereum Blog, 15 January 2016) https://blog.ethereum.org/2016/01/15/privacy-on -the-blockchain/ accessed 8 June 2019 (hereafter Buterin, 'Privacy on the Blockchain').
[60] James Smith et al, 'Applying Blockchain Technology in Global Data Infrastructure' (2016) Technical Report ODI-TR-2016-001, Open Data Institute https://data.gov.ru/sites/default/files/documents/315354748-applying-blockchain-technology-in-global-data-infrastructure.pdf accessed 9 June 2019.
[61] See Chapter 2.3 Personal Data.
[62] For example, < https://shop.wikileaks.org/donate>
[63] See https://www.chainalysis.com/.

some cases.[64] In *Patrick Breyer v Germany* the CJEU decided that a dynamic IP address is personal data even if a third party is in possession of the relevant information required to identify the specific data subject.[65]

Which parties are considered for the purposes of the *Breyer* test? The answer depends on whose knowledge and skills are taken into account under the test of pseudonymity.[66] The test has been interpreted broadly before. In *Breyer*, the Court said that means are not *reasonably likely* to be used if the identification of the data subject is 'prohibited by law' or is 'practically impossible'. Identification is 'practically impossible' if it requires a 'disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears to be insignificant'.[67] Furthermore, the information of a third party is taken into account only if the controller has legal means to obtain the additional information from the third party.[68] Consequently, third parties who gain access to the on-chain data in addition to the controller and processor are relevant with respect to blockchain. As a result, all users that can access the on-chain data and have legal means to obtain additional information which allows to identify a data subject must be considered under this test.

The GDPR does not apply to processing conducted by a natural person in the course of a purely personal or household activity.[69] Data processing which has no connection to a professional or commercial activity is exempt from the GDPR.[70] The smart contract is not a purely personal or household activity because it is used to fulfill contractual obligations between mutually distrusting parties, often in a commercial context. Furthermore, information stored on public permissionless blockchains is available to every internet user and cannot be exempt under the household exception because of the scope of accessibility is larger than that of household activities.

Consequently, in order to effectively protect data subject rights on a blockhain, the public key should also constitute personal data for the purposes of the GDPR. However, the public key

[64] Biryukov et al, 'Deanonymisation of Clients in Bitcoin P2P Network' (2014) <https://arxiv.org/pdf/1405.7418.pdf> accessed 30 April 2019.
[65] Case C-582/14 *Patrick Breyer* [2016] EU:C:2016:779.
[66] See Section 3.3 on personal data.
[67] CJEU Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EC:C:2016:779, para 46.
[68] ibid. para 47.
[69] Art. 2(2)(c) GDPR.
[70] Recital 18 GDPR.

cannot be transferred to a private data storage, because it is essential on-chain metadata. There are solutions to complicate identification. So called ‘noise’ can be added to the smart contract data, which means that transactions are grouped together in order to make it difficult to identify senders and recipients outside of network of the relevant parties. This technique has been recognised by the WP29 Guidelines on Anonymisation as an anonymisation technique.[71]

3.5.3 Can General Principles of Data Processing be Complied with on Blockchain?

The main concern for compliance is the append-only nature of blockchain. Distributed ledgers collect more data as blocks of information are added. Additionally, each node contains an independent copy of the entire database which goes against the general principles of data processing.

The validation rules of blockchains are commonly available to users. Thus, the transparency and lawfulness of the processing is not difficult to comply with. Issues arise with respect to accountability, because the controller is not a centralised entity and cannot be identified on a permissionless blockchain. Hence, a controller is potentially impossible to contact for the purposes of a data subject request. If the nodes are joint controllers, or an actor is designated as the controller on a governance structure on a private blockchain, accountability is easier to comply with because the data subjects can express their consent to having their data processed to an identified actor.

With respect to purpose limitation, on-chain data can encounter usage which was unfamiliar to the collecting party and the data subject at the beginning of the processing. Art. 5(1)(b) GDPR requires the collecting party to notify the data subjects of all forms of processing that the personal data is being engaged with and monitor its own behavior carefully in order to avoid infringing the GDPR. It is possible to inform the data subject of the purpose, but it is difficult to prevent someone from accessing on-chain data and using it for another purpose, especially on a public permissionless blockchain.

[71] WP29 Guidelines on Anonymisation Techniques (n 56) 12-13.

Distributed ledgers collect more data as blocks of information are added. Additionally, each full node contains an independent copy of the entire database which goes against the principle of data minimisation. The principle is difficult to implement in practice. One solution is to store transactional data off-chain, allowing the data to be minimised without interference to the chain. This is easier to implement on a private permissioned blockchain which can be controlled by a specific amount of nodes in a specific enterprise. However, the purpose of using the blockchain is reduced as an external database must be used instead of a solely distributed solution.

The principles of data accuracy and storage limitation are in direct conflict with the functioning of blockchain, which has severe implications for the enforcement of two data subject rights: (1) the right to erasure and (2) the right to amendment. Blockchains keep the entire transaction history on-chain and prevent modifications, except under extreme circumstances of full-consensus and system forks.[72] This means that on-chain data cannot be modified or deleted on-demand, as required by the GDPR.

3.5.4. Solutions and Examples

The easiest way to comply with the general principles of data processing is to store data off-chain. However, this diminishes the benefits of using blockchain, because a centralised data silo is more vulnerable to privacy infringements and does have the efficiency benefits of distributed data solutions. Another solution is to use a different private key/public key combination for each new transaction.[73] This prevents the continuity of identities of transactional actors on the basis of public key data sets. Yet another solution is to implement zero-knowledge proofs, according to which a party (the user) can prove to another party (the validator) that he/she has knowledge of the value of x, without transferring any additional information.[74] Compliance solutions will be discussed in greater detail in Chapter 7.

[72] These concepts are covered in greater detail in Chapter 5 on the Controller in Blockchain.
[73] J. D. Nick, "Data-driven De-Anonymization in Bitcoin," Master's thesis, Computer Systems Institute - ETH Zurich, 2015 < https://www.research-collection.ethz.ch/handle/20.500.11850/155286> accessed 10 June 2019.
[74] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von Neumann architecture," in 23rd USENIX Security Symposium (USENIX Security 14), <https://eprint.iacr.org/2013/879.pdf> accessed 10 June 2019.

3.5.5 Interim Conclusion

On-chain data of smart contracts, as well as the public keys come under the material scope of GDPR. The general principles of data processing are difficult to implement by virtue of the immutability of blockchain, but there are technical workarounds, such as using centralised data silos and various public key sets.

4 Can Data Subject Rights be Enforced on Blockchain?

4.1 Introduction

As mentioned above, both the transactional data and the public keys can constitute personal data for the purposes of the GDPR. Under the GDPR, the data subjects have a number of rights with respect to the processing of their personal data. This chapter examines the issues which can be encountered when data subject rights are claimed against the controller on a blockchain. It may be possible that the data subject can claim rights against every single node on the blockchain. This issue will be further examined in Chapter 5 in respect of the controller on blockchain. Currently, it remains unclear how data can be corrected, erased or accessed on blockchain due the immutable nature of the platform.

4.2 Right of Access by the Data Subject

Under Art. 15 of the GDPR, a data subject has the right to receive information as to whether or not his or her data is being processed.[75] The sub-paragraphs of the provisions state a number of categories of information which must be provided, such as the purpose of the processing, the recipients to whom the personal data will be delivered and the right to file complaints regarding the processing.[76] Furthermore, the data subject has the right to receive a copy of information which is being processed.[77] For example, a Facebook user can request to receive a copy of all personal data that has been processed on the website.[78]

Art. 15(2) GDPR states that the data subject has the right to be informed about the safeguards that can be used in situations where data is transferred outside of EU/EEA.[79] This is relevant with respect to a node operating in the EU which shares personal data with other nodes that operate outside of the EU/EEA. Since under some circumstances controllers will not know

[75] Art. 15 GDPR.
[76] ibid.
[77] Art. 15(3) GDPR.
[78] Facebook, 'Accessing and Downloading Your Facebook Information' <https://www.facebook.com/help/contact/2032834846972583> accessed 4 June 2019.
[79] Art. 15(2) GDPR.

what data is stored on the blockchain and where other nodes are located, Art. 15 is difficult to enforce in practice. Especially, because on-chain personal data is hashed or pseudonymised.

The right of access is not an absolute right, but must be enforced without adversely affecting the rights and freedoms of others.[80] Para 63 of the Preamble to the GDPR also states that where the controller processes a large quantity of personal data, the controller should be able to request the data subject to specify the information, and or processing activities to which the request relates.[81] This is difficult in blockchain because of asymmetric encryption but not impossible by virtue of some technical solutions.[82] In any case, it can be argued that the data controller could refuse the data subject request if it is is manifestly unfounded or excessive under Art. 12(5) GDPR. This is because the controller cannot identify which on-chain data belongs to a specific data subject.

If a data subject attempts to contact a node in order to make a data subject right request under the suspicion that his or her personal data is being processed, the node is not able to comply with this obligation due to the cryptographic measures that have rendered the data unidentifiable *prima facie*.[83] Furthermore, under Art. 15(3) GDPR the data subject has the right to receive a copy of information which is being processed.[84] For example, a Facebook user can request to receive a copy of all personal data that has been processed on the website.[85] Encrypted copies of data would unlikely be considered to have been provided in a 'commonly used electronic form' because they have little to no use to the data subject. [86] On a permissionless blockchain this may be different because the data subject could access the data himself. It must be considered whether this could satisfy the conditions of Art. 15. The issue is that the data controller does not provide the data. Instead, the data subject would have to go through all the data of a public chain to identify his or her personal data on the basis of hash locations.

[80] Art. 15(4) GDPR.
[81] Para. 63 of the Preamble to the GDPR.
[82] See para. 3.5.4. Solutions and Examples.
[83] Finck (n 3) 30.
[84] Art. 15(3) GDPR.
[85] Facebook, 'Accessing and Downloading Your Facebook Information' < https://www.facebook.com/help/contact/2032834846972583> accessed 4 June 2019.
[86] Art. 15(3) GDPR.

The bottom-line is that considering Art. 15, it is arguably more advisable to store the transactional data off-chain and leave a hash location on-chain. This allows personal data to retain easily identifiable form, while still letting businesses take advantage of the integrity of a blockchain, for example for accounting purposes.

4.3 Right to Rectification

Under Art. 16 of the GDPR, the data subject has the right to request the rectification of data from a controller without undue delay. Enforcing the right to rectification is confusing because a data subject has to contact one or more nodes on the blockchain. Firstly, the data subject cannot identify the nodes that have a full copy of the ledger. This is because nodes can be offline or change their IP addresses.[87] Secondly, even if a node was successfully reached, it cannot change the on-chain data because the platform is immutable. Thus, the stored information can only be altered under extreme circumstances, such as where a system fork is applied.[88] A system fork refers to a process where the source code of a programme is copied. As a result, independent chain development is then commenced on the copy.[89] Enforcing the right to rectification on blockchain seems almost impossible.

It is argued that Art. 16 can be enforced with reference to the particular technology that is being used. Art. 16 of the GDPR says that 'purposes of the processing' have to be taken into account and data can be rectified 'by means of providing a supplementary statement'.[90] At the end of the day, it is up to the courts to decide if data can be rectified by adding a statement on a new block of data. This will not delete or correct the old data, but can ensure compliance under Art. 16. Considering this, it is still preferable to store transactional data off-chain, so that it can be altered later on without struggling with the immutable nature of blockchain. However, this can only ensure compliance for the purposes of transactional data and not public keys which remain on-chain under all circumstances.[91]

[87] Bitcoin nodes, 'Global Bitcoin Nodes' <https://bitnodes.earn.com/> accessed 2 May 2019.
[88] Michael del Castillo, 'Ethereum Executes Blockchain Hard Fork to Return DAO Funds' < https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds> accessed 9 May 2019.
[89] 'Understanding Hard Forks in Cryptocurrency' https://cryptocurrencyfacts.com/understanding-hard-forks-cryptocurrency/ accessed 10 May 2019.
[90] Art. 16 GDPR.
[91] Finck (n 3) 29.

So far, the right to rectification is the only right that provides slight leeway for the purposes of implementing it on the blockchain, i.e., the regulation expressly mentions that the application depends on the purpose of the processing. This can be interpreted as providing leeway with respect to particular technologies. The controller must communicate the rectification to each person to whom the personal data may have been disclosed.[92] This can be avoided on the blockchain if the fulfilment of this obligation proves to be 'impossible or involves disproportionate effort'.[93]

4.4 Right to Erasure ('Right to be Forgotten')

The data subject has the right to request the 'erasure of personal data concerning him or her without undue delay.'[94] This obligation must be fulfilled by the controller under a number of conditions: (1) the personal data may no longer be necessary for the purposes it was processed; (2) the data subject has withdrawn consent on which the processing was based or other grounds have ceased to exist; (3) the data subject has objected to the processing and the controller has no overriding legal interest; the data is being processed unlawfully; (4) controller is subject to EU Member State law that requires the personal data to be erased; or (5) the personal data was collected for the purposes of offering information society services.[95]

The blockchain is unable to forget information that has been stored on it. Satoshi Nakamoto designed the data system to be resistant to censorship.[96] Consequently, enforcing the right to be forgotten in its pure form is inapplicable on the blockchain because data cannot be changed or deleted by default. A distinction can be made between the transactional data and the public keys. If the transactional data is stored in an off-chain database it can be deleted accordingly with the GDPR requirements.

Public keys are less clear. Art. 17 of the GDPR does not give the data subject an absolute right. When the data controller receives a request to erase data, he or she must take into account 'available technology and the cost of implementation'.[97] Consequently, the controller

[92] Art. 19 GDPR.
[93] ibid.
[94] Art. 17 GDPR.
[95] Art. 17(3) GDPR.
[96] Nakamoto (n 6).
[97] Art. 17(2) GDPR.

must take 'reasonable steps, including technical measures, to inform controllers processing personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data'.[98] An option is to interpret 'available technology' as allowing data to not be completely erased because of the technical nature of blockchain. De Filippi has suggested that deleting the private key of the data subject can constitute erasure for the purposes of the GDPR.[99] As a result, the transactional data will remain on-chain but cannot be accessed anymore by the controllers or the data subject himself. This method has also been suggested by CNIL, which states that although erasure is technically impossible on blockchain, state-of-the-art technology can be used to make information inaccessible.[100] Deleting the private key makes the verification of hashed data impossible.[101]

4.5. Right not to be Subject to Decisions Based on Solely Automated Data Processing

Under Art. 22(1) of the GDPR the data subject has a right not to be subject to decisions based on solely automated processing:

> 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'[102]

The data subject can claim his or her respective right according to Art. 22 under the following conditions: (1) a decision must be executed; (2) the decision must be executed as a result of automated processing; (3) the decision must be the result of *solely* automated processing; and (4) the decision must be executed without *human intervention*. If these conditions are met, Art. 22 can be invoked by the data subject if the decision (A) 'produces legal effect

[98] ibid.
[99] Primavera De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) 9 Journal of Peer Production http://peerproduction.net/wp-content/uploads/2016/08/blockchain-technologies-draft.pdf accessed 10 May 2019.
[100] Commission Nationale Informatique & Libertés, 'Blockchain: Solutions for a responsible use of the blockchain in the context of personal data' (2018) 8 < https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf> accessed 28 May 2019.
[101] ibid. 9.
[102] Art. 22(1) GDPR.

concerning him or her' or (B) 'similarly significantly affects him or her'.[103] A question arises: is Art. 22 a right or a prohibition?

Under a purposive interpretation of Art. 22, the provisions of have been enacted in order to *prevent* data subjects from being subject to decisions taken by machines, which enable legal effects on them.[104] Under a literal interpretation, the functioning of Art. 22(1) is dependent on whether or not the data subject exercises his or her free will to claim the right against a data controller. Omitting to exercise this would mean that automated decisions including the qualifying characteristics of Art. 22(1) could be taken in respect of the data subject. This implies the possibility to execute fully automated decisions with legal consequences on the data subject, without him or her having legal means to dispute the decision.[105] This gives too much leeway for controllers to execute decisions regarding data subjects, considering that the the purpose of the GDPR is to give data subjects independent control of their data. Consequently, the purposive interpretation should be followed. The term 'right' in the provision means that Art. 22(1) of the GDPR prohibits decision-making based on solely automated processing, and it applies regardless of whether the data subject takes action against a decision.[106]

Art. 22(2) lays down exceptions when automated decision-making is allowed. When Art. 22(2)(a) or (c) applies, the controller must implement certain safeguards under Art. 22(3) to enforce the legitimate rights and interests of the data subject. Under these circumstances the data subject has a right to obtain human intervention on the part of the controller and contest the decision.[107] This right must be exercised by the data subject, compared to the data subject being protected under a general prohibition under Art. 22(1).

Whether a blockchain-based smart contract is considered solely automated data processing warrants a more extensive examination in Chapter 5. This involves a detailed discussion as to what constitutes a decision, when is it *solely automated* and who can intervene in its execution etc.

[103] Art. 22(1) GDPR.
[104] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer Publishing 2017) 180 (emphasis added).
[105] WP29 Guidelines on Automated Decision-Making (n 55) 20.
[106] ibid. 19.
[107] Art. 22(3) GDPR.

4.6 Interim Conclusion

Data subject rights are problematic to enforce on blockchain. Issues arise especially due to the immutable nature of the platform. While right of access and right to information can be granted via methods of general notice or other digital means coded onto the blockchain, right to erasure and amendment can never be enforced entirely as legislated in the GDPR. The controller and developer should consider storing the hash location of personal data on-chain whereas the actual data can be stored on a separate off-chain data storage. Although, this diminishes the purpose for using blockchain, it can enable the controller to avoid large fines under Art. 83. A test-case should be tried where the hashed data is made inaccessible by virtue of erasure of the private key. Whether or not this solution is equal to the protection required under the GDPR remains to be decided in court.

The bottom-line is that until the exercise of these rights on a blockchain is examined thoroughly by the European Data Protection Board, and before binding judgments come from the CJEU, undertakings should be advised to use private permissioned blockchains. This is because the number of nodes is significantly more limited compared to public permissionless blockchains, and specific governing bodies can be designated in order to protect data subject rights and interests. This makes erasure of on-chain data simpler and the risk of data subject rights infringements is smaller.

5 Does a Smart Contract come under Art. 22?

5.1 Introduction

Under Art. 22(1) GDPR the data subject shall have a right not to be subject to decisions based on solely automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

It will now be examined whether the execution of a smart contract comes under the scope of Art. 22 GDPR. The execution of a smart contract can come under Art. 22 of solely automated data processing if it can be considered fully automated data-processing and produces legal or significantly similar effects on the data subject. The conditions of Art. 22(1) shall be examined in the following order: (1) the meaning of decision; (2) meaning of solely automated processing; (3) capability of smart contracts to produce legal or significantly similar effects; (4) exceptions to Art. 22(1); and (5) meaning of human intervention.

5.2 Decision for the purposes of Art. 22(1)

A smart contract must be considered a 'decision' under Art. 22(1) GDPR. Decision is not explicitly defined in the provision, but automated processing is referred to as 'the ability to make decisions by technological means without human involvement.[108] The WP29 Guidelines on Automated Decision-Making suggest that automated processing does not need to include profiling in order to fall within the scope of Art. 22(1). Therefore, when a decision is executed by virtue of technological means, without human intervention, it shall come under the scope of Art. 22(1).

Firstly, a 'decision' can be the final digital execution of the smart contract code on blockchain where property and other legal obligations are transferred between mutually distrusting individuals. This follows the rationale of Art. 22(1) because there is no human involvement in this particular event. Secondly, 'decision' can refer to a much larger scope of events such as the pre-contractual negotiation stage where the code is designed, where input

[108] ibid. 8.

values are stored on-chain and where a contract is *de facto* negotiated between mutually distrusting parties. Recital 71 GDPR reads that data subjects have the right not to be subject to a 'decision, which may include a measure' based on automated processing.[109] Thus, the term 'measure' could refer to pre-contractual negotiations or other infrastructural matters.

However, this interpretation is less likely to be applicable, because Art. 22(2)(a) includes an exemption from the prohibition of solely automated data processing where the smart contract is used for contractual performance.[110] If para. 1 would take pre-contractual negotiations into account, the scope of the prohibition would be easy to avoid and there would be no purpose for it in the first place. Moreover, the WP29 Guidelines provide examples for solely automated data processing, such as a fine issued on the basis of speeding camera evidence. This is a simple social contract that functions on the basis of 'if x then y',[111] which suggests that trivial pre-contractual events cannot fall under the scope of Art. 22(1). The example suggests that the focus is on the execution of the decision. The CJEU is likely going to decide accordingly in the near future.

Finally, Recital 71 states that the data subjects have the right 'not to be subject to a decision […] evaluating the personal aspects relating to him or her'. This implies a narrow scope, but its applicability would render the provision useless for many smart contract applications. Dr. Lukas Feiler suggests that until this issue is clarified by the CJEU, it should be assumed that Art. 22(1) also applies to decisions that are not based on evaluations of personal aspects relating to the data subject.[112] Accordingly, a narrow interpretation would render many smart contracts inapplicable under Art. 22(1), because a large amount of use-cases consider basic factual data, e.g., whether payment has been received or whether goods have been transferred. Therefore, a broad scope protects the data subjects' right not to be subject to automated data processing better.

Consequently, the execution of the smart contract must be considered a decision for the purposes of Art. 22(1). The smart contract can fall under the scope of Art.22(1) if the execution is additionally a form of solely automated data processing.

---

[109] Recital 71 GDPR.
[110] Art. 22(2)(a) GDPR '[Para. 1 shall not apply] if the decision is necessary for entering into, or performance of, a contract between the data subject and a data controller'.
[111] WP29 Guidelines on Automated Decision-Making (n 55) 8.
[112] Lukas Feiler (n 40).

5.3 What is Solely Automated Data-Processing?

Under Art. 22(1) of the GDPR, the decision must be based on *solely* automated processing, which means that there can be no human involvement in the decision-making process.

The WP29 Guidelines on Automated Decision-Making contain a narrow interpretation for 'solely'. The Guidelines read that ' "based solely" means that there is no human involvement in the decision-making process. In order to avoid qualification as solely automated decision by virtue of human intervention, the intervention cannot be "fabricated" and must have "an actual influence on the result" '.[113]Any external influence on the decision must also be 'meaningful'.[114] On blockchain, only a consensus of protocol actors have the power to materially change on-chain data, which means that human intervention is difficult to conduct by default.

It is difficult to have an external effect on a smart contract, because the process is a coded if/then event. Constituting a meaningful external effect can require the consensus of all the blockchain actors to reboot the chain in order to change the hashed data or the rules of processing. A single node or an actor cannot change the data of all ledgers on blockchain. It can be argued that the party who has authority and competence to change the decision is the data subject because he/she has the capacity to agree to the processing of input values. Therefore, there can be no final contract without the exercise of free will of the data subject.

The definition of 'meaningful' remains to be examined. It can be argued that a *de minimis* threshold shall be used on a case-by-case basis but it is unclear on whom the burden of proof would rest. According to a purposive interpretation of Art. 22(1), the data controller shall have the burden of proof because Art. 22(1) is a prohibition, not an exercisable right. This is also suggested by the WP29 Guidelines which advocate for the controller to identify and record any degree of human involvent in a given decision-making process. [115] Consequently, businesses that take advantage of certain smart contracts can incur an obligation that their actions with respect to the execution of the smart contract had the required effect of 'meaningful' human intervention. A 'meaningful' on-chain influence can be a change in

[113] WP29 Guidelines on Automated Decision-Making (n 55) 21.
[114] ibid.
[115] WP29 Guidelines on Automated Decision-Making (n 55) 21.

ledger data that occurred via the consensus of the blockchain protocol. Alternatively, a written notice which is added on a subsequent block to correct previous incorrect data could also suffice. This raises the issue of controller identity again because the data controller must execute a meaningful influence.

Consequently, the analysis shows that a smart contract can be considered a solely automated decision under Art. 22(1). This is because the execution of a smart contract is a coded execution of a transaction under most circumstances. It is also difficult to have a meaningful effect on on-chain transactional data because of the nature of blockchain. However, a smart contract must still be capable of producing legal or similarly significant effects on the data subject.

5.4 Can Smart Contracts Produce Legal Effects?

Article 22(1) only applies to data subjects when they are being subjected to decisions based on automated processing that confer legal effects on them, or similarly significantly affect them. Art. 22(1) defines none of these terms.

The WP29 Guidelines on Automated Decision-Making defines 'legal effect' as a change in the legal rights or obligations, legal status or rights of the data subject under a contract.' Accordingly, if a smart contract is executed between mutually distrusting parties, the decision must have an effect on the legal rights and status of the parties. For example, in a smart contract for the sale of goods, a title to a product is exchanged in return for digital payment. There can also be smart contracts that do not produce any legal effect on the data subjects, such as blockchain applications in machine-to-machine payments.[116]

If right of ownership or similar interests are not transferred during the execution of a smart contract, there may still be a 'similarly significant' effect on the data subject. A 'similarly significant effect' is generated when the consequences of the decision are 'sufficiently great or important to be worthy of attention',[117] which includes having a permanent or prolonged

[116] DXC Labs, 'Machines that pay each other using digital wallets'< https://blogs.dxc.technology/2019/01/29/machines-that-pay-each-other-using-digital-wallets/> accessed 16 May 2019.
[117] WP29 Guidelines on Automated Decision-Making (n 55) 21.

impact on a data subject, as well as an effect on the circumstances or behaviour of a natural person.[118]

This ambiguous wording is of little assistance. For example, the passcode to a building which is provided by an on-chain access ledger can be trivial to one, but important to another individual. Therefore, an objective analysis should be completed on a case-by-case basis, because a subjective test would be an unreasonably heavy burden.[119] Furthermore, neither the GDPR, nor the WP29 Guidelines impose a minimal threshold test. A very wide interpretation of Art. 22(1) would therefore include even the most 'trivial' appearing if/then situations where legal consequences have occurred on the data subject. An example is the use of a vending machine, which a reasonable person would call trivial compared to a credit decision or a recruiting decision, as listed in Recital 71.[120] It can be argued that under most circumstances of smart contracts, a legal effect or a similarly significant effect will be executed on the data subject, because smart contracts are usually used to confer licenses, fines or title to goods to natural persons.

What sort of data is required to produce 'legal' or 'similarly significant' effects on the data subject? It is unclear whether personal data must be included in the input values of a smart contract, or whether the execution of the code regarding the data subject suffices itself,[121] because Art. 22(1) only mentions decisions applying to the data subject. The obvious solution is that personal data, which has been used as the input values of a smart contract, render the execution applicable under Art. 22(1). However, it is possible that regardless of whether or not the input values for the digital code include personal data, Art 22(1) may apply by virtue of the fact that the decision, or measure for that matter, is taken in relation to a data subject. The broad interpretation should be chosen in order to follow the general purpose of the provision, which is to protect the data subject's rights and legitimate interests.

Based on the previous analysis, smart contracts can come under the scope of Art. 22(1) at least under circumstances where there is no human intervention involved. A coded execution of a smart contract fits into the purposive interpretation of Art. 22 and the GDPR as a whole.

[118] ibid.
[119] Michèle Finck, 'Smart Contracts as a Form of Solely Automated Data Processing under the GDPR' (2019) Max Planck Institute for Innovation and Competition Research Paper No. 19-01, 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370> accessed 11 June 2019.
[120] Recital 71 GDPR.
[121] Finck (n 119) 11.

Accordingly, the data subject has the right not to be subjected to executions of smart contracts under certain circumstances. The 'right' acts as a prohibition on the data controller. However, there are exceptions which allow solely automated processing under Art. 22(2) and they will be discussed in the paragraphs below.

5.5 Exceptions to the Qualified Prohibition

There are three different situations where automated processing is lawful and allowed under Art. 22(2) of the GDPR. They apply where the automated data processing:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c) is based on the data subject's explicit consent.[122]

5.5.1 Necessity for the Performance of a Contract

Article 22(2)(a) allows automated decision-making where it is required in order to enter into a contract. Accordingly, smart contracts have the most potential to be used as an automated method of legal contracting, and if an undertaking chooses to use smart contracts, this exception can be relied upon.

The exception is subject to contractual obligations being executed between the controller and the data subject.[123] With respect to business ventures that use private blockchains, this exception shall not provide complications. A bank that utilizes the if/then code to execute the direct debit of a client's payment is party to the contract and processes the client's personal data on the respective nodes.

Art. 22(2)(a) neither gives a definition to the word *necessary,* nor does it state a *de minimis* threshold test for its application. The question as to what is '*necessary* for entering into, or

[122] Art. 22(2) GDPR.
[123] Art. 22(2)(a) GDPR.

performance of, a contract between the data subject and a data controller' is unclear.[124] It can be argued that a smart contract can only be used when no other alternative human methods are available to successfully execute the contract. This seems unlikely because Recital 71 gives examples such as a credit score and automated recruiting as appropriate circumstances. These decisions do not set a high threshold and can arguably be performed without automated decision-making.[125] On the other hand, the WP29 Guidelines on Automated Decision-Making state that if 'other effective and less intrusive means to achieve the same goal exist' then automation is unnecessary.[126] It is also stated in the WP29 Guidelines that automated decision-making can be necessary when the volume of the workload is exceptionally high and renders a job burdensome. In this case the data controller has to show that the chosen method of processing is necessary, 'taking into account whether a less privacy-intrusive method could be adopted.'[127] This means that if blockchain based smart contracting is the more efficient method than a traditional central data silo based solution, the controller must give evidence for this when it chooses to avoid other more traditional methods.

Issues arise on permissionless blockchains which can be accessed by any number of peers. This is because a permissionless system makes it difficult to assess which node, or which party is considered the data controller. For the purposes of this sub-section, it is important to note that the controller could be one or more nodes, the data subject itself or a combination of the infrastructural parties and nodes. The French Data Protection Authority has suggested it can even be the developer of the smart contract.[128] Whatever the solution, a contractual relationship must exist between the two parties for the purposes of this exception. Therefore, undertakings that use smart contracts are advised to clearly state who the the contracting parties are in an informative manner, and how are they represented on blockchain for the successful enforcement of Art. 22(2)(a).

[124] ibid.
[125] Recital 71 GDPR.
[126] WP29 Guidelines on Automated Decision-Making (n 55), 23.
[127] ibid.
[128] https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.

5.5.2 Authorisation by EU or Member State Legislation

Art. 22(2)(b) of the GDPR authorises Member States or the Union to create laws that explicitly allow automated processing, on the condition that certain safeguards are implemented to enforce the data subject's interests. So far, there is no specific Member State or EU legislation on blockchain, or DLT for that matter. However, the European Blockchain Partnership has engaged in active measures to ensure EU Member States collaborate on the establishment of a functioning legal framework for blockchain.[129] It is clear that blockchain-specific legislation will be implemented in the near future as Mariya Gabriel, Commissioner for Digital Economy and Society stated that all public services will use blockchain in the future.[130]

5.5.3 Explicit Consent of the Data Subject

Automated data processing is also allowed if it is based on the explicit consent of the data subject.[131] The GDPR lacks a definition for 'explicit'.

The Article 29 Working Party Guidelines on Consent read that explicit consent is required under circumstances where there are serious data protection risks, i.e., where high level of individual control over personal data is required.[132] Under these circumstances, the data subject must provide an express statement of consent, for example in a written statement.[133] This can be easily implemented on blockchain by virtue of an electronic signature.

A significant issue arises for the controller if the data subject revokes the on-chain consent, because on-chain data cannot be deleted, except under extreme circumstances.[134] It should be noted that the data subject has the right to revoke consent for data processing at any given moment. Even though the right to revoke consent does not affect the lawfulness of the pre-

[129] European Commission, 'European Countries Join Blockchain Partnership' https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership accessed 11 June 2019.
[130] ibid.
[131] Art. 22(2)(c) GDPR.
[132] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (2018) WP259, 18, hereinafter 'WP29 Guidelines on Consent'.
[133] ibid.
[134] Art. 7(3) GDPR.

existing processing, a major issue will be deleting the on-chain personal data after consent has been revoked.

5.5.4 Interim Conclusion

The analysis above shows that there are ways to lawfully execute smart contracts under the GDPR. However, they must be executed on the condition of complying with other data subject rights, such as the right to revoke consent, or authorised by EU Member State law. In the event of Art. 22(a) or (c), the controller must enable certain safeguards to enforce the legitimate interests and rights of the data subject. These include the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.[135]

5.6 Human Intervention

Art. 22(3) says that when automated data processing is executed under Art. 22(2)(a) or (c), the data controller must implement suitable measures to 'safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision'.[136] Accordingly, the data subject must exercise the right to obtain human intervention, compared to being protected under a general prohibition under Art. 22(1).

5.6.1 What is Human Intervention?

Under the WP29 Guidelines on Automated Decision-Making, human intervention is form of *ex post* factual evaluation conducted by someone with 'appropriate authority and capability to change the decision'.[137] The evaluation must consider all the relevant data, and additional information that has been provided by the data subject.[138] On blockchain, this refers to the transactional data and on-chain public keys, as well the descriptive information the data subject can give to the data controller with respect to the transaction, i.e., what the transaction was for, or when it took place.

[135] Art. 22(3) GDPR.
[136] ibid.
[137] WP29 Guidelines on Automated Decision-Making (n 55) 27.
[138] ibid.

Because smart contracts are simple 'if x, then y' events, a review mechanism should be easy to implement on blockchain, but it must be noted that smart contracts can also be coded to prevent the ex-post review of transactional data by default, depending on the nature of a given blockchain.[139] The WP29 Guidelines suggest that an *ex post* review is sufficient, and that a mechanism that intercepts the smart contract is not necessary under law.

Under Art. 22(3), human intervention must be provided by the controller. It is unclear who the controller is on blockchain. On a private permissioned blockchain, undertakings can designate a specific actor, or a governing body to act as the controller, but this is not equally simple on a public permissionless blockchain because of the large number of on-chain actors and public accessibility of data. An argument can be made that the data subject can engage the human intervention itself by accessing the on-chain data with the correct private key. This enables the data subject to review the decision independently, but it does not necessarily ensure that the accessible information is clear or understandable to a data subject under the safeguard framework of the GDPR.

5.6.2 Right to Obtain Information on Measures taken Under Art. 22

Under Art. 12(1), the controller shall take appropriate measures to provide information regarding decisions based on solely automated data processing to the data subject. This information must be provided in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'.[140] This provision is closely tied to Art.13(2)(f), under which the data subject is entitled to know about the existence of automated decision-making referred to in Art. 22(1) and (4). This includes providing the data subject 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.[141] Furthermore, Art. 14(2)(g) contains the same obligation under situations where personal data was not directly obtained from the data subject. Similar wording is also used in Art. 15(1)(h) GDPR.[142]

[139] Finck (n 119) 17.
[140] Art. 12(1) GDPR.
[141] Art. 13(2)(f) GDPR.
[142] Art. 15(1)(h) GDPR 'the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.

All of the aforementioned provisions require the data controller to provide information on the following characteristics: (1) the existence of a decision; (2) information about the logic involved in the decision; and (3) significance and the envisaged consequences of the decision. Recital 71 clarifies this by referring to 'suitable safeguards' which must provide 'an explanation of the decision reached after such an assessment and to challenge the decision'.[143] Hence, an issue of interpretation arises because Recital 71 is more in-depth than Art. 12(1). This suggests that the controller must explain the reasoning of an executed smart contract to the data subject. As established earlier, Recitals cannot be used as individually binding legal acts, or to change the meaning of the legislation itself.[144] Thus, the Recital can only provide interpretative guidance as to how a decision should be explained to a data subject. In order to avoid infringing upon this right, undertakings should make sure that the data subject has a clear understanding of the decision and why it was taken. Whether this requires the controller to open up the so-called 'black box' algorithm of a smart contract is a matter of debate. For the general purpose of GDPR, this may be reasonable under circumstances where the revealing of the algorithm does not infringe upon an undertaking's right to protect trade secrets or other IP rights. Essentially, a case-by-case balancing act may be required.

There is academic disagreement as to the practical implications of information and explanation. Wachter et al suggest that a right to explanation of the automated decision-making does not exist in the GDPR, and that Art. 12(1) is an *ex ante* right which only clarifies the existence of such processing to the data subject. Thus, there is no *ex post* right to be informed of the reasoning of a decision.[145] On the other hand, Commandè and Malgieri suggest that Arts. 13-15 can be used to explain algorithms of automated decision-making.[146] This interpretation suggests that even though undertakings have the right to protect trade secrets and algorithmic data, the law should favor protecting the data subject's rights and legitimate interests.

[143] Recital 71 GDPR.
[144] See Chapter 3.5.1. Interpreting the GDPR.
[145] Wachter et al, 'Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76. <https://academic.oup.com/idpl/article/7/2/76/3860948> accessed 11 June 2019.
[146] Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243 < https://doi.org/10.1093/idpl/ipx019> accessed 11 June 2019.

The bottom-line is that the CJEU must decide how to interpret this with respect to smart contracts. This thesis argues that the data subjects should have an *ex ante* right that explains the use of algorithms and an *ex post* right to obtain human intervention that reviews the result of the decision, auditing for the existence of algorithmic bias. This ensures that data subjects have a remedy in situations where a digital execution may have discriminated upon the data subject, or otherwise infringed upon his or her legitimate interests.

WP29 Guidelines on Automated Decision-Making support this view. Accordingly, the data controller must (1) inform the data subject that automated decision-making is being conducted, (2) give meaningful information with respect to the logic of the decision, and (3) explain the significance and envisaged consequences of the processing.[147] Meaningful information refers to numerous categories of information: (1) the categories of data that have been or will be used in the profiling or decision-making process; (2) why these categories are considered pertinent; (3) how any profile used in the automated decision-making process is built, including any statistics used in the analysis; (4) why this profile is relevant to the automated decision-making process; and (5) how it is used for a decision concerning the data subject.[148] In order to clarify the algorithmic transparency, the controller can consider visual aids.[149] This supports the argument that Article 29 Working Party considers it necessary that data subjects be informed of the algorithmic basis of automated decisions.

5.6.3 Right to Explanation with Respect to Smart Contracts

The WP29 Guidelines on Automated Decision-Making state that the controller must use simply measures to tell the data subject about the rationale behind a decision, or what criteria was relied upon.[150] This does not equate to a complex explanation of the algorithms, or disclosing them to the data subject for that matter.[151] Most smart contracts are simple to explain because they include few variables that change on the basis of the parties' actions. In fact, if a smart contract decides to reject a driver's license application, the rationale can be explained to the data subject using the applied data of *x* and *y*. The same example applies in the situation of a speeding fine issued on the basis of speed camera evidence. Smart contracts

[147] WP29 Guidelines on Automated Decision-Making (n 55) 25.
[148] ibid. 31.
[149] ibid.
[150] ibid.
[151] ibid.

typically do not include a vast amount of data, which may change if complicated nexus smart contracts are used.[152] Compliance under Art.22(3) will only prove difficult where the controller must be identified, which seems to be the recurring problem with respect to all data subject rights that are enforced on a blockchain.

5.7 Interim Conclusion

The previous analysis shows that smart contracts will come under Art. 22(1) in most circumstances where the execution of the decision lacks human intervention. Art. 22(1) lays down a general prohibition for automated data processing, whereas Art. 22(2) gives exceptions under which automated data processing is allowed. Under the exceptions, the data subject has the right to obtain human intervention on the part of the controller and contest the decision according to Art. 22(3). This means that the controller must explain the logic and parameters of the decision, the envisaged consequences and review the decision. It must be noted that the data subject can also choose to not obtain human intervention with respect to the decision.

The major issue is compliance of smart contracts in the blockchain context. Human intervention cannot be claimed by the data subject if a controller cannot be identified on a public permissionless blockchain. Even if human intervention can be claimed, the on-chain transactional data cannot be changed. Until the issue of the controller is clarified by the CJEU, undertakings and other service providers should store the transactional data of smart contracts, either on private permissioned blockchains or off-chain data storages in order to avoid infringing data subject rights.

[152] A nexus smart contract is an autonomous and algorithmic system which functions on the basis of software algorithms that control assets and resources. De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018) 146.

6 Division of Data Controller's Responsibilities

6.1 The Data Controller

Under Art. 4(7) GDPR, the controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. If EU or Member State law defines explicitly what the purposes and means of processing are, the controller shall be determined according to that law. A controller determines who is responsible for the compliance with data protection laws and how the data subjects can enforce their rights.[153] The CJEU has ruled that this provision shall be interpreted broadly in order to ensure the effective and full protection of data subjects' rights and interests.[154] Accordingly, even an administrator of a Facebook page takes part in determining the purposes and means of processing the personal data of visitors, because the administrator can determine the target audience of the Facebook page.[155] On the other hand, the processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[156]

A controller is referred to as a single entity in Art. 4(7), which reveals that the GDPR was primarily drafted for centralized data filing systems that have a sole identifiable controller under most circumstances. However, Art. 4(7) also acknowledges the possibility of joint controllers. Where the multiple controllers are facilitating the data processing to a different degree, the controllers shall have unequal liability in practice.[157] When two or more nodes jointly determine the purposes and means of data processing, they qualify as joint controllers under Art. 26. These joint controllers can be involved in the processing at different stages and degrees.

The complexity of applying the concept of controller and processor is explicitly acknowledged by the WP29 Guidelines on the Controller, specifically because of modern

[153] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010) 6 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf> (hereinafter: WP29 Guidelines on the Controller) accessed 24 May 2019.
[154] C-210/6 *Wirtschaftsakademie Schleswig Holstein* [2018] EU:C:2018:388.
[155] ibid, para 39.
[156] Art. 4(8) GDPR.
[157] CJEU (n 154) para. 43.

technological advancements and use of global data management.[158] Because the controller is primarily identified as a functional actor, it must be designated using a factual, rather than a formal analysis.[159] This means that the controller is the entity that 'determines' rather than 'lawfully determines' the means and purposes for the data processing.[160]

It has been established that the central issue with respect to enforcing data subject rights on blockchain is the lack of certainty with respect to the identity of the controller. In an application of a DLT system, more than one network actor can be in the position of the data controller for the purposes of the GDPR. Issues arise especially on public permissionless blockchains, which can be accessed and utilized by an unlimited number of peers by virtue of the financially incentivized consensus mechanism. If an individual actor, or a group of actors are allocated the obligations of the controller, they will be held liable under certain circumstances. However, this liability is difficult to enforce if the actors cannot be contacted, cease to exist or move between different jurisdictions. On-chain personal data of permissionless public blockchains can be located anywhere around the world, which severely complicates the enforcement of the GDPR administrative fines and, more importantly, data subject rights.

The aim of this chapter is to examine which party on a blockchain determines the means and purposes of the processing, i.e., the 'why' and 'how' of the processing.[161] The 'purpose' refers to the outcome of the processing, whereas 'means' refers to how the outcome is obtained.[162] 'Means' includes within it technical and organizational aspects, as well as elements related to the inherent nature of the controller, e.g., the scope of data which is processed and for how long it is processed. Whereas determining the 'purpose' of processing qualifies a party as the controller, determining the 'means' will only do so if the determination relates to the 'essential elements' of the processing.[163]

[158] WP29 Guidelines on the Controller (n 153) 2.
[159] ibid. 9
[160] ibid.
[161] ibid. 13.
[162] ibid.
[163] ibid. 14.

6.2 Designating the Controller on a Public Permissionless Blockchain

The public permissionless blockchain consists of full and lightweight nodes. A lightweight node contains a limited version of the blockchain data and mainly serves to validate the transactions stored on full nodes that contain the entire blockchain ledger and download new data according to the current protocol consensus.[164] Miners organise on-chain transactional data onto blocks for an independent financial gain.[165] They run a special version of a full node and use computer processing power to solve cryptographic puzzles, hence the term 'proof-of-work'.[166] This cooperation of mining and and building is called the 'blockchain protocol'. The parties that must be examined as potential controllers on a public permissionless blockchain are (1) the two versions of a node, (2) a miner, (3) a developer and (4) a network user.[167] The controller's obligations shall be examined in relation to Bitcoin transactions for ease of explanation.[168]

It should be noted that Bitcoin is a public permissionless blockchain, hence the following analysis does not apply on a permissioned private blockchain where undertakings and consortiums can designate a clear governing body for the actors that operate as controllers and processors. Moreover, the financial incentive mechanism of mining does not exist on a private permissioned blockchain because the members and their roles are designated by a central authority. On a private permissioned blockchain, the nodes are most likely data processors that have contracted with the governing body to facilitate data processing. This means that the governing body is the data controller, or joint controller where it exercises a certain influence over the means and purposes of the data processing.[169]

[164] Bitcoinwiki, 'Full Node'< https://en.bitcoin.it/wiki/Lightweight_node> accessed 24 May 2019.
[165] Satoshi Nakamoto (n 6); The current reward for a block is 12,5 BTC < http://www.bitcoinblockhalf.com/> accessed 24 May 2019.
[166] ibid.
[167] Mario Martini and Quirin Weinzierl, 'Die Blockchain-Technologie und das Recht auf Vergessenwerden sind Antagonisten' (2017) Neue Zeitschrift für Verwaltungsrecht, 1251.
[168] A transfer of cryptocurrency is arguably one of the simplest transactions that can take place on a blockchain.
[169] Natalie Eichler; Silvan Jongerius; Greg McMullen; Oliver Naegele; Liz Steiniger; Kai Wagner, 'Blockchain, data protection, and the GDPR' (2018) Blockchain Bundesverband, VR 36105 B https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf accessed 18 June 2019.

6.2.1 Nodes

The lightweight node in Bitcoin can transfer BTC to the user's own address or to the address of someone else. The GDPR obligations cannot arise in the former case where data processing is solely concerned with transfers related to the user itseld. This is because of the GDPR's purpose itself, which is to give data subjects control over their personal data that is processed by undertakings. For example, the right to information is useless where the data subject has control of the information being processed.[170]

The purpose of this particular type of data processing is the transfer of cryptocurrency, and it cannot be changed by a single user. In addition, the independent node cannot influence how long data will be stored on-chain, who has access to the data, or when it will be deleted from the blockchain.[171] This is because of the append-only nature of blockchain. Therefore, categorising the lightweight user as a controller would be an unreasonably wide interpretation for the purposes of Art. 4(7). A single lightweight node is not a controller on a public permissionless blockchain.

Full nodes complete much of the same tasks as lightweight nodes but contain a complete copy of the ledger. These actors check the validity of transactions signed with private keys in accordance with the current protocol. The household exception also does not apply here because the actions related to transactions are delivered to the public at large, and clearly surpass an intensity for household activities. Even though the contributions of full nodes are essential to the functioning of the network, a full node cannot determine the means or purposes of the data processing because the blockchain protocol requires fully consensual actions in order to be changed. Therefore, similarly to lightweight nodes, full nodes cannot be considered controllers alone on a public permissionless blockchain.

Nodes participate in the public blockchain network either for a financial incentive, or in order to support the network. Their actions are independent of third parties. Moreover, they do not determine the means and purposes of data processing. On the contrary, some argue that by downloading the data and choosing certain software/hardware combinations, the nodes

[170] Art. 12(1) GDPR.
[171] Thomas Buocz et al., 'Bitcoin and the GDPR: Allocating responsibility in distributed networks' (2019) Computer Law & Security Review 35, 182-198, 194, <https://www.sciencedirect.com/science/article/pii/S0267364918303170> accessed 24 May 2019.

determine the means and purposes of data processing *de facto*. This argument must be examined by the courts. However, if a node were to be categorised as the controller, enforcing the data subject rights would face significant complications, because a node exercises its free will to participate in the network. It is very difficult to contact a node and oblige it to perform certain tasks with respect to on-chain personal data which is encrypted. However, this can be an entirely different case on a private permissioned blockchain which nodes can be designated as specific governing actors by the particular undertaking.

6.2.2 Miners

A miner on a blockchain uses full nodes to contribute to the functioning of the blockchain by storing transactions into blocks and validating them using the proof-of-work method. The miners do not participate in facilitating the end goal of the transactions.[172] Similarly to the previous actors, miners also fall outside of the household exception because their actions are public and they have a financial incentive to participate in the facilitation of the chain. Although the mining of blocks is essential to the blockchain, miners cannot determine any part of the purposes or means of processing either. Therefore, an independent miner cannot be categorised as a controller on a public permissionless blockchain.

6.2.3 Developers

The overriding code of a blockchain determines how nodes validate transactions and how new blocks can be created. This concept is called the 'governing infrastructure'.[173] The most famous blockchain platforms are Bitcoin and Ethereum and those are open source projects.[174] The community of Bitcoin Core users is constantly communicating and adapting changes to the digital environment. The more active and long-term a contributor is, the more trust he/she gains in the community.[175] For example, Satoshi Nakamoto coded the original version of

[172] Commission Nationale Informatique & Libertés (CNIL), 'Blockchain – Solutions for a responsible use of the blockchain in the context of personal data' (2018) < https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> accessed 30 July 2019.
[173] Tina Ehrke-Rabel, Iris Eisenberger et al., 'Bitcoin-Miner als Prosumer: Eine Frage staatlicher Regulierung? Dargestellt am Beispiel das Glücksspielrechts' (2017) Austrian Legal Journal 188-219 < https://alj.uni-graz.at/index.php/alj/article/download/116/181/> accessed 15 June 2019.
[174] Bitcoin.org, 'Bitcoin Core' https://bitcoin.org/en/bitcoin-core/ ; Ethereum, < https://www.ethereum.org/> accessed 25 May 2019.
[175] ibid.

Bitcoin, whereas Gavin Andresen rendered the platform open-source.[176] Even though a group of highly-skilled contributors have a say in the eventual functioning of the protocol, their suggestions do not transfer to absolute rules of the processing. Accordingly, Bitcoin Core does not decide the means and purposes of the data processing, because it should be thought of as a proposal of rules,[177] rather than a fully-fledged implementation on the platform. Additionally, holding the developer accountable for the duties of the data controller is unfeasible in practice.

6.2.4 Network User

The network user that encrypts or hashes data onto the blockchain can be considered a controller on a blockchain. If the network user gives one or more nodes the permission to process a data subject's personal data, the nodes qualify as on-chain processors and the user arguably determines the means and purposes of the data processing by storing the data on-chain.[178] In this case, the network user has the capability to control the personal data over the private key which grants him or her the access to the blockchain. Therefore, under certain circumstances the network user implicitly accepts the obligations to protect and enforce data subject rights on a public permissionless blockchain.

The network user could be exempt from the application of the GDPR if his/her actions of buying and selling cryptocurrency come under the household exception in Art. 2(2)(c).[179] However, if the transactions and storage of data are carried out in the course of commercial or professional business, the household exemption does not apply and there is a possibility to interpret the network user as a data controller. This happens when a notary, i.e., the network user, stores the details of his or her clients property deeds on a public permissionless blockchain, or when a service provider executes a smart contract that stores data on blockchain.

[176] Primavera De Filippi and Benjamin Loveluck, 'The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure' (2016) 5(4) Internet Policy Review 1, 9 https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure accessed 17 June 2019.
[177] Buocz et al. (n 171) 196.
[178] Lukas Feiler (n 40) 63.
[179] Commission Nationale Informatique & Libertés, 'Blockchain: Solutions for a responsible use of the blockchain in the context of personal data' (2018) https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf accessed 28 May 2019.

6.2.5 Cooperation Between Nodes and Miners

The analysis shows that individual network actors cannot be categorised as controllers on a public permissionless blockchains, because they cannot determine the means and purposes of data processing. However, there are specific circumstances under which the rules of the blockchain protocol can change. These circumstances are referred to as system forks. A hard fork creates a new version of the blockchain and renders the old version incompatible with the new one, whereas a soft fork restricts or changes the existing rules of the protocol.

The parties that have the power to fork a certain blockchain have the competence to determine the means and purposes of data processing.[180] Accordingly, the successful execution of a soft fork requires that a large number of users are in charge of full nodes and miners under a common consensus. Full nodes validate new rules and miners create blocks that register them.[181] The combination of the two categories of actors is essential, because if miners upgrade blocks to the new rules, and nodes do not validate corresponding transactions for the blocks, the new blocks serve no purpose. Similarly, if nodes begin to validate new rules for transactions but there are no new blocks created by miners, no rules can be changed.[182] Consequently, for change to occur in the means and purposes of on-chain data processing, the consensual cooperation of the collective is an essential requirement.

6.2.6 Implications for the Controller

Examining all individual actors on a permissionless blockchain has shown that individual users who are in charge of nodes and mining cannot determine the on-chain means and purposes of data processing. Even though the protocol can be influenced by a group of skilled developers, only a collective of full nodes and miners can adopt real changes under a common consensus. Accordingly, a collective of actors on the infrastructural level is in charge of determining the means and purposes of data processing on a public permissionless blockchain. The collective can be a controller under Art. 4(7), or the actors within the collective constitute joint controllers under Art. 26.

[180] Jeffery Atik and George Gerro, 'Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice' (2018) 1(1) Stanford Journal of Blockchain Law & Policy https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203893 accessed 25 May 2019.
[181] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 accessed 25 May 2019.
[182] Buocz et al. (n 170) 196.

Under Art. 26(1) GDPR two or more controllers that jointly determine the purposes and means of processing are considered joint controllers.[183] Article 26 paras. 1 and 2 GDPR require the multiple data controllers to transparently determine their respective responsibilities under the GDPR, especially with respect to Articles 13 and 14 of the GDPR.[184] This information should also be made 'available to the data subject.'[185] According to Recital 79 of the GDPR, the aim of Article 26 is to allocate the responsibilities of joint controllers in a clear manner in order to protect data subject rights.[186]

It has been suggested that the provision requires *ex ante* clear and transparent allocation of responsibility between the nodes.[187] This makes it impossible to apply the provision on a public permissionless blockchain, because the network actors act independently and without clear reachable identities. However, examination of Art. 26 reveals that a 'clear and transparent allocation of responsibility' may not be a condition, but rather an obligation. The joint controllers must determine their respective responsibilities *'in a transparent manner'*.[188] If this was a condition, joint controllers could circumvent their liability by establishing simple non-transparent structures as placeholders on a blockchain. Instead, the controllers on a public permissionless blockchain are in constant motion and operate via the consensus mechanism. The identities and actions of individual actors change with time as users enter and exit the chain. As a result, proving that a certain node or miner was active during a specific timeframe and violated data subject rights is burdensome, but not impossible by default.[189]

The semantic value must be clarified by the courts, but it could be argued that the Commission included Art. 26 in the regulation in order to provide an objective basis for different data systems. This way the GDPR can be transposed to a variety of different platforms where multiple actors have an influence on the means and purposes of data processing. Thus, requiring them to form an explicit arrangement *de facto*.

[183] GDPR Art. 26(1).
[184] GDPR Art. 26(1)-(2).
[185] ibid.
[186] GDPR Recital 79.
[187] Finck (n 3) 26.
[188] Art. 26(1) GDPR (emphasis added).
[189] See Chapter 2.

6.2.7 Issues of Enforcement

If the collective constitutes the controller, several issues arise by virtue of blockchain being a decentralised platform. Firstly, the amount of actors that supposedly possess controller's obligations is larger than in regular centralised data systems. This makes enforcing the GDPR rules on a blockchain system burdensome. Furthermore, it is difficult to identify a controller and raise a claim for data subject rights, because the nodes cannot identify each other, and even if they could, the correspondence between network users would happen on a virtual and remote basis. Therefore, any scope of shared responsibility between the parties exists without clear representation of the collective.[190]

If the infrastructural actors of the collective are joint controllers under Art. 26, the same issues apply. In both situations, a controller must take responsibility for ensuring compliance of the blockchain, which means implementing 'appropriate technical and organisational measures to ensure […] that processing is performed in accordance with the GDPR'.[191] It is impossible to force the collective of independent actors to perform certain tasks because they are able to shut down their operations on the network at any moment.

The GDPR allows the processing of personal data when it is based on a legal ground listed in Art. 6(1). Accordingly, the data processing on blockchain can be based on consent,[192] necessity for performance[193] or the legitimate interest of the controller.[194] Furthermore, the controller must ensure that the data subject rights are protected.[195] At first glance, enforcing the right to access will not create large issues vis-à-vis public permissionless blockchains because the ledgers are public. This means that any user can join the chain as a node and obtain a copy of the ledger. However, the right to access is subject to the condition that a high level of organisational transparency can be ensured on a blockchain. Permissionless blockchains do not offer such transparency, and it is unclear whom the data subject must contact in order to make a claim. Moreover, the right to rectification seems impossible to enforce due to the default immutable nature of the ledger.

[190] Tina Ehrke-Rabel (n 173) 217.
[191] Art. 24(1) GDPR.
[192] Art. 6(1)(a) GDPR.
[193] Art. 6(1)(b) GDPR.
[194] Art. 6(1)(f) GDPR.
[195] These include Art. 15 right to access, Art. 13 right to information, Art. 16 right to rectification and Art. 17 right to erasure.

In the event of an infringement of data subject rights, a significant number of controllers, i.e., nodes, may have to be contacted, whereas only one party has to be contacted on centralized databases. Under extreme circumstances this can lead to the complete shutdown of an entire blockchain if the data subjects cannot claim their rights through other means.[196] It is also unclear how fines would be calculated against the provider of a permissionless blockchain, given that Art. 83 GDPR calculates them by evaluating the annual worldwide turnover of an undertaking.[197] If a node or a miner is interpreted as the undertaking on a public permissionless blockchain, it is immediately unrealistic to expect a node to pay such high fines for breaching data subject rights, not to mention enforcing the fines against an actor.

6.2.8 Extraterritorial Claims Against a Controller

Public permissionless blockchains are likely to run on nodes, which are located even outside of EU/EEA territory. Blockchains are transnational data stores by nature, which creates jurisdictional issues with respect to enforcing data subject rights.

The GDPR's territorial scope applies to the 'processing of personal data in the context of the activities of an establishment of a controller of a processor in the EU, regardless of whether the processing takes place in the Union or not.[198] This provision was drafted in order to prevent jurisdictional shopping by undertakings, i.e., seeking for a territory with the weakest data protection requirements in national legislation. This is why the GDPR also applies if the controller or processor is located outside of EU/EEA territory but the processing activities relate to the sale of goods and services to a data subject based in EU/EEA territory.[199] Consequently, many blockchains will be bound under GDPR due to an indirect link to the EU.

An issue arises especially where on-chain data is engaged in cross-border data processing. Under the GDPR, third country data transfers can only occur under a number of conditions stated under Arts. 44-50. For example, the miner who hashes the data onto blocks can be based outside of EU/EEA territory. The blockchain is updated subsequently on all nodes

[196] Finck (n 3) 27.
[197] GDPR Art. 83.
[198] Art. 3(1) GDPR.
[199] Art. 3(2) GDPR.

around the world. This can lawfully happen if the Commission declares the third country as one that provides an adequate level of protection, and where the controller and processor provide appropriate safeguards and remedies for the data subjects.[200] Enforcing this on a blockchain is difficult because more data is stored on blockchain constantly according to the independent actions of the infrastructural parties, i.e., regulating the flow of on-chain data is difficult due to the nature of the system. New network users can obtain a copy of the ledger in any jurisdiction where they set up as a peer.

Undertakings that wish to use blockchain technology should opt to obtain the data subject's explicit consent for third-country data transfers under Art. 49(1)(a) after having been informed of the risks of the data transfer. This can be difficult to transpose onto public permissionless blockchains that are out of the control of a centralised party by default. However, on a private permissioned blockchain this is simple to implement because of the limited amount of network actors and the possibility to regulate a governing on-chain body. A consortium of companies can regulate in which jurisdictions they choose to set up nodes and other infrastructural parties on a private permissioned blockchain.

The solution for undertakings is to only implement private blockchains and designate the relevant parties clearly in a data protection notice. As such, the implementation of public permissionless blockchains is not advisable, because it is extremely difficult to designate a clear hierarchy of controllers that fulfil their respective obligations.

6.3 Interim Conclusion

The data controller is highly important for the purposes of the GDPR, because it is responsible for enforcing and protecting data subjects' rights and legitimate interests. Its identity is one of the most unclear, but important issues with respect to blockchain. Blockchain technology is append-only, censorship resistant and distributed by nature, which means the GDPR is difficult to transpose onto blockchain. The GDPR was drafted for centralised data systems that contain one or more clearly identifiable controllers, whereas blockchain's central premise is to eliminate central validating parties that govern transactions

[200] Art. 45(1) GDPR.

between mutually distrusting parties. This is why the controller is especially difficult to identify amongst the large numbers of network users on a public permissionless blockchain.

The analysis above shows that the controller on a public permissionless blockchain can be the infrastructural collective, represented as a single body under Art. 4(7). Alternatively, the network users of the collective are joint controllers under Art. 26. Until these solutions are examined by the CJEU, undertakings face significant risk in infringing data subject rights. Whichever solution is proven to be correct, similar issues exist regardless, e.g., it is difficult to contact a network user to make a data subject request and it is difficult to obtain remedies where personal data has been processed wrongfully.

The easiest solution to this issue is to avoid blockchain technology altogether. However, if it is chosen, personal data should be stored on a private permissioned blockchain, where the undertaking can designate specific roles for actors that facilitate the chain. Accordingly, third country data transfers can be avoided, a controller and a point of contact for data subject requests can be designated and data subject infringements can be minimised. Moreover, private permissioned blockchains should be used in cooperation with off-chain data silos so that data subject rights, such as the right to erasure and the right to be forgotten are easier to enforce. Above all, undertakings must consider implementing solutions on the issue of controller from the ground-up. This is why privacy by design under Art. 25 of the GDPR must be examined as a final point in this thesis.

7 Designing a Compliant Blockchain

7.1 Data Protection by Design and Default

Under Art. 25(1) GDPR, data subject rights must be protected by establishing technical and organizational measures 'both at the time of the determination of the means for processing and at the time of the processing itself'.[201] The 'state of the art, the cost of the implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing' should be taken into account.[202]

The data controller must ensure that blockchain-based smart contracts are implemented via *ex ante* and *ex post* measures that enable it to enforce data subject rights and interests consistently throughout the data processing. However, Art. 25(1) is difficult to transpose onto blockchains, because the identity of the controller is not clear. As established previously, a full consensus of network actors is required to change existing on-chain rules and procedures. A better solution is that the European data protection authorities and community developers cooperate in creating use-cases that achieve compliance under the GDPR. Hence why, the certification method of Art. 25(3) is especially attractive under these circumstances. Alongside Art. 42, the certification method can be used to demonstrate that a certain information platform is compliant under EU legislation. Certification is not mandatory, but is used to 'enhance transparency' that allows 'data subjects to quickly assess the level of data protection of relevant products and services.'[203] This concept can prove to be useful with respect to new distributed information platforms, such as blockchain, as its development requires cooperation between legislative bodies and the developers.

7.2 Solutions and Compliant Designs

Undertakings can consider designing measures that allow data subjects to contest decisions that are taken regarding them. These include building digital platforms that allow the data

[201] Art. 25(1) GDPR.
[202] ibid.
[203] Recital 100 GDPR

subjects to make requests regarding their on-chain personal data. As a result, data subjects can have the opportunity to be involved in the actual design stage of a blockchain platform and co-operate with the digital engineer in flagging out design choices that may infringe upon the data subject rights in the future.[204] This approach delivers *contestability by design*, thus ensuring, for example the right to human intervention to some degree.[205]

It is also possible to avoid the scope of the GDPR altogether. This rests on the development of cryptographic processes that have the capabilities of successfully anonymising personal data for the purposes of the GDPR. The standard methods of hashing such as SHA-256 or the SHA-3 could be capable of anonymising data according to the European Court of Justice or the European Data Protection Supervisor.[206] However, the safe way to ensure the protection of data subject rights is to assume that encryption will be broken at some point in the future due to technological advancements. To avoid this, undertakings should regularly update their encryption methods in order to maintain current industry standards.

There are other technical developments which allow transactional data of smart contracts not to be stored directly on blockchain.[207] Personal data could be stored off-chain and be linked to the chain by using a hash pointer. This means the on-chain hash would locate the reader to an external database, such as a centralized data silo. This solution combines data-management on blockchain and off-chain databases, but brings alongside it an additional obligation to ensure that the off-chain data is treated accordingly for the purposes of the GDPR. Hence, a centralized data storage may require the implementation of an additional controller which may or may not defeat the original purpose of using blockchain altogether. An example of this sort of experiment is the Luxtrust and Cambridge Blockchain.[208] This implementation is focused on storing proof of data validity and identity management on-chain whereas off-chain data is held on an external database.

---

[204] Janet Davis, 'Design Methods for Ethical Persuasive Computing' (2009)ACM: Proceedings of the 4th International Conference on Persuasive Technology <http://cs.whitman.edu/~davisj/pubs/davis-persuasive2009.pdf> accessed 16 April 2019.
[205] Marco Almada 'Human intervention in automated decision-making: Toward the construction of contestable systems' (2019) University of São Paulo <https://www.academia.edu/38554058/Human_intervention_in_automated_decision-making_Toward_the_construction_of_contestable_systems> accessed 21 June 2019.
[206] Finck (n 3) 23.
[207] See Page 18, Transactional Data of Smart Contracts.
[208] LuxTrust and Cambridge Blockchain: Business Wire, 'LuxTrust and Cambridge Blockchain Announce Privacy-Protecting Identity Platform' (Sys-Con Media, 15 May 2017) <https://www.businesswire.com/news/home/20170515005091/en/LuxTrust-Cambridge-Blockchain-Announce-Privacy-Protecting-Identity-Platform> accessed 25 April 2019.

7.2.1 Data Protection Impact Assessments

Implementing a blockchain system will trigger an obligation for the specific undertaking to carry out a Data Protection Impact Assessment (DPIA) with respect to the envisaged data processing. Under Art. 35(1) of the GDPR, this takes place where the data processing is engaged with (1) execution of new technologies; or where (2) the scope, nature and context of the data processing have significant risks to the rights and interests of natural persons.

Art. 35(3) requires that DPIAs are carried out when the data processing involves (1) extensive evaluation of personal aspects related to the natural persons, which is based on automated processing; (2) processing of special categories of data, such as data related to criminal convictions; or (3) a systematic and large scale of processing. If the DPIA suggests that the envisaged processing involves a high risk for the rights and interests of data subjects, and that there are no possible mitigatory measures to be taken, the controller must inform a supervisory authority.[209]

Because Art. 35(3) suggests that a DPIA is required to be carried out when the processing is conducted on an extensive and systematic scale with respect to personal aspects of natural persons, it may not be necessary to conduct a DPIA with respect to all smart contracts. This issue depends on the nature of the smart contract, but *prima facie* it seems that the scope, nature and context of smart contracts are not always a high risk to the rights and interests of natural persons, because they mostly process data simple transactional data such as property rights and funds. Furthermore, smart contracts themselves are not 'new technology', considering the fact that they date back to Nick Szabo's idea in 1996. The technology has been in daily use in vending machines, certain types of financial transactions and passport control mechanisms. However, blockchain-based smart contracts are likely to be considered 'new technology' which require a DPIA. Blockchain platforms pose a risk to the interests and rights of natural persons, because of the default transparency and lack of clear hierarchical structures which make compliance with GDPR burdensome. A DPIA will have to be carried out on a case-by-case basis as the risks differ regarding different technical and infrastructural use-cases. For example, a private permissioned blockchain poses significantly less issues

[209] Art. 36(1) GDPR.

with respect to the identity of data controllers than public permissionless blockchains and can allow more control with respect to data subject rights, such as the right to erasure.

7.2.2 Consent-based Blockchain Design

The centre of personal data protection is the data subject's consent under Art. 6(1) GDPR and it is one of the fundamental justifications for processing personal data. Therefore, it can be transferred into technical arrangements. Consent means that the the data subject is asked for his/her approval for the processing of personal data. Furthermore, the data subject must be able to withdraw consent given to a specific party.[210] Whenever personal data is processed, the data subject can be notified through the blockchain, in order to give the data subject control over his/her data.

The data subject should be the only person with the competence of decrypting on-chain personal data. To facilitate this, a public key encryption method can be used where the issuing party encrypts the verified personal data using their public key, sends the encrypted data to the data subject and retains only the hash point of the data.[211] The hash is located on-chain and allows any third party to validate the decrypted personal data, delivered by a smart contract. As a result, the data subject can be notified every time personal data is requested for processing. Consequently, instead of giving consent once during first access, the data subject can provide consent for every action concerning the processing of personal data.[212] However, this is a larger burden on the undertaking that must ensure compliance under the GDPR.

Provided that the data subject has 'freely' given consent to the processing according to Recital 32, the on-chain smart contract shall process one type of personal data issued by the third party at any given time. This way an up-to-date copy of the data can be applied on the condition that the smart contract has validated the certification of the third party and the consent of the data subject.[213] This arrangement works if the data subject is the only one who can access the decrypted version of the on-chain data with the private key. Hence, blockchain

[210] Art. 7(3) GDPR.
[211] Christian Wirth, Michael Kolain. 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data' (2018) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies, 3 https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf accessed 5 June 2019.
[212] ibid.
[213] Christian Wirth et al. (n 211) 3.

is a suitable platform for this particular application. Ensuring that additional copies of personal data are accurate and up-to-date when the specific hash changes is achievable by modifying the on-chain timestamp in the data when access to it is requested. This is not a direct change on the on-chain data, but can satisfy the requirements of the right to rectification and the right to erasure.[214]

7.3 Interim Conclusion

Undertakings must transpose the GDPR's privacy requirements onto blockchain platforms from the ground-up. Even though blockchain faces challenges with many of the GDPR's principles of data processing, the system may also enable the efficient protection of data privacy. This requires that adequate transparency exists on a blockchain through which the data subject's rights and legitimate interests can be protected in real-time.

Undertakings should consider combining their blockchain applications with centralised data silos which enables them to modify and erase data. This means storing hash-pointers on-chain and storing the personal data related to various transactions off-chain. Smart contracts embedded into blockchain will almost certainly require undertakings to conduct a DPIA in order to clarify the risks posed to the legitimate rights and interests of data subjects. Additionally, a blockchain design that relies on the data subject consent can assist in respect of compliance by making the system adhere to the general data processing principles of the GDPR better.

[214] ibid. 4.

8 Concluding Remarks

With the aim of examining the compliance of blockchain-based smart contracts with the GDPR, this thesis has analysed how, and by which party, data subject rights can be enforced on a blockchain. In the overall conclusion, data subject rights and the general principles of data processing raise several concerns of infringement for undertakings that choose to implement blockchain technology in their data processing. The examination demonstrates that the highest risk of non-compliance and administrative fines is raised by the public permissionless blockchain. This is due to the peer-to-peer mechanism which eliminates the clear governing structure of data subject rights enforcement the GDPR seeks to establish. Hence, the controller on a public permissionless blockchain is either the collective of network actors as a single body under Art. 4(7) of the GDPR, or the network actors function as joint controllers under Art. 26. Undertakings should implement blockchain designs that allow seamless transitioning of data between external data silos and the blockchain. Until the developers and legislators successfully cooperate to solve issues with respect to the public permissionless blockchain, e.g., the identity of the controller, data erasure and data minimisation, the designs must be private permissioned blockchains. These use-cases have resemblance to centralised data systems because companies and consortia can designate clear governing bodies and identities for the network actors. As a result, enforcement of data subject rights and legitimate interests becomes less burdensome. The bottom line is that these issues serve as an incentive towards the development of blockchain-specific primary legislation and cooperation between blockchain developers and the legislators.

List of References

Primary Sources

EU Legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119)

EU Case Law

C-210/6 *Wirtschaftsakademie Schleswig Holstein* [2018] EU:C:2018:388.

CJEU Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EC:C:2016:779

Case C-267/06 *Tadao Maruko* [2008] ECLI:EU:C:2008:179

Case C-162/97, *Nilsson*, [1998] ECLI:EU:C:1998:554

Secondary Sources

Books

Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer Publishing 2017)

Lukas Feiler, *The EU General Data Protection Regulation (GDPR -) A Commentary* (German Law Publishers 2018)

De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018)

Journal Articles

Michèle Finck, 'Blockchains and Data Protection in the European Union' (1/2018), European Data Protection Law Review, 17-35. < https://doi.org/10.21552/edpl/2018/1/6>

Conte de Leon et al, 'Blockchain: Properties and Misconceptions' (2017) 11 Asia Pacific Journal of Innovation and Entrepreneurship https://www.emeraldinsight.com/doi/full/10.1108/APJIE-12-2017-034

Davidson S., De Filippi P. and Potts J., 'Blockchains and the economic institutions of capitalism' (2018) Journal of Institutional Economics 14(4), 639-658 https://doi.org/10.1017/S1744137417000200

Paulina Jo Pesch, Christian Sillaber, 'Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements' (6/2017) Computer Law Review International,167-172, <https://ssrn.com/abstract=3210499>

Primavera De Filippi, 'The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) 9 Journal of Peer Production http://peerproduction.net/wp-content/uploads/2016/08/blockchain-technologies-draft.pdf

Wachter et al, 'Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76 <https://academic.oup.com/idpl/article/7/2/76/3860948>

Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243 < https://doi.org/10.1093/idpl/ipx019>

Mario Martini and Quirin Weinzierl, 'Die Blockchain-Technologie und das Recht auf Vergessenwerden sind Antagonisten' (2017) Neue Zeitschrift für Verwaltungsrecht, 1251

Thomas Buocz et al., 'Bitcoin and the GDPR: Allocating responsibility in distributed networks' (2019) Computer Law & Security Review 35, 182-198, 194, <https://www.sciencedirect.com/science/article/pii/S0267364918303170>

Tina Ehrke-Rabel, Iris Eisenberger et al., 'Bitcoin-Miner als Prosumer: Eine Frage staatlicher Regulierung? Dargestellt am Beispiel das Glücksspielrechts' (2017) Austrian Legal Journal 188-219 < https://alj.uni-graz.at/index.php/alj/article/download/116/181/>

Primavera De Filippi and Benjamin Loveluck, 'The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure' (2016) 5(4) Internet Policy Review 1, 9 https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure

Jeffery Atik and George Gerro, 'Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice' (2018) 1(1) Stanford Journal of Blockchain Law & Policy https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203893

Working Papers

Valeria Ferrari, 'EU Block chain Observatory and Forum Workshop on GDPR, Data Policy and Compliance', Institute for Information Law Research Paper No. 2018-04, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247494> accessed 3 April 2019

Gavin Wood, 'Ethereum: A secure decentralized generalised transaction ledger' Ethereum Project Yellow Paper (2014) 151 <https://gavwood.com/paper.pdf> accessed 19 April 2019

Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 accessed 25 May 2019

James Smith et al, 'Applying Blockchain Technology in Global Data Infrastructure' (2016) Technical Report ODI-TR-2016-001, Open Data Institute https://data.gov.ru/sites/default/files/documents/315354748-applying-blockchain-technology-in-global-data-infrastructure.pdf accessed 9 June 2019

Biryukov et al, 'Deanonymisation of Clients in Bitcoin P2P Network' (2014) <https://arxiv.org/pdf/1405.7418.pdf> accessed 30 April 2019

J. D. Nick, "Data-driven De-Anonymization in Bitcoin," Master's thesis, Computer Systems Institute - ETH Zurich, 2015 < https://www.research-collection.ethz.ch/handle/20.500.11850/155286> accessed 10 June 2019

E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge
for a von Neumann architecture," in 23rd USENIX Security Symposium (USENIX Security 14), <https://eprint.iacr.org/2013/879.pdf> accessed 10 June 2019

Natalie Eichler; Silvan Jongerius; Greg McMullen; Oliver Naegele; Liz Steiniger; Kai Wagner, 'Blockchain, data protection, and the GDPR' (2018) Blockchain Bundesverband, VR 36105 B https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf accessed 18 June 2019

Janet Davis, 'Design Methods for Ethical Persuasive Computing' (2009) ACM: Proceedings of the 4th International Conference on Persuasive Technology <http://cs.whitman.edu/~davisj/pubs/davis-persuasive2009.pdf> accessed 16 April 2019

Marco Almada 'Human intervention in automated decision-making: Toward the construction of contestable systems' (2019) University of São Paulo <https://www.academia.edu/38554058/Human_intervention_in_automated_decision-making_Toward_the_construction_of_contestable_systems> accessed 21 June 2019

Christian Wirth; Michael Kolain, 'Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data' (2018) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially

Embedded Technologies, 3
https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf accessed 5 June 2019

Websites and Online Sources

European Commission, 'The GDPR: new opportunities, new obligations' < https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf> accessed 14 May 2019

Satoshi Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' (2009) <https://bitcoin.org/bitcoin.pdf> accessed 18 April 2019

Karl Wüst, Arthur Gervais, 'Do you need a Blockchain?' (2017) <https://eprint.iacr.org/2017/375.pdf> accessed 18 April 2019

Grant Thornton, *GDPR & Blockchain, Blockchain solution to General Data Protection Regulation*, <https://www.grantthornton.global/globalassets/___spain___/links-ciegos/otros/gdpr--blockchain.pdf> accessed 10 April 2018

Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 11 March 2019

Nathan Reif, 'Who is Nick Szabo, and is he Satoshi Nakamoto?' (2018) < https://www.investopedia.com/news/who-nick-szabo-and-he-satoshi-nakamoto/> accessed 4 June 2019

DLA Piper, 'A guide to the General Data Protection Regulation' (2018), https://www.dlapiper.com/en/uk/insights/publications/2016/12/a-guide-to-the-general-data-protection-regulation/, accessed 4 March 2019

The Swedish Data Protection Authority, Datainspektionen, 'The purposes and scope of the General Data Protection Regulation' < https://www.datainspektionen.se/other-lang/in-

english/the-general-data-protection-regulation-gdpr/the-purposes-and-scope-of-the-general-data-protection-regulation/> accessed 7 June 2019

Vitalik Buterin, 'Privacy on the Blockchain (Ethereum Blog, 15 January 2016) https://blog.ethereum.org/2016/01/15/privacy-on -the-blockchain/ accessed 8 June 2019

https://shop.wikileaks.org/donate> accessed 8 June 2019

https://www.chainalysis.com/ accessed 8 June 2019

Facebook, 'Accessing and Downloading Your Facebook Information' <https://www.facebook.com/help/contact/2032834846972583> accessed 4 June 2019

Bitcoin nodes, 'Global Bitcoin Nodes' <https://bitnodes.earn.com/> accessed 2 May 2019

Michael del Castillo, 'Ethereum Executes Blockchain Hard Fork to Return DAO Funds' < https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds> accessed 9 May 2019

'Understanding Hard Forks in Cryptocurrency' https://cryptocurrencyfacts.com/understanding-hard-forks-cryptocurrency/ accessed 10 May 2019

Commission Nationale Informatique & Libertés, 'Blockchain: Solutions for a responsible use of the blockchain in the context of personal data' (2018) 8 < https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf> accessed 28 May 2019

DXC Labs, 'Machines that pay each other using digital wallets'< https://blogs.dxc.technology/2019/01/29/machines-that-pay-each-other-using-digital-wallets/> accessed 16 May 2019.

European Commission, 'European Countries Join Blockchain Partnership' https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership accessed 11 June 2019

Bitcoinwiki, ‘Full Node‘< https://en.bitcoin.it/wiki/Lightweight_node> accessed 24 May 2019

Bitcoin.org, ’Bitcoin Core‘ https://bitcoin.org/en/bitcoin-core/ accessed 25 May 2019

Ethereum, < https://www.ethereum.org/> accessed 25 May 2019

LuxTrust and Cambridge Blockchain: Business Wire, ‘LuxTrust and Cambridge Blockchain Announce Privacy-Protecting Identity Platform’ (Sys-Con Media, 15 May 2017) <https://www.businesswire.com/news/home/20170515005091/en/LuxTrust-Cambridge-Blockchain-Announce-Privacy-Protecting-Identity-Platform> accessed 25 April 2019

Other Sources

Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679,* WP 251 (3 October 2017, revised 6 February 2018)

Article 29 Working Party, ‘Opinion 04/2014 on Anonymisation Techniques’ (2014) 0829/14/EN, 20

Article 29 Data Protection Working Party, ‘Opinion 1/2010 on the Concepts of “Controller” and “Processor”’ (2010) 6 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>