

FACULTY OF LAW  
Stockholm University

---

# **The General Data Protection Regulation vs. The Blockchain**

**- A legal study on the compatibility  
between blockchain technology and the  
GDPR**

---

*Sebastian Ramsay*

Thesis in *Law and Informatics*, 30 HE credits  
Examiner: Peter Wahlgren  
Stockholm, *Spring* term 2018



## **Abstract**

This thesis examines open distributed blockchain technology from a legal perspective. The blockchain is a technology used to secure and ensure the integrity of data in an unsafe digital environment. Traditionally, peer-to-peer networks (P2P-networks), synonymous with distributed networks, have faced the issue of ensuring the integrity of data and deterring scams such as double spending, which refers to someone using the same assets twice, and has discouraged people from using P2P-networks. Scams like double spending have been possible in the absence of a governing party ensuring the integrity of the data, that is until the introduction of Bitcoin in 2008, which introduced a cryptographic solution to ensuring the data's integrity in a P2P electronic cash system. By relying on cryptography, instead of trusting institutions for the integrity of transactions, the introduction of Bitcoin facilitated a move towards decentralization where classical middleman services, like banking, are becoming obsolete.

The General Data Protection Regulation (GDPR), which is to be implemented in all European Union (EU) member countries on May 25<sup>th</sup>, 2018, is a regulation that aims to harmonize data privacy laws across Europe. The GDPR introduces several fundamental rights and freedoms for natural persons regarding the protection of their personal data. This means that certain responsibilities are imposed on the responsible parties that process personal data.

This thesis examines to which extent the GDPR is applicable to an open distributed blockchain and if the fundamental principles under the regulation can be upheld, respectively if the responsible parties can fulfill their responsibilities imposed by the regulation.

## **Abbreviations**

A29WP	Article 29 Data Protection Working Party
CJEU	Court of Justice of the European Union
E.g.	For example
Etc.	Et cetera
EU	European Union
Ff.	And the following pages
GDPR	General Data Protection Regulation
I.e.	In other words
P2P	Peer-to-peer
Ref.	Reference
SvJT	Svensk Juristtidning (Swedish Law Journal)
TfR	Tidsskrift for Rettsvitenskap (Periodical for Nordic Jurisprudence)

# Table of Contents

<b>1 INTRODUCTION.....</b>	<b>5</b>
1.1 AIM AND RESEARCH QUESTIONS.....	7
1.2 DELIMITATIONS.....	7
1.3 METHOD.....	8
1.4 MATERIAL.....	11
1.5 TERMINOLOGY.....	13
1.6 DISPOSITION.....	14
<b>2 BLOCKCHAIN TECHNOLOGY.....</b>	<b>15</b>
2.1 BREAKING THE BLOCKCHAIN INTO PIECES.....	15
2.2 A TECHNICAL DETOUR.....	17
2.2.1 Hash Functions.....	17
2.2.2 Hash References.....	18
2.2.3 Hash Puzzles.....	19
2.2.4 Asymmetric Cryptography and Digital Fingerprints.....	19
2.2.5 Digital Signatures.....	20
2.3 THE 7 STEPS.....	20
2.3.1 Describing Ownership.....	21
2.3.2 Protecting Ownership from Unauthorized Access.....	21
2.3.3 Storing Transaction Data.....	22
2.3.3.1 Data-structure.....	22
2.3.3.2 Adding and Changing Transaction Data.....	24
2.3.4 Preparing Ledgers to be Distributed in an Untrustworthy Environment.....	24
2.3.5 Recap Heretofore.....	25
2.3.6 Forming a System of the Ledgers.....	25
2.3.7 Adding Transactions to the Ledger.....	26
2.3.8 Choosing the Ledger that Represents the Truth.....	27
2.4 BLOCKCHAIN SUMMARY AND RELEVANCE.....	28
<b>3 THE GDPR.....</b>	<b>29</b>
3.1 PERSONAL DATA.....	29
3.2 PROCESSING.....	31
3.3 CONTROLLER.....	31
3.4 PROCESSOR.....	32
3.5 RIGHTS AND RESPONSIBILITIES.....	33
3.5.1 Fundamental Principles.....	33
3.5.2 Data Subjects Rights.....	35
3.5.2.1 Right to Information.....	35
3.5.2.2 Right to Erasure, Rectification and Restriction of Processing.....	36
3.5.2.3 Right to Data Portability.....	36
3.5.2.4 Right to Object and Automated Decision Making.....	37
3.6 THE CONTROLLERS ADDITIONAL RESPONSIBILITIES.....	37
3.6.1 Data Protection Measures.....	38

3.6.2 Joint Controllership and Responsibilities .....	38
3.6.3 Processor Measures .....	39
3.6.4 Keeping Records of Processing Activities.....	39
3.6.5 Security Measures When Processing .....	39
3.7 GDPR CONCLUSION.....	40
<b>4 THE BLOCKCHAIN AND THE GDPR .....</b>	<b>41</b>
4.1 PERSONAL DATA .....	41
4.1.1 Public Keys and Transaction Data .....	41
4.1.2 Nodes.....	42
4.2 PROCESSING .....	43
4.2.1 Processing Public Keys and Transaction Data.....	44
4.2.2 Processing Nodes .....	44
4.3 CONTROLLER.....	45
4.3.1 Labelling the User.....	45
4.3.2 Labelling the Creator(s).....	46
4.4 PROCESSOR .....	47
4.5 RESPONSIBILITIES .....	48
4.5.1 Organizational Measures.....	48
4.5.1.1 Data Protection .....	48
4.5.1.2 Processor Measures .....	50
4.5.1.3 Keeping Records of Processing Activities .....	51
4.5.1.4 Security of Processing.....	52
4.6 RIGHTS OF THE INDIVIDUAL .....	53
4.6.1 Right to Information .....	54
4.6.2 Right to Erasure, Rectification and Restriction of Processing .....	54
4.6.3 Data Portability.....	56
4.6.4 Right to Object and Automated Decision Making.....	57
4.7 FUNDAMENTAL PRINCIPLES .....	58
4.8 CONCLUSION .....	60
<b>5 FINAL COMMENT.....</b>	<b>61</b>
<b>6 BIBLIOGRAPHY .....</b>	<b>62</b>

# 1 Introduction

*“With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.”*

—Satoshi Nakamoto, Founder of Bitcoin

To say that cryptocurrencies and innovations that utilize blockchain technology have exploded during the last few years would be an understatement. When entering the year of 2018, cryptocurrencies altogether had a market cap of roughly 600 billion United States Dollars (USD). Having only reached 18 billion USD the year before, this meant that the cryptocurrency market-cap had grown roughly 3200% in one year.<sup>1</sup> As of entering the new year we also saw over 1400 cryptocurrencies, indicating that the number of innovations doubled from last year, as there were only just over 700 going into 2017.<sup>2</sup> The surge of money being invested in blockchain technology and the increasing use-cases has caught the public’s and media’s attention, attracting more investors and speculators daily.

Having a completely new technology immerse in such a short span of time does not come without its own problems, especially if the technology continues to grow and gain massive traction. The implications can be many, such as security concerns, primarily if the technology is vulnerable to data leaks and if it jeopardizes a person's integrity, and also regulatory concerns. Regulatory frameworks, that are specifically targeting technology and innovations, can be rendered useless since technology is always one step ahead of the legal development. This ultimately leads to a climate where regulatory issues of a technological character are a day-to-day issue for governments and organizations.

Nationally and internationally there are growing concerns regarding how data is processed, especially personal data, i.e. data that can identify someone as a natural person, due to privacy and personal integrity matters.<sup>3</sup> In an attempt to protect individuals in the golden age of information the EU has laid forth the General Data Protection Regulation (GDPR).<sup>4</sup> The GDPR

---

<sup>1</sup> Web.archive.org. (2018). All Currencies | Crypto-Currency Market Capitalizations. [online] Available at: <https://web.archive.org/web/20170115051728/http://coinmarketcap.com/all/views/all/> [Accessed 19 Apr. 2018].

<sup>2</sup> Coinmarketcap.com. (2018). Global Charts | CoinMarketCap. [online] Available at: <https://coinmarketcap.com/charts/> [Accessed 19 Apr. 2018].

<sup>3</sup> Klamberg, M., Magnusson Sjöberg, C. and Öman, S. (2015). *”Skydd av personlig integritet och informationsfrihet”*. In: Magnusson Sjöberg, C. (ed.), *Rättsinformatik: juridiken i det digitala informationsmiljöet*. 1st. ed. Lund: Studentlitteratur, p. 144.

<sup>4</sup> 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).

will be implemented on May 25<sup>th</sup>, 2018, and seeks to protect the individual's privacy, which is a fundamental right under The Charter of the European Union, by setting rules for the processing of personal data.<sup>5</sup> In short, the GDPR seeks to harmonize all Data Privacy Laws across Europe with the aim of contributing to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.<sup>6</sup> The GDPR seeks to do so by clarifying existing rules and imposing new rules on how personal data is processed with the goal of increasing transparency and integrity.

Integrity is often described as an internal consistency or lack of corruption in electronic data.<sup>7</sup> Integrity can, in other words, be described as the assurance of the accuracy and correctness of data and is a central building block of the information security triad: confidentiality, integrity and availability (CIA).<sup>8</sup> The blockchain's strength lies in securing the integrity of data in networks without a central point of connection, peer-to-peer (P2P) networks, by utilizing cryptography to create distributed registers.<sup>9</sup> The registers can be publicly viewed as well as publicly modified and could potentially be considered to process personal data.<sup>10</sup> Processing under the GDPR is not specific to any piece of technology but is rather any set of actions performed on personal data, such as storing or even the alteration of data.<sup>11</sup> Both the GDPR and the blockchain aspire to increase integrity, trust and transparency in a generally unsafe environment. The GDPR does so by imposing responsibilities upon data controllers and data processors that are, according to a more classical computing environment philosophy, single providers of computing resources and storage.<sup>12</sup> Hence, the GDPR assumes to an extent that data controllers and data processors are centralized actors with control over the system. The blockchain, on the other hand, ensures trust and transparency in P2P-networks, that by nature are decentralized, by utilizing the computational power of the masses and by sharing the register

---

<sup>5</sup> Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter').

<sup>6</sup> Recital 2 in the GDPR.

<sup>7</sup> Oxford Living Dictionaries. (2018). [online] Oxford University Press. Available at: <https://en.oxforddictionaries.com/definition/integrity> [Accessed 11 May 2018].

<sup>8</sup> Rouse, M. (2018). Confidentiality, integrity, and availability (CIA triad). [online] WhatIs.com. Available at: <https://whatIs.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> [Accessed 20 May 2018].

<sup>9</sup> Mougayar, W. and Buterin, V. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons, Incorporated, New York, p. 20.

<sup>10</sup> Finck, M. (2017). Blockchains and Data Protection in the European Union Max Planck Institute for Innovation & Competition Research Paper No. 18-01, pp. 17 – 35.

<sup>11</sup> Article 4(2) in the GDPR.

<sup>12</sup> Article 24-43 in the GDPR.

with all peers in the P2P-network.<sup>13</sup> Therefore, the blockchain contradicts the assumption that there always is a centralized actor with control over the system and facilitates a move towards decentralized models.<sup>14</sup> In turn, this can eliminate traditional actors as more people see the benefits of utilizing the blockchain and P2P-networks.

### **1.1 Aim and Research Questions**

The aim of this thesis is to investigate the extent to which the GDPR and the obligations it creates can be applied to the blockchain considering the following research questions:

- What is the blockchain and how does it work?
- What are the fundamental principles as encapsulated in the GDPR and how do they relate to the blockchain?
- How do the role divisions imposed by the GDPR and the associated obligations relate to the blockchain?

### **1.2 Delimitations**

The target audience of this thesis are lawyers with a basic understanding of software and software architecture. The thesis will set the stage for a new area of technology from a legal perspective, resulting in an analysis that does not immerse in specific conceptions but instead creates a broad underlay to understand and conceptualize the legal problems surrounding the technology. An explanation of the blockchain will be made to the extent the author finds it necessary for the reader to comprehend the basic technological aspects. Inquiries regarding different blockchain technologies will be limited to avoid a thesis that is of too technical a character. Ethereum, for example, uses a non-binary hash tree, unlike Bitcoin that uses a binary hash tree, which is not of relevance for the basic understanding of the technology. This thesis focuses on openly distributed blockchains, which means blockchains that are openly viewable and available to everyone.<sup>15</sup> Different kind of cryptocurrencies and tokens will also only be mentioned to the extent it is necessary to clarify the underlying technology. The economic value of blockchain will not be discussed as this does not hold any relevance to questions regarding the GDPR and blockchain. Digital fingerprints will only be mentioned in a blockchain context

---

<sup>13</sup> Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress, Berkeley, CA, p. 24.

<sup>14</sup> Cox, T. and Solomon, A. (2018). Block chain: Is the GDPR out of date already? | Lexology. [online] Lexology.com. Available at: <https://www.lexology.com/library/detail.aspx?g=d4c0481a-c678-4748-80cb-4ab917e66207> [Accessed 19 Apr. 2018].

<sup>15</sup> BlockchainHub. (2018). Blockchains & Distributed Ledger Technologies. [online] Available at: <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/> [Accessed 19 Apr. 2018].

and the legality of digital fingerprints will not be discussed. Also, centralized data-structures will only be discussed to the extent it is necessary to understand blockchain technology.

While blockchain technology is interesting out of many regulatory aspects, e.g. the taxation of cryptocurrencies, this paper is strictly limited to those aspects that are of relevance to answer the aforementioned questions. Other regulations will only be mentioned where it attributes to achieving the aim of the paper and to answer the research questions mentioned above.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data will not be discussed, to the extent that the relevant Articles are discussed in the GDPR.

While the GDPR offers many interesting Articles applicable to blockchain technology, certain limitations will have to be made to ensure a qualitative paper that examines the problems laid forth and gives the reader a deeper level of understanding considering the research questions. The paper will discuss provisions within Chapter 1-4 in the GDPR since the contained Articles directly concern the research questions mentioned above. The organizational responsibilities and rights of data subjects under the GDPR are limited to those that hold the most relevance from a blockchain perspective. Chapter 5 in the GDPR regarding transfers of personal data to third countries or international organizations, as well as all other provisions relating to transfers of personal data and sanctions, will not be discussed in this thesis due to formal limitations.

### **1.3 Method**

This thesis will use the traditional ‘legal method’, also referred to as ‘legal dogmatics’, as its point of departure. The legal method focuses on the utility of solving legal problems by researching the classical sources of law, namely, legislation, case law, legislative history and doctrine.<sup>16</sup>

The legal method is not easily described and what it, in reality, consists of has been subject to discussion by scholars.<sup>17</sup> Sandgren questions the qualities of the legal method as the method has developed into a norm where more than often jurisprudence is labeled as dogmatic without any deeper clarification of what that in reality entails.<sup>18</sup> Kleineman clarifies that it is often easier to describe what exactly one is doing when applying the given method instead of trying to

---

<sup>16</sup> Greenstein, S. (2017). *Our Humanity Exposed: Predictive Modelling in a Legal Context* (Ph.D. dissertation). Department of Law, Stockholm University, Stockholm, p. 33.

<sup>17</sup> Sandgren, C. (2005). Är rättsdogmatiken dogmatisk? *Tidsskrift for Rettsvitenskap*, TfR, 118(4–5), 648 ff. See also, Jareborg, N. (2004). Rättsdogmatik som vetenskap. *Svensk Juristtidning*, 1–10, p. 1 ff.

<sup>18</sup> Sandgren, *Är rättsdogmatiken dogmatisk*, p. 649.

explain the method itself, as this can result in a vague, uncertain and contradictory explanation.<sup>19</sup> The purpose of the method is often described as the recreation of established law by applying such law to a specific legal problem.<sup>20</sup> That requires that the method itself has to be derived from a certain set of rules and Jareborg describes the classical legal method to be derived from legislation, case law, legislative history and doctrine.<sup>21</sup> Jareborg does not rule out the possibility of widening one's perspective to look for answers outside of the established law as all scientific activities strive to seek new and better answers.<sup>22</sup> Kleineman says that one first has to assess the principal questions that are actualized as these can limit the underlay for the analysis and mentions the principle of legality as an example since the principle imposes certain restrictions on how one is to interpret established law.<sup>23</sup> If seen from Jareborgs and Kleinemans perspective, the core of the method is that it more than often has a specific legal problem as its outset.<sup>24</sup> The purpose is then to arrive at a conclusion through the recreation of established law, but not being limited to the established law as the process also is subject to a creative analysis that creates a solution that might not have been explicit before the recreation was made.<sup>25</sup>

Olsen explains the legal method as a means for expressing and motivating an authoritative dictum concerning current law.<sup>26</sup> Since the dictum is to be authoritative it must be derived from authoritative sources. This results in a very limited and unpractical analysis of law, for which the method has received a lot of critique. Olsen problematizes the legal method by bringing up the scarcity of authoritative material to analyze and describe newer judicial areas.<sup>27</sup> The core focus is therefore, according to Olsen, only the current law, which is completely disconnected from values, expert's opinions and even *de lege ferenda*. This can be problematic when faced with a legal problem that is without an exact answer and *de lege lata* is not enough to solve the problem. For this reason, several other legal methods have evolved out of the legal method to assess its faults and repair them.<sup>28</sup> Olsen would rather classify the method as a theory with the goal of establishing what the current law is, which can be useful for judges and other legal

---

<sup>19</sup> Kleineman, J. (2013). "*Rättsdogmatisk metod*". In: Korling, F. and Zamboni, M. (eds.), *Juridisk metodlära*. 1st. ed. Lund: Studentlitteratur, p. 21.

<sup>20</sup> Kleineman, "*Rättsdogmatisk metod*". In: Korling & Zamboni (eds.), *Juridisk metodlära*, p. 21.

<sup>21</sup> Jareborg, *Rättsdogmatik som vetenskap*, p. 8.

<sup>22</sup> *Ibid.*, p. 4.

<sup>23</sup> Kleineman, "*Rättsdogmatisk metod*". In: Korling & Zamboni (eds.), *Juridisk metodlära*, pp. 30-31.

<sup>24</sup> Kleineman, "*Rättsdogmatisk metod*". In: Korling & Zamboni (eds.), *Juridisk metodlära*, p. 23.

<sup>25</sup> *Ibid.*, p. 44.

<sup>26</sup> Olsen, L. (2004). *Rättsvetenskapliga perspektiv* (Perspectives of Jurisprudence), SvJT, p. 118.

<sup>27</sup> Olsen, L. *Rättsvetenskapliga perspektiv*, p. 120.

<sup>28</sup> *Ibid.*, p. 121.

practitioners, but to say that the method would be a practical tool for solving complex legal issues would not agree with Olsen's philosophy.

Sandgren shares, to an extent, Olsen's opinion on the legal method and says that most jurisprudential writings are not about identifying established law, but rather about systemizing the material, developing the conceptual apparatus, analyzing arguments and possible solutions, forming theories and principles and critically examining the legal position.<sup>29</sup> Sandgren assesses if such a practice truly can be viewed as dogmatic when questions regarding external resources, goals and values arise. This translates, according to Sandgren, into a clear distinction between the dogmatic practice and the analytical practice.<sup>30</sup> Sandgren means to say that most jurisprudential writings of today are of analytical character.

Like many other countries, Sweden is a member of the European Union (EU). A membership in the EU comes with its own set of governing rules and legal principles that all member states must abide by.<sup>31</sup> This means that new sets of binding legislations, case law and principles are merged into the already existing national motor.<sup>32</sup> Since the member states have committed to the EU they have a responsibility towards the EU and their own citizens to enforce the EU's sets of rules and principles, widening the applicable sources of law within the legal method. The EU legal method is a legal method that serves the purpose of guidance on how to approach and handle EU derived sources of law.<sup>33</sup>

This thesis aims to analyze a technology that is characterized by regulatory uncertainty. The analysis will have to be widened to include material and sources that are excluded from the traditional legal method, to cater to assessments where the legal method fails to provide a sufficient answer. The legal framework will then be analyzed in light of such sources and materials to ensure that the paper satisfies its aim. This approach is what Sandgren refers to as the legal analytic method.<sup>34</sup> The legal analytic method does not limit the writer to any form of material, but rather grants the writer access to all material to satisfy an interest for further knowledge.<sup>35</sup> While the legal method serves the purpose of assessing the legal sources, the legal analytic method serves the purpose of analyzing the law. An analysis is not bound by the

---

<sup>29</sup> Sandgren, *Är rättsdogmatiken dogmatisk*, p. 652.

<sup>30</sup> Sandgren, *Rättsvetenskap för uppsatsförfattare*, p. 45 ff.

<sup>31</sup> Hettne, J. and Otken Eriksson, I. (eds.), (2011). *EU-rättslig metod*. Stockholm: Norstedts juridik, p. 21.

<sup>32</sup> Reichel, J. (2013). *"EU-rättslig metod"*. In: Korling, F. and Zamboni, M. (eds.), *Juridisk metodlära*. 1st. ed. Lund: Studentlitteratur, p. 115.

<sup>33</sup> Hettne and Otken Eriksson, *EU-rättslig metod*, p. 21.

<sup>34</sup> Sandgren, *Är rättsdogmatiken dogmatisk*, p. 656.

<sup>35</sup> *Ibid.*, p. 655.

traditional sources of law, but the use of the legal analytic method often has its outset in assessing the legal sources, which causes the methods to overlap to some extent.

Metaphors have been described by legal scholar Winter as: “*the imaginative capacity by which we relate one thing to another*”.<sup>36</sup> Solove describes metaphors as not only a way of describing a phenomenon, but also a way of conceptualizing something theoretical.<sup>37</sup> Much like Winter and Solove, philosopher Johnson and linguistics professor Lakoff describe metaphors as a way of “*experiencing one kind of thing in terms of another*”.<sup>38</sup> Therefore, metaphors can in a legal context act as an instructive method, not for their realism, but for their way to direct our focus to certain social and political phenomena that can help conceptualize unfamiliar theories by applying such theories to layman’s examples.<sup>39</sup>

Therefore, the thesis will assess, describe and systemize the blockchain with an outset in the classical sources of law, namely, legislation, case law, legislation history and doctrine. Legislation and its history will, however, be given the most validity to answer the research questions that have their origin in the wording and purpose of the GDPR and herein lies the systemization and describing of the GDPR. Metaphors and alike will be used to conceptualize theories through practical examples. Due to the nature of the subject, it is deemed necessary to seek guidance from sources that are not derived from the classical sources of law. Therefore, the thesis will use the method that Sandgren describes as the legal analytic method. The method will be used to analyze expert’s opinions, research papers and sources that are derived from relevant fields, to complement the potential inadequacies concerning the relation between the GDPR and blockchain technology. The analysis will result in a critical assessment concerning the relation between the GDPR and blockchain technology to be able to identify the faults and how these faults can be mended.

## **1.4 Material**

The technological aspects presented acts as the premises of the thesis. A description of the technological aspects of the blockchain is not available through the classical legal sources and will, therefore, be assessed and explained through Computer Science-, IT- and other relevant scientific articles, books and relevant material, to provide the required understanding of the technological aspects to be able to discuss them out from a legal point of view. Due to

---

<sup>36</sup> Winter, S. (2001). A clearing in the forest. Chicago: University of Chicago Press, p. 65.

<sup>37</sup> Solove, D. (2004). The Digital Person: Technology and Privacy in the Information Age. New York University Press, New York, p. 28.

<sup>38</sup> Lakoff, G. and Johnson, M. (1980). Metaphors we live by. Chicago: University of Chicago Press, pp. 145-146.

<sup>39</sup> Solove, D. The Digital Person, p. 28.

blockchain being a fairly new technology, the absence of extensive research by scholars require that certain non-traditional sources, like internet sources, be weighed in with caution. This is done to gain a broader underlay which in turn satisfies the interest for further knowledge in an area which is embossed by speculation.

Thereafter, the technological aspects will be analyzed and assessed considering the presented provisions in the General Data Protection Regulation 2016/679 (GDPR), by assessing the systematical and terminological structure of the regulation. When uncertainties regarding the GDPR's application on the blockchain arises, such uncertainties will be assessed and examined through other traditional legal sources by flagging for the purposes and aims through case law, doctrine and the preparatory work. When such an assessment is not enough to please the interest for further knowledge, other sources may be weighed in with carefulness. An explanation of the material used in the thesis and the validity of such material will follow below.

Relevant judgements from the Court of Justice of the European Union (CJEU) will be mentioned to highlight the objectives of data protection and privacy legislation within the EU. Even though such judgements have not been decreed with the GDPR as their outset, the cases that are used in this thesis are very recent and align with the goals of the GDPR.

Also, it is of importance to highlight that certain instruments mentioned in this thesis do not have a legally binding authority in the strict sense.<sup>40</sup> Such an instrument is the Article 29 Data Protection Working Party (A29WP).<sup>41</sup> The A29WP was established to encourage data protection and integrity within the EU by providing opinions, working papers, documents and recommendations and consists of representatives from each member states data protection authorities. Even though the A29WP is not a legislative body, nor do they represent the European Commission, they provide the European Commission with independent advice that is highly regarded and valued when developing and harmonizing policies for data protection within the EU and can be referred to as soft law.<sup>42</sup>

When the GDPR, case law, doctrine, preparatory work and soft law do not suffice when assessing a problem, online sources, such as journals, articles and forum posts by individuals and organizations working in relevant fields, such as data protection or law, will be weighed in deliberately to satisfy the interest for further knowledge and to aid in clarifying uncertainties.

---

<sup>40</sup> Greenstein, *Our Humanity Exposed*, p. 38.

<sup>41</sup> Data Protection Working Party established by Article 29 of Directive 95/46/EC.

<sup>42</sup> European Data Protection Supervisor. (2018). A - European Data Protection Supervisor. [online] Available at: [https://edps.europa.eu/data-protection/data-protection/glossary/a\\_en](https://edps.europa.eu/data-protection/data-protection/glossary/a_en) [Accessed 20 Apr. 2018].

Such sources are not given any validity under the classical sources of law and merely act as an addition to the classical sources of law and are used accordingly.

## 1.5 Terminology

Certain terminology used in the thesis will need further clarification to avoid confusion. A *node* or *user* is a single system user on a P2P-network, often a single computer.<sup>43</sup> Nodes will be referred to as individual computers on a P2P-network in this thesis. A *P2P-network*, also referred to as a *distributed network*, is a means for nodes to communicate with each other, without any central point of connection.<sup>44</sup> The term *blockchain*, sometimes referred to as *system*, is used in this thesis as an umbrella term for the P2P-network and the list of records that is used to ensure trust and integrity on a P2P-network, which in turn consists of the following components. *Blockchain technology* refers to the underlying computational and mathematical models that are utilized for the blockchain to function. The term *blockchain-data-structure* refers to the structural manner of how data is stored on the blockchain in a secure and immutable fashion. *Immutable* means that an object cannot be changed or altered. The blockchain-data-structure makes it possible to maintain a list of transaction data in an on-going fashion, this list mimics a register and is commonly referred to as a *ledger* and each node on the blockchain maintains their own ledger by utilizing the structural foundation of the blockchain-data-structure. *Open distributed blockchain* refers to a P2P-network that is open for everyone to join, which distributes the ledger to all nodes. A *block* is an individual package containing data and when chained together with other *blocks* they form the blockchain. A *block header* is the block at the end of the chain. There are also certain validation rules concerning data that is to be stored, defined by the *blockchain algorithm*. An *algorithm* is a collection of instructions for the computer that are executed in a specific order to reach the intended outcome.<sup>45</sup> The term *hash function* refers to an algorithm that turns a text of arbitrary length into a non-readable text of fixed length, known as a *hash-value*.<sup>46</sup> The term *hash reference* refers to pointing to a specific hash-value. A *hash puzzle* is a computational problem that is to be solved when appending new blocks to the blockchain-data-structure, the process of solving such puzzles is referred to as *mining*.<sup>47</sup> A *Merkle tree* is a hierarchical way of storing transaction data in a sensitive manner

---

<sup>43</sup> Morabito, V. (2017). Business Innovation Through Blockchain The B<sup>3</sup> Perspective. Cham: Springer International Publishing, p. 7.

<sup>44</sup> Ibid., p. 3.

<sup>45</sup> Farrel, J. (2013). A Beginner's Guide to Programming Logic And Design: Comprehensive. 7<sup>th</sup>. ed. Course Technology, Cengage Learning, p. 9.

<sup>46</sup> See section 2.2.1.

<sup>47</sup> Mougayar and Buterin, The Business Blockchain, p. 36.

using hash functions.<sup>48</sup> The art of *cryptography* is a discipline in mathematics that refers to turning information into an unreadable format by using a key, while still being able to reverse the process and turn the unreadable information into the readable information, and is divided into *symmetric*, where only one key is used, and *asymmetric*, where two keys are used.<sup>49</sup> A *Private key* and a *Public key* refers to the two separate keys that are used in asymmetric cryptography, a private key held by an individual and a public key held by the counterparty/parties.

## **1.6 Disposition**

The thesis consists of five chapters which are ordered to give structure and understanding, as well as answer the research questions stated above. Following this introduction, chapter two explains the blockchain and the underlying technological components. Chapter three will outline and explain relevant articles in the GDPR, primarily what personal data is and how personal data is to be processed under the GDPR. Chapter four will examine the correlation between the blockchain and the GDPR by assessing the actors on the blockchain, personal data on the blockchain, processing on the blockchain and responsibility on the blockchain. Lastly, chapter five will consist of the writer's conclusions.

---

<sup>48</sup> See section 2.3.3.1.

<sup>49</sup> See section 2.2.4.

## 2 Blockchain Technology

Most people have heard or read about the blockchain due to Bitcoin and its explosive growth. For many, the term blockchain is synonymous with Bitcoin and the underlying technology is either forgotten or falls between the cracks as it can seem daunting, difficult and distant. This chapter seeks to clarify and simplify the key concepts in the blockchain and exemplify how it works, using real-world examples.

Bitcoin and other similar technologies are distributed and open blockchains, which implies that the contents are shared over P2P-networks, where instead of acting through middlemen, people can act directly with their peers, hence the term peer-to-peer.<sup>50</sup> Banks are an example of a middleman service, where all accounts are centrally registered and all transactions move through the bank. Different banks in different countries cause transactions to be expensive and time-consuming.<sup>51</sup> On a P2P-network there is no centralized entity, instead transactions move directly from peer-to-peer, minimizing cost and time. The openness insinuates that the data being transacted on the blockchain is publicly viewable and that anyone can join and make their own transactions. The blockchain itself refers to a way of ensuring integrity on P2P-networks that are open to everyone.<sup>52</sup> Therefore, the main components of the blockchain are the P2P-networks that are used to communicate in a decentralized manner and the blockchain ledger itself, that ensures integrity in the absence of a middleman to do so. These concepts will be examined and explained in this chapter.

### 2.1 Breaking the Blockchain Into Pieces

The true difference between centralization and decentralization is that a centralized model assumes central control by an authority while a decentralized model assumes no control.<sup>53</sup> There is also the element of architectural (de)-centralization where a classical solution, like a bank, has one connecting point that unifies all nodes in the system, making it centralized. The blockchain, on the other hand, utilizes a P2P-network with no central point of failure, that connects all nodes with each other in a web-like fashion, making it architecturally decentralized.<sup>54</sup>

---

<sup>50</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 20.

<sup>51</sup> Ibid., p. 21.

<sup>52</sup> Ibid., p. 24.

<sup>53</sup> Medium. (2018). The Meaning of Decentralization – Vitalik Buterin – Medium. [online] Available at: <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274> [Accessed 18 Apr. 2018].

<sup>54</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 11.

Figure 1

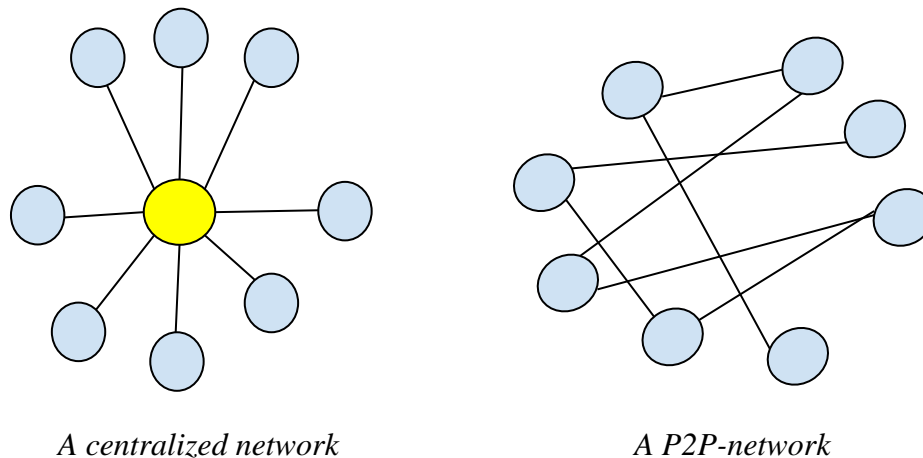


Figure 1 illustrates how a P2P-network looks compared to a centralized network.

These P2P-networks interact very similarly to how social groups of humans interact.<sup>55</sup> Imagine that each node in the system represents a human. Humans communicate with each other by using spoken or written word, so one could say that language is our medium. The biggest connector of computers that exists to date is the internet, why a P2P-network most likely would use the internet as their communication medium. The nodes on said P2P-network are identified by a unique address, they can connect or disconnect to the system as they like, they maintain an independent list of peers that they communicate with and they send messages to peers over the internet by their unique addresses.<sup>56</sup>

P2P-networks are not exclusive to the blockchain and have existed for a long time. Open P2P-network have their advantages but have also had their faults. The users of these distributed systems have not been able to deter scams, like double spending. Double spending refers to using a currency token more than once and centralized models have tackled double spending by e.g. making physical money hard to copy.<sup>57</sup> Without proper security measures, digital currency tokens are easily copied and double spent which is why the centralized data-handling model has been more attractive in the past. That is until the creation of Bitcoin in 2008. The technology provided a solution for the so-called double spending problem by using a mathematical model to ensure the integrity of the system.<sup>58</sup> This meant the start of technologies

---

<sup>55</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 146.

<sup>56</sup> Ibid., p. 147.

<sup>57</sup> Pérez-Sol'a, C., Delgado-Segura, S., Navarro-Arribas, G. and Herrera-Joancomart', J. (2018). Double-spending Prevention for Bitcoin zero-confirmation transactions. [online], p. 1. Available at: <https://eprint.iacr.org/2017/394.pdf> [Accessed 12 May 2018].

<sup>58</sup> Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system [White paper], p. 1. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 18 Apr. 2018].

being developed on the blockchain, relying on the toolset for achieving integrity while also utilizing the benefits of P2P-networks.

Different blockchain technologies serve different purposes. For this example, we are going to assume a blockchain that manages ownership, one of the most common blockchain-models that boils down to proving what data belongs to whom in the most transparent and trustworthy way possible.<sup>59</sup> Not all blockchains are alike and the example is a generalization of the most commonly used technologies. The blockchain consists of several complex elements that will be broken into the following segments to make it as pedagogical as possible: (1) Describing ownership, (2) Protecting ownership from unauthorized access, (3) Storing data consisting of transactions (ledgers), (4) Preparing these ledgers to be distributed in an untrustworthy environment, (5) Forming a system of these ledgers, (6) Adding new transactions to the already existing ledgers and (7) Deciding what ledgers most accurately represent the truth.

## 2.2 A Technical Detour

To understand how the blockchain works a deeper understanding of several mathematical and computational processes is required. What follows is a simplified explanation of the concepts on which the foundation of the blockchain is built upon.

### 2.2.1 Hash Functions

One of the most foundational concepts in ensuring the blockchains integrity, therefore protecting ownership from unauthorized access, is ‘hash functions’, also known as ‘hashing’. Hashing is when one transforms a text of arbitrary length into a text of fixed length, the transformed text is known as a ‘hash-value’.<sup>60</sup> These are used to create a digital fingerprint for data without publishing the data itself and are commonly used in digital signatures.<sup>61</sup>

Figure 2

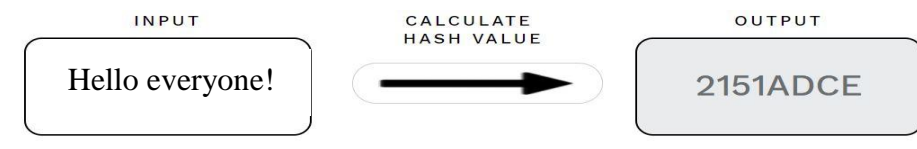


Figure 2 illustrates how a hash function looks in practice.<sup>62</sup> The underlying algorithm is different for every hash function and consists of complex mathematics. The hash function transform text into a fixed length of text and numbers and is case sensitive, even the slightest change alters the hash-value into a completely different value.

<sup>59</sup> Mougayar and Buterin, The Business Blockchain, p. 19.

<sup>60</sup> Menezes, A., Van Oorschot, P. and Vanstone, S. (1997). Handbook of applied cryptography. Boca Raton: CRC Press, p. 33.

<sup>61</sup> Ibid.

<sup>62</sup> Blockchain-basics.com. (2018). Hashing. [online] Available at: [http://blockchain-basics.com/Hashing.html?hash\\_input=Hello+everyone%21](http://blockchain-basics.com/Hashing.html?hash_input=Hello+everyone%21) [Accessed 16 Apr. 2018].

Figure 3

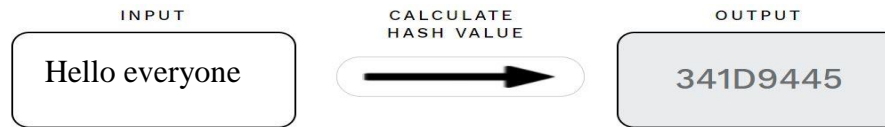


Figure 3 illustrates the same hash function, only, one character has been changed compared to Figure 2.<sup>63</sup> The hash-values are entirely different even though the input difference is minuscule, illustrating the sensitivity of hash functions and how two similar sentences or texts make up a completely different cryptographic hash-value.

These hash functions can be used to see whether data has been altered. I.e. if data is changed, the hash-value corresponding to that data will also change, thereby reflecting that the data has been tampered with.

### 2.2.2 Hash References

Hash references utilize the uniqueness of hash-values illustrated in the previous segment and are vital for the blockchain. A hash reference can be described as a reference to a specific hash-value.<sup>64</sup> To simplify references, imagine that the hash-value is a coat in a coat room and the reference is the coat check ticket. To identify a coat, the matching coat check ticket is required. If the value on the ticket were changed, it would not refer to the specific coat, breaking the reference.<sup>65</sup> References in computer systems work the same way, they point to a physical location where the given data is supposed to be stored and if the hash-value is changed the reference does not point to the specific data anymore.

It is possible to create a chain of hash-values and references. In such a chain, one piece of data also contains the hash reference to the previous piece of data, forming a chain of linked data.<sup>66</sup>

To simplify, it would look something like this:

Figure 4



Figure 4 illustrates how data can be linked by organizing it in a chain-like manner.<sup>67</sup> By doing so, one is able to retrace back to DATA1 by only knowing REF.DATA 3 as these are chained together. Due to the sensitivity of hash-values, by chaining hash-values like above, an alteration in the illustrated chain would be easily recognizable as the reference no longer points to, for example, DATA1, because of the alteration, breaking the linked chain.<sup>68</sup>

<sup>63</sup> Blockchain-basics.com. (2018). Hashing. [online] Available at: [http://blockchain-basics.com/Hashing.html?hash\\_input=Hello+everyone%21](http://blockchain-basics.com/Hashing.html?hash_input=Hello+everyone%21) [Accessed 16 Apr. 2018].

<sup>64</sup> TutorialsPoint. (2018). Perl Basics: Perl References. [online] Available at: [https://www.tutorialspoint.com/perl/perl\\_references.htm](https://www.tutorialspoint.com/perl/perl_references.htm) [Accessed 16 Apr. 2018].

<sup>65</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 83.

<sup>66</sup> Cormen, T., Leiserson, C. and Rivest, R. (2014). Introduction to Algorithms. Cambridge: MIT Press, p. 236.

<sup>67</sup> Lee, D. and Deng, R. (2017). Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2: ChinaTech, Mobile Security, and Distributed Ledger. Academic Press, pp. 1-3.

<sup>68</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 88.

### 2.2.3 Hash Puzzles

These hash-values and hash references also pose the opportunity of creating ‘hash puzzles’, problems that require computational power to be solved, a key element of an open distributed blockchain.<sup>69</sup> A deeper explanation of hash puzzles require some technological knowledge and is not essential for the understanding of the blockchain, the concept is, however essential for the understanding. The puzzles are time-consuming computational problems that cannot be solved in any other way than by trial and error, like solving a lock combination by trying all possible combinations until the lock is opened. The hash puzzles are solved by the nodes on the blockchain and will be discussed further in section 2.3.4.

### 2.2.4 Asymmetric Cryptography and Digital Fingerprints

The blockchain also utilizes a mathematical cryptographic model called asymmetric cryptography, also known as public-key cryptography, which makes it possible to read encrypted data by using a key, unlike hash puzzles that only are solvable by computational power. Asymmetric cryptography involves using two sets of keys, one to encrypt the data, i.e. turning it into something unreadable, and another key used to decrypt said data, turning it into something readable, unlike symmetric cryptography that uses one key for encrypting and decrypting.<sup>70</sup>

Figure 5

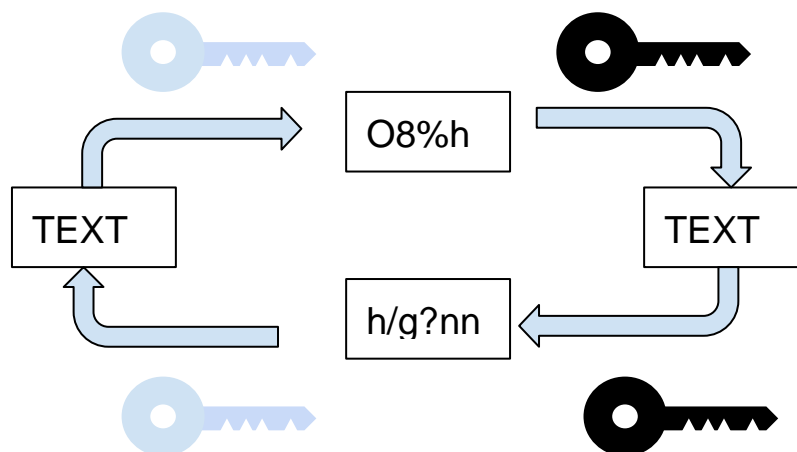


Figure 5 illustrates asymmetric cryptography. Using one of the keys the data is encrypted into something completely different and using the other key the encrypted data can be decrypted.

If, for example, Alice wanted to send an encrypted message to Michael, using symmetric cryptography they would both use the same key to encrypt and decrypt the message. This would,

<sup>69</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 89.

<sup>70</sup> Ibid., p. 97.

on an untrusted network like the blockchain, be very impractical as it requires that each individual user must share a symmetric key with every other user to be able to send authenticated messages and transactions.<sup>71</sup> Instead, asymmetric cryptography can be used in untrusted networks to send messages and can also be utilized to uniquely identify users and authenticate transactions.<sup>72</sup> On the blockchain, an individual key, a ‘private key’, is given to every unique user. A key-pair to that specific private key is given to everyone else on the blockchain, the so-called ‘public key’. By using the public key, Michael, or anyone else with the key for that matter, can send Alice a secret message, but only Alice can decrypt the message using her private key and the same applies if Alice wishes to send a message to someone using her private key as only the corresponding public key can be used to decrypt the message.<sup>73</sup>

### **2.2.5 Digital Signatures**

Digital signatures combine the previously mentioned concepts into the digital equivalent of a handwritten signature. The digital signature is used to authorize, verify and identify fraudulent transactions. This is done by combining the data that is to be authorized with a digital signature. If someone wanted to send a message to the world saying: “Hello everyone!” and have them know that they authorized this message they would start by hashing the message. As previously illustrated, using a certain hash function, the hash-value would be 2151ADCE. They would then encrypt the hash-value using their private key, resulting in another random string of text, let’s say 123456789. The text “Hello everyone!” and their signature 123456789 are then stored in a file that constitutes their digitally signed message to the world.<sup>74</sup> To verify that it was them who sent this message the world would use their public key connected to the private key to decrypt the signature, 123456789, resulting in 2151ADCE, and would then hash the text “Hello everyone!”, resulting in 2151ADCE. If the values match, it is an authorized message and if the values do not match, the message is deemed fraudulent.

## **2.3 The 7 Steps**

With a basic understanding of the underlying mathematical and cryptographical models it will be easier to understand how the blockchain ensures ownership through transparency and trust. How this is done in practice will be explained in the seven following steps.

---

<sup>71</sup> Paar, C. and Pelzl, J. (2010). Understanding cryptography. Berlin: Springer, p. 150.

<sup>72</sup> Romano, D. and Schmid, G. (2017). Beyond Bitcoin: A Critical Look at Blockchain-Based Systems. Cryptography, 1(2), p. 12.

<sup>73</sup> Smart, N. (2016). Cryptography Made Simple. Cham: Springer International Publishing, p. 202.

<sup>74</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 105.

### **2.3.1 Describing Ownership**

Ownership is the proof of something being one's property. Certain governmental agencies keep records of belongings. For example, The Swedish Patent and Registration Office, a centralized governmental agency, keeps records regarding ownership of intellectual property. As for the private sector, there are banks that keep records of money in people's accounts. These records are there to ensure that a person's property is connected to them. Classical models, like these, use so-called 'inventory data', which is a list of current possessions of a certain person. The blockchain has a unique way of identifying ownership, instead of keeping records that portray the current state of ownership, the blockchain maintains a list of transaction data in an on-going fashion, also known as a 'ledger'.<sup>75</sup>

Imagine a relay running race that is forever on-going, seeing who currently has the baton in their possession is easily done by looking at whom the previous exchange was made to. In this example, the owned property is the baton and the runner is the person with the property in their possession.<sup>76</sup> Data of these transactions are kept in a ledger that acts as an audit trail that provides evidence of how everyone achieved his or her possession.<sup>77</sup> Every transaction is basically recorded as who hands off ownership to whom and when the ownership is handed off. Therefore, the necessary information to make such a transaction is an identifier of the account that is to hand of ownership as well as for the receiver, a specification of the goods being transacted, the time of said transaction, payment to the system for executing the transaction as well as proof of ownership of the account that hands off the ownership.<sup>78</sup> It is important that the ordering of the transaction data in the ledger is correct since the history of transfers is an indicator of ownership at a given point in time. Another element that is essential to ensuring trust in the blockchain is the integrity of said ledger, because if anyone can modify the ledger to portray ownership in their favor, the blockchain is rendered useless. The blockchain must, therefore, provide security measures to ensure that only authorized and valid transactions are added to the ledger, in order to avoid unauthorized access.

### **2.3.2 Protecting Ownership from Unauthorized Access**

An open distributed blockchain is open to everyone. Unlike the patents that are kept by a centralized agency that secures ownership from unauthorized access, everyone can transfer and

---

<sup>75</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 1.

<sup>76</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 63.

<sup>77</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 1 ff.

<sup>78</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 65.

submit data to the blockchain. Hence, measures to ensure that only a lawful owner of data can transfer the ownership are required.<sup>79</sup> The use of digital signatures ensures authorized transactions through signing and verification of transactions. By signing a transaction, the owner of the data states agreement with the transaction, as the owner is the only one who can create such a signature.<sup>80</sup> The signing of a transaction requires (1) that the owner describes information regarding the transaction, such as the involved account numbers, (2) states the amount being transferred, (3) that the owner creates a hash-value of the transaction data, (4) that the owner encrypts the hash-value with their private key and (5) that the owner adds the encrypted hash-value to the transaction.

The product of this is a digitally signed transaction, that can be verified by (1) creating the hash-value of the data being transacted, excluding the encrypted hash-value, (2) decrypting the encrypted hash-value and (3) comparing the hash-value with the decrypted value, if they match, the owner has authorized the transaction, if not, the transaction is deemed fraudulent.

### **2.3.3 Storing Transaction Data**

Storing authenticated transactions in a historically accurate and secure fashion requires certain steps to be taken. As previously discussed, hash references form a chain-like data-structure, which poses the opportunity of maintaining a ledger in a sensitive manner that preserves the order in which the transactions were added.<sup>81</sup> The ledger poses two questions of interest, namely, what the data-structure looks like and how new transactions are added to the ledger.

#### **2.3.3.1 Data-structure**

The data-structure of the blockchain is not completely different from that of an old-fashioned library card catalog where each card has a reference to a book that is being stored somewhere in the library. Only, instead of the cards following a chronological order they would reference the previous card, creating a chain of cards, which depicts a more accurate picture of the blockchain-data-structure. The blockchain-data-structure is built on the following elements: a block header, a reference to the previous block header and transaction data contained in a tree-like structure. These components make up one block, while many blocks, in turn, make up the blockchain.<sup>82</sup>

---

<sup>79</sup> Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, p. 104.

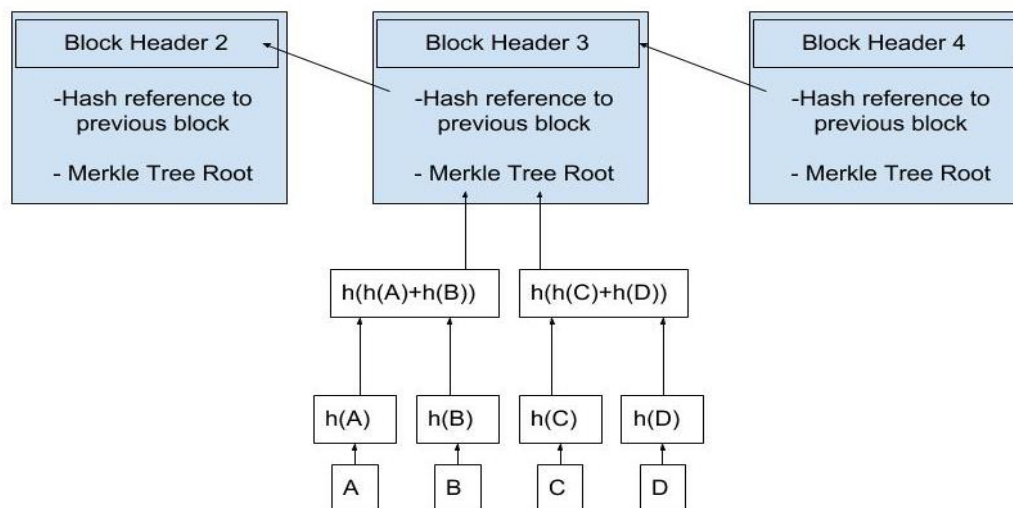
<sup>80</sup> Mougayar, W, and Buterin, V, *The Business Blockchain*, p. 27.

<sup>81</sup> Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, p. 112.

<sup>82</sup> Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, p. 4.

Block headers serve the purpose of uniquely identifying a block and are the hash-values of the data being maintained in the block they are header for. Each block contains its own block header as well as a reference to the preceding block, consequently forming a chain of block headers.<sup>83</sup> If you know what the last block in the chain is, you will always be able to trace through the whole chain since each block contains a reference to the previous one. Each block also stores a hash reference to the transaction data being maintained by the block.<sup>84</sup> The hash-reference points to the root of a 'Merkle tree', which is how transactions are stored within the blockchain.<sup>85</sup> The Merkle tree is a so-called 'hash tree', which is a structure consisting of several hash-values being combined to finally form a single hash-value, the root of the hash tree. At the bottom of the tree, we have the actual transaction data that is hashed into a hash-value. This hash-value is then concatenated, which means that two strings are combined to form one string, with a hash-value at the same height.<sup>86</sup> The concatenated string of the two hash-values is then hashed, forming a new hash-value placed one level higher in the hierarchy. This process continues until the root of the Merkle tree is reached, which is then put into the block as a reference.

Figure 6



*In Figure 6, A, B, C and D are all transaction data. The data is hashed using the  $h(X)$  function. The hash-values of said transaction data are then hashed once again after being added together with another transaction data's hash-value. This continues until the root of the tree is reached, which is then referenced in the block. By having the block headers in the chain identified by their hash-values and by them containing a reference to the previous block header by their hash reference the order of the blocks is preserved and therefore historically accurate.*

<sup>83</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 120.

<sup>84</sup> Ibid.

<sup>85</sup> Merkle, R. (1980) "Protocols for public key cryptosystems" In: Symposium on Security and Privacy, IEEE Computer Society, April 1980, pp. 122-133.

<sup>86</sup> Medium. (2018). Merkle Tree Introduction – Evan Kozliner – Medium. [online] Available at: <https://medium.com/@evankozliner/merkle-tree-introduction-4c44250e2da7> [Accessed 19 Apr. 2018].

### 2.3.3.2 Adding and Changing Transaction Data

It takes a great amount of computational power to alter transaction data since tracing one step back from a hash-value requires solving a complex hash puzzle. Therefore, changing transaction data would require altering every single reference in the chain, since even the smallest change would render the chain of references completely useless. This is intentionally made into an elaborate process to keep the data-structure consistent and to maintain its integrity.<sup>87</sup> Satoshi Nakamoto explains this in the following way:

*“Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.”<sup>88</sup>*

To add new transaction data to the blockchain one would have to append this to the head of the blockchain, meaning the hash reference to the preceding block in the chain.<sup>89</sup> The adding of data is done in three steps; (1) Creating a new Merkle tree that contains all the new transactions to be added, (2) creating a new block header that contains the hash reference to the preceding block header and the root of the Merkle tree, which contains the transaction data from step 1, and lastly, (3) the creation of a new hash reference to our recently created block which now constitutes the head of the blockchain, to which a new block will be added, and so on.<sup>90</sup>

### 2.3.4 Preparing Ledgers to be Distributed in an Untrustworthy Environment

Hash puzzles were briefly discussed in section 2.2.3, and it was mentioned that hash puzzles make it possible to impose computational costs for the altering of data. As illustrated in the previous section, the adding of a block is not computationally expensive. To make a blockchain-data-structure immutable this process must be computationally expensive to be able to distribute such ledgers in an untrustworthy environment.<sup>91</sup> In an untrustworthy environment, the possibility of relying on cryptographic proof poses the opportunity of making the structure immutable.<sup>92</sup> This requires certain criteria to be added to the process of appending the blockchain-data-structure with a new block, resulting in the block header including additional data.<sup>93</sup> Such additional data imposes a hash puzzle on each block header, and in order to be able

---

<sup>87</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 132.

<sup>88</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 4.

<sup>89</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 124.

<sup>90</sup> Ibid.

<sup>91</sup> Ibid., p. 139.

<sup>92</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 1.

<sup>93</sup> Okupski, K. (2016). *Bitcoin Developer Reference Working Paper* [White paper], p. 5. Available at: [https://lopp.net/pdf/Bitcoin\\_Developer\\_Reference.pdf](https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf) [Accessed 19 Apr. 2018].

to add a new block, one must solve said puzzle, which costs computational power. The way the hash puzzles are implemented also ensures that the order of in which the transactions are added are in fact correct. The process of solving said puzzles and appending the blockchain with new blocks is most likely a familiar term to most people following the sudden cryptocurrency explosion, the process is commonly referred to as *mining*.<sup>94</sup>

### **2.3.5 Recap Heretofore**

The security and integrity of the blockchain originates from its unique utilization of hash-values and references. First and foremost, all transactions are digitally signed by the lawful owner when transferring ownership. Such transaction data is bundled together with other transaction data and a hash-value is created out of their combined hash-values. The combined hash-value is then put into the newly created block along with a reference to the previous block. Each block in the blockchain contains a set amount of transactions and after those transactions are filled a new block is created and appended with transactions, creating an ever-changing ledger. The adding of a new block requires computational power and the solving of a hash puzzle. Since hash references are case sensitive, even the smallest alteration of the transaction data in any of the blocks renders the chain useless because the hash-value that is referenced no longer exists, therefore breaking the chain. The next steps will clarify how such a ledger can be utilized in a system.

### **2.3.6 Forming a System of the Ledgers**

On a P2P-network the nodes engage in three different kinds of communication: (1) small talk that upholds relationships, (2) sharing of news among peers and (3) introducing new peers into the group, which requires some sort of initiation rite and sharing of the group history.<sup>95</sup> Point (1), small talk, is done by sending small messages to other nodes and serves the purpose of maintaining a correct list of peers on the network, due to nodes being able to disconnect from the P2P-network at any given time. The individual list that each node maintains does not constitute all nodes, but rather a small subgroup. Combined, all subgroups make up the entire P2P-network. Point (2) is the actual purpose of the system, the sharing of transaction data and blocks that are to be added to the blockchain-data-structure. This is done in a gossip-like fashion where all nodes forward information to each node on their maintained list until every node on the system has received the information. This kind of information is shared as it occurs and if

---

<sup>94</sup> Okupski, *Bitcoin Developer Reference Working Paper*, p. 36.

<sup>95</sup> Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, p. 147.

a node reconnects to the system it will receive all transaction data and blocks that have been forwarded during the time they were disconnected. Point (3) indicates that when a new computer wishes to join the P2P-network it sends out requests to nodes already on the system, the responding nodes add the computer to their maintained list and send a confirmation message upon which the computer becomes a node in the P2P-network. To become a reliable and full-fledged node, a copy of the whole up-to-date blockchain-data-structure is transferred to the node. The communication ensures that the information is spread correctly and that new peers can join the system easily, thus increasing the size and processing power of the network.

### **2.3.7 Adding Transactions to the Ledger**

Transactions that are added to the ledgers being upheld by nodes should be verified and validated. When exactly everyone, even the most dishonest person, can add transaction data to the blockchain-data-structure, managing the integrity of said structure requires that all nodes also have a form of supervisory function. The nodes supervise that their peers add valid and authorized transactions and reward them for doing so, while nodes that detect errors in transactions also are rewarded, creating an incentive to both add correct transactions to scout for errors in transactions.<sup>96</sup> Therefore, the nodes require a certain set of instructions on how to define correctness and wrongfulness when it comes to transactions and are guided by the blockchain algorithm that enforces validation rules for transaction data and validation rules for block headers.<sup>97</sup> The transaction rules are individual for each blockchain as they have different goals, but they have the common goal of encompassing correctness and authorization. The block header rules are agnostic of the correctness of transaction data, as the transactions already have been validated and added to the block. Block header validation is focused on the verification of the hash puzzle, as discussed in section 2.3.4. Only blocks whose block header contains a solution for its hash puzzle passes the validation.<sup>98</sup>

The blockchain effectively adds blocks to its data-structure by engaging all the nodes in a form of competition where the end goal is to receive compensation for one's work or punishment if someone counteracts the integrity of the system. The blockchain algorithm consists of computer code that instructs how the nodes are to execute certain functions to achieve the abovementioned result. This is done effectively by having new transaction data and blocks forwarded in the gossipy fashion among the nodes, as mentioned in section 2.3.5. The node

---

<sup>96</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 3.

<sup>97</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 156.

<sup>98</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 3.

collects the transaction data they receive and validates it. The validated transaction data is then put into a Merkle tree by the node with which the node starts creating a new block by solving its hash puzzle. When the hash puzzle is solved the block has been created and is sent out to all other nodes. If a node sends out a finished block, all other nodes stop their processes and validate the block with the highest priority by verifying that the solution for the hash puzzle is correct and by verifying that the underlying transaction data meets the validation requirements. When a node has validated a block, it is added to the individual ledger being upheld by the node and sent forward to the other nodes. The receiving nodes then remove all transactions that are in that block from their own list of processing and move on to validate other transactions or blocks. The node that created the accepted block will receive the fee for all the transactions in said block. Blocks that are invalid will not be added to the structure and are instead discarded.<sup>99</sup>

And this is mining, the part of the blockchain algorithm and data-structure that can earn you so-called tokens or cryptocurrencies. The reward is a digital asset whose ownership is managed by the blockchain itself and is a form of payment to the node for contributing to the integrity of the blockchain-data-structure. This engages the nodes in a sort of carrot and stick competition where the nodes compete both in speed and quality, where peer control through the computational power of the masses is the judge.<sup>100</sup>

### **2.3.8 Choosing the Ledger that Represents the Truth**

When sending out transactions to other nodes on the P2P-network it is a certainty that some nodes will pertain different versions of the blockchain-data-structure in their personal ledgers due to the news not reaching them yet. This could potentially be used by attackers to undermine the blockchain-data-structure, but the blockchain algorithm is created with the task of not letting this happen. The longest or heaviest chain (depending on the blockchain-type) serves as proof that the majority of the computing power from the nodes was used to create that chain, and is therefore deemed the ledger that represents the truth.<sup>101</sup> If more computing power is dedicated to validating blocks instead of attacking the blockchain data-structure, it's integrity is secure. An attacker would have to pace back through all previous blocks consisting of transactions since the only way of breaching the blockchain is by brute force and there is not enough

---

<sup>99</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 162.

<sup>100</sup> Bits on blocks. (2018). A gentle introduction to immutability of blockchains. [online] Available at: <https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/> [Accessed 19 May 2018].

<sup>101</sup> Nakamoto, Bitcoin: A peer-to-peer electronic cash system, p. 1.

processing power to brute force blockchain-data-structures of the magnitude we see today.<sup>102</sup> Since all nodes validate blocks individually, as discussed in section 2.3.6, the nodes accept validated blocks and add them to their ledger and start appending the blockchain-structure with the newly validated block. As all nodes do this individually a comparison of ledgers will always reveal the truthful ledger, i.e. the longest ledger, since the most process power was devoted to this one and most nodes validated and started appending that blockchain-data-structure. Imagine that the nodes partake in a hypothetical voting schema to collectively decide what ledger represents the truth, where the individual blockchain-data-structure being upheld by individual nodes is the vote.

## **2.4 Blockchain Summary and Relevance**

This concludes the section on the underlying aspects of blockchain technology. The blockchain is nearly, if not completely, immutable due to the underlying data-structure combined with the computational power of the masses. Nodes keep an individual copy of the ledger and compare the individual copies to one another to reach consensus regarding the truthful ledger. The nodes also validate blocks and transactions and search for fraudulent transactions using cryptographic hashing and hash-puzzles, which creates a monetary incentive to provide processing power to the blockchain. The goal of the blockchain is to guarantee ownership through transparency and openness by utilizing collective mathematical assurance. The blockchain can be used for many things and the ledger being upheld can take many forms. However, an open distributed blockchain will always consist of several users that maintain their own copy of a ledger that contains every block, which in turn contains transaction data. But how is any of this of relevance to the GDPR? As mentioned, every single node receives, processes and stores transactions. It, of course, depends on the function of the specific blockchain, but one thing is guaranteed, some transaction data will be personal data as defined in the GDPR. Since the GDPR does not exclude any technology, blockchain technology does not fall outside of its reach. The question is how to define the specific actors within the blockchain under the key provisions in the GDPR. To be able to do this we shall first assess the key provisions.

---

<sup>102</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 177.

### 3 The GDPR

The GDPR, described as the “start of a new era within data security”, introduces new concepts and codifies existing EU case law.<sup>103</sup> The GDPR acknowledges that the technological development can result in certain privacy-related risks for individuals and introduces material obligations for the responsible parties and extends the rights and freedoms of the individual.<sup>104</sup>

When discussing the GDPR it is always important to assess two key components. Namely, in what cases does the regulation apply and to whom does the regulation apply? The regulation’s material scope applies to any processing of personal data.<sup>105</sup> The GDPR applies to anyone, regardless of legal entity, that processes or controls the processing of personal data.<sup>106</sup> Therefore, it is essential for the understanding of the GDPR to gain insight into these definitions.

#### 3.1 Personal Data

Personal data is the core of the GDPR and is the protected property by the provision, referring to the so-called ‘data subject’.<sup>107</sup> The word data refers to electronically stored information, signs or indications.<sup>108</sup> Data, in itself, does not fall within the scope of the regulation, it must be ‘personal’ to do so. The GDPR states that information relating to an identified or identifiable natural person can be defined as personal.<sup>109</sup> Therefore, data is personal if it is directly or indirectly possible to identify a natural person by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological genetic, mental, economic, cultural or social identity of that natural person.<sup>110</sup> Under Article 4(1) in the GDPR it is possible to define information that in itself would not be deemed personal data but, when combined with other information, can be deemed personal data. There is also no clear definition of who is to be able to identify the natural person from the given data, meaning that the complementary information need not necessarily be in

---

<sup>103</sup> Holtz, M. (2018). Den nya allmänna dataskyddsförordningen — några anmärkningar, SvJT, p. 240.

<sup>104</sup> Nicolaidou, IL. and Georgiades, C. (2017) “*The General Data Protection Regulation: A Law for the Digital Age*”. In: Synodinou, TE., Jougoux, P., Markou, C. and Prastitou T. (eds.), EU Internet Law. Springer, Cham, p. 8.

<sup>105</sup> Article 2(1) in the GDPR

<sup>106</sup> Voigt, P. and Bussche, A. (2017). The EU general data protection regulation (GDPR). Cham: Springer International Publishing, p. 17.

<sup>107</sup> Article 4(1) in the GDPR.

<sup>108</sup> Voigt and Bussche, The EU General Data Protection Regulation, p. 11.

<sup>109</sup> Article 4(1) in the GDPR.

<sup>110</sup> Ibid.

possession of the data controller/processor.<sup>111</sup> Also, The GDPR expands upon the act of pseudonymizing, which is a technique used to enhance privacy by separating information that allows data to be attributed to a specific person.<sup>112</sup> Pseudonymizing is not meant to make it impossible for someone to derive a natural person from the data, only make it more difficult. Therefore, account should be taken of all the means likely to be used to try to single out a natural person from the pseudonymized data, weighing in all objective factors like cost, time required for identification and available technology.<sup>113</sup> Hence, each individual pseudonymizing process must be assessed to be able to conclude if a pseudonymized dataset is to be labeled as personal data or not. Unlike pseudonymized data, anonymized data is entirely excluded from the GDPR.<sup>114</sup> Data that is anonymized was never personal data, to begin with, or has undergone such extensive technical anonymization that no natural person is identifiable through such data.

To further develop on a topic that was briefly mentioned earlier, the GDPR does not rule out that natural persons may be identifiable through their online presence due to the ever-increasing usage of the internet.<sup>115</sup> This can extend to almost everything we use in our day-to-day lives, from devices, applications, to protocols such as internet protocol addresses (IP-address) or cookie identifiers, all of which can leave digital traces and can be used to identify natural persons when combined with unique identifiers and other information.<sup>116</sup> IP-addresses, which are the numerical values that act exactly like addresses in order for computers to be able to send each other data, are particularly interesting because every single device has a corresponding IP-address.<sup>117</sup> This is of significance since nodes on a P2P-network can communicate and potentially identify each other through the usage of IP-addresses, but more on this later.

The GDPR excludes information of deceased persons from being labeled as personal data.<sup>118</sup> This does, however, not exclude the deceased person's personal data from being labeled as an identifier as per Article 4(1) as the deceased person's personal information can help identify a natural person that is alive.

---

<sup>111</sup> Voigt and Bussche, The EU General Data Protection Regulation p. 12.

<sup>112</sup> Article 4(5) in the GDPR.

<sup>113</sup> Bygrave, L. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. Oslo Law Review, Volume 4, No. 2, 2017, p. 114.

<sup>114</sup> Recital 26 in the GDPR.

<sup>115</sup> Recital 30 in the GDPR.

<sup>116</sup> Ibid.

<sup>117</sup> Iann.org. (2011). Beginner's Guide To Internet Protocol (IP) Addresses. Internet Corporation for Assigned Names and Numbers (ICANN). [online], p. 4. Available at: <https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf> [Accessed 19 Apr. 2018].

<sup>118</sup> Recital 27 in the GDPR.

### 3.2 Processing

Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.<sup>119</sup> Processing under the GDPR is, as previously mentioned, not exclusive to any piece of technology and is therefore neutral to technological advances, as it will always be applicable when processing of personal data takes place.<sup>120</sup>

Processing under the GDPR means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means.<sup>121</sup> The definition is made broad to serve the individuals rights and freedoms.<sup>122</sup> Therefore, processing can be almost anything that is done to personal data such as; collection, recording, organizing, structuring, storing, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.<sup>123</sup> The definition is not exclusive to any means, implying that both manual- and automated processing falls within the scope of the regulation.<sup>124</sup> In practice, processing is something that takes place in our day-to-day lives. Every time we purchase from a service provider, every time we register for social media and every time we buy something online there is an underlying process that handles our personal data. This means huge undertakings for corporations whose businesses rely on the processing of personal data for monetary gain. Due to the wide definition of the term processing in the GDPR, processing can also be short-term use of small amounts of data.<sup>125</sup> This implies that personal data that is being displayed on a computer screen or personal data that is being stored intermediately on a computer through, for example, the cache of the internet browser falls within the scope of the GDPR.

### 3.3 Controller

*Controller* refers to a legal person, public authority, agency or other body that jointly or alone determines the purpose and means of processing of the personal data.<sup>126</sup> This means that the

---

<sup>119</sup> Recital 1 in the GDPR.

<sup>120</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 10.

<sup>121</sup> Article 4(2) in the GDPR.

<sup>122</sup> Recital 4 in the GDPR.

<sup>123</sup> Article 4(2) in the GDPR.

<sup>124</sup> Holtz, Den nya allmänna dataskyddsförordningen — några anmärkningar, p. 243.

<sup>125</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 10.

<sup>126</sup> Article 4(7) in the GDPR.

controller is responsible for the processing of personal data, which imposes several legal responsibilities for the controller.<sup>127</sup> The legal definition controller can be broken up into three components; (1) Legal person, public authority, agency or other body (2) that jointly or alone (3) determines the purpose and means of processing.

The first component clarifies that no one, not even a natural person, is excluded from responsibility when it comes to the processing of personal data. The second component widens the reach of the definition controller to include joint responsibility for the processing of personal data. The GDPR introduces the concept of ‘joint controllership’ in Article 26. What this exactly entails for the controllers is for now unclear, but since the parties assume mutual responsibility it is apparent that they have to cater for a clear allocation of responsibilities.<sup>128</sup> Joint controllership can take different forms and does not, according to the A29WP, have to be mutually shared.<sup>129</sup> This means that the joint controllers can either have a very close relationship, with shared infrastructure, purpose and means of processing, or a loose relationship with only partly shared means or purposes of processing.<sup>130</sup> The third component, and arguably the most important component, exemplifies that the one who has the decision making power, not the factual power over the processing, is to be classified as a controller.<sup>131</sup> ‘Means’ in the provision does not only refer to the technical ways of the processing, but also to how the personal data is to be processed, when it is to be deleted and with whom it is to be shared.<sup>132</sup> Purposes are subjective, they can be almost anything and being a controller is primarily the consequence of deciding to process personal data for one's own purpose.<sup>133</sup> The controller can, however, delegate certain tasks when it comes to the processing of personal data to a third party, legally defined as a ‘processor’.

### 3.4 Processor

The processor is labeled as a processor because the controller decided to outsource certain tasks relating to the processing of personal data to a third party and is regulated in the GDPR under Article 4(8). The processor, like the controller, can be a natural or legal person, public authority,

---

<sup>127</sup> Article 5(2) in the GDPR.

<sup>128</sup> Voigt and Busche, *The EU General Data Protection Regulation*, p. 18.

<sup>129</sup> Art. 29 Data Protection Working Party. (2014). Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, WP 169, p. 19.

<sup>130</sup> *Ibid.*

<sup>131</sup> A29WP, Opinion 1/2010, p. 8.

<sup>132</sup> A29WP, Opinion 1/2010, p. 14.

<sup>133</sup> *Ibid.*, p. 8.

agency or other body who processes data on behalf of the controller.<sup>134</sup> Therefore, a controller must exist for a processor to exist. Furthermore, to be classified as a processor, it is required that they are a separate legal entity with regard to the controller.<sup>135</sup> Hence, the processor serves the controllers interests and gets tasks delegated to them, within the means and purposes of the controller's own agenda.<sup>136</sup>

The purpose of strictly regulating the relationship between the processor and the controller, and therefore the responsibility of the processor, is based on a will to maintain the level of data protection that the data subject is provided by the controller.<sup>137</sup> This means that a controller cannot hire third-party service providers that do not meet the level of security that the data subject can expect when processing one's personal data.

Processors can, like the controllers, take a wide variety of legal forms and several processors can be instructed to act at the same time by the controller.<sup>138</sup> Being a processor does not originate from the fact that an entity processes personal data, but rather from the processors work in regard to a specific activity.<sup>139</sup> That means that the label processor is given to someone due to their contractual relationship with a controller, but only in regard to that specific activity of data processing. If the processor performs other activities they can be deemed controller regarding that specific activity, as the label of processor is not exclusive regarding other activities of processing. Note, that a processor who exceeds their responsibility and acquires a position that is relevant to the determining of the means and purposes of the processing of the personal data is labeled as a joint controller alongside the original controller, widening their responsibility.<sup>140</sup>

### **3.5 Rights and Responsibilities**

#### **3.5.1 Fundamental Principles**

The GDPR lays down very specific criteria regarding how the controller and processor process personal data to ensure the integrity and increase transparency. The goal is to enforce processing that is fair and lawful.<sup>141</sup> To do so, only the required data is collected and the means and

---

<sup>134</sup> Article 4(8) in the GDPR.

<sup>135</sup> A29WP, Opinion 1/2010, p. 25.

<sup>136</sup> Ibid.

<sup>137</sup> Ibid., p. 24.

<sup>138</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 20.

<sup>139</sup> A29WP, Opinion 1/2010, p. 25.

<sup>140</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 20.

<sup>141</sup> Recital 39 in the GDPR.

purposes are communicated with the data subject while awareness is raised regarding how and why the personal data is gathered, all provisioned in Article 5 in the GDPR.<sup>142</sup>

The first building block of enforcing the values consists of a purpose limitation and a general principle that portrays the core of the GDPR, namely; ‘lawfulness, fairness and transparency’.<sup>143</sup> Lawfulness according to the GDPR is achieved by, for instance, gaining the data subjects consent in regard to one or several purposes.<sup>144</sup> Lawfulness can be achieved in other ways per Article 6 in the GDPR, for example, if the controller must do so in order to fulfill a legal obligation, if the processing is required to fulfill the purposes and the controller’s interests outweigh the data subjects right to integrity and more. Hence the controller must, when gathering personal data, specify the exact purpose/purposes (purpose limitation) that are to be served when processing the gathered personal data and only then is the processing lawful as per Article 5(1)(a) in the GDPR.<sup>145</sup>

The second building block consists of principles relating to what kind of personal data is stored and how the data is stored.<sup>146</sup> First and foremost, the GDPR enforces the principle of data minimization, as per Article 5(1)(c), to regulate that data is to be kept relevant, adequate and limited to what is necessary.<sup>147</sup> The GDPR also enforces the following principles in Article 5(1) (d-f): The principle of accuracy, to ensure data be kept up to date and inaccurate data be deleted. The principle of storage limitation enforces that the period for which the personal data is stored is limited to a very strict minimum and in direct correlation with the fulfillment of the purpose of the processing.<sup>148</sup> Lastly the principle of integrity and confidentiality, which ensures that the data subjects personal data is processed and stored in a fashion that ensures safety measures to prevent unauthorized access and unlawful processing as well as to avoid damage and complete loss of the data.

These principles, found in Article 5 in the GDPR, portray the core of the GDPR and constitute a strict requirement for the controller regarding the personal data, processing and storing of

---

<sup>142</sup> Article 5(1) in the GDPR.

<sup>143</sup> Article 5(1)(a-b) in the GDPR.

<sup>144</sup> Article 6(1)(a) in the GDPR.

<sup>145</sup> Forgó, N., Hänold, S. and Schütze, B. (2017) "*The Principle of Purpose Limitation and Big Data*". In: Corrales, M., Fenwick, M. and Forgó, N. (eds.), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation*. Springer, Singapore, p. 26.

<sup>146</sup> Recital 39 in the GDPR.

<sup>147</sup> Bygrave, Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, p. 115.

<sup>148</sup> European Data Protection Supervisor. (2018). Guidelines on the protection of personal data in IT governance and IT management of EU institutions. [online], p. 13. Available at: [https://edps.europa.eu/sites/edp/files/publication/it\\_governance\\_management\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf) [Accessed 19 May 2018].

such data. The controller is held accountable and must be able to demonstrate compliance with the principles under Article 5(2) in the GDPR.

### **3.5.2 Data Subjects Rights**

Considering the above-mentioned principles, the data subject receives a vast amount of rights in relation to the processing of their personal data that is reflected in Article 12-21 in the GDPR, which in turn imposes certain obligations on the controller.

#### **3.5.2.1 Right to Information**

The controllers are obliged to provide the data subject with extensive information regarding the processing and storage of their personal data according to Article 12 in the GDPR.<sup>149</sup> The communication of such information must be made in a “concise, transparent, intelligible and easily accessible form, using clear and plain language”.<sup>150</sup> Under Article 13 and Article 14 in the GDPR, the controller must, when gathering personal data, inform the data subject of not only the identity of the data controller but also who the corresponding data protection officer is, as well as the aim of the data collection and information relating to the processing and storage.<sup>151</sup> The extensive requirement of information towards the data subject is in accordance with the goal of increasing transparency and trust when processing personal data.<sup>152</sup>

These rights are not only limited to information and are expanded to impose the data subject with the right to access as per Article 15, the right to erasure as per Article 17, the right to object to processing as per Article 21, the right to restriction of processing as per Article 18, the right to rectification as per Article 16 and the right to data portability as per Article 20.

The right to access strengthens the data subject’s possibility to verify that the controller is acting lawfully, therefore enforcing the data subject’s rights.<sup>153</sup> The right to access goes beyond the obligation of providing information under Article 13 and 14 and gives the data subject, whose personal data the controller processes, the right to receive in-depth information.<sup>154</sup> By gaining a deeper knowledge the data subject can exercise their rights under Article 16-22 in the GDPR.

---

<sup>149</sup> Sobolewski, M., Mazur, J. and Paliński, M. (2017). GDPR: A Step Towards a User-centric Internet?. *Intereconomics*, 52(4), pp. 207-213.

<sup>150</sup> Article 12(1) in the GDPR

<sup>151</sup> Sobolewski, Mazur and Paliński. GDPR: A Step Towards a User-centric Internet?, p. 4.

<sup>152</sup> Recital 58 in the GDPR.

<sup>153</sup> Recital 63 in the GDPR.

<sup>154</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 150.

### 3.5.2.2 Right to Erasure, Rectification and Restriction of Processing

The right to erasure, commonly referred to as ‘the right to be forgotten’, enables data subjects to be in control of their personal data in an environment that is not oriented towards forgetting.<sup>155</sup> The right to be forgotten is a topic that has been subject to great discussion during the past few years, given our technological development and corporations utilizing, if not abusing, personal data for monetary gain. The CJEU ruled in the case *Google v. Spain* that the fundamental rights to privacy outweighs the economic interest of commercial firms and, sometimes, the public's interest of accessing information.<sup>156</sup> The GDPR has incarnated the empowerment of the data subject and the right to their data by enforcing the right to erasure and widening the scope to impose the controller, who has made the personal data public, with the duty of informing the controllers processing the data to erase all links to, or copies or replications of such personal data.<sup>157</sup> The right to rectification is also based on the concept of empowering data subjects to be in control of their own personal data, imposing the controller with the responsibility of correcting, on demand and without undue delay, inaccurate personal data concerning the data subject.<sup>158</sup> The data subject also obtains the right to the restriction of processing, which limits the controller in their possibilities to process their personal data. These three rights are not only a way of empowering the data subject with control of their own personal data, but also a way of enforcing means for the data subject to eliminate law infringements, performed by the controller on their personal data.<sup>159</sup>

### 3.5.2.3 Right to Data Portability

Through the implementation of the right to data portability, the data subject is further empowered regarding their personal data. This right creates the possibility of transferring data “from one electronic processing system to and into another, without being prevented from doing so by the controller”.<sup>160</sup> The right, as per Article 20 in the GDPR, creates the possibility for a data subject to, without interference from a non-cooperative controller, request their personal data in a common and easily readable computer format and transmit the data to another

---

<sup>155</sup> Nicolaidou and Georgiades. “*The General Data Protection Regulation: A Law for the Digital Age*”. In: Synodinou, Jougoux, Markou and Prastitou. (eds.), *EU Internet Law*, p. 43.

<sup>156</sup> Case C- 131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* [2014], ECLI:EU:C:2014:317, Court of Justice of the European Union.

<sup>157</sup> Recital 66 in the GDPR.

<sup>158</sup> Recital 65 in the GDPR.

<sup>159</sup> Voigt and Busche, *The EU General Data Protection Regulation*, p. 154.

<sup>160</sup> Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data COM (2012) 11 final, p. 9

controller.<sup>161</sup> The right to data portability can be seen as an extension of the data subject's right to access, contributing to the principle of transparency toward the data subject.<sup>162</sup>

#### **3.5.2.4 Right to Object and Automated Decision Making**

According to Article 21 in the GDPR, the data subject has the right to object to the processing of one's personal data, even if the data is processed lawfully and is necessary for carrying out a task that is of public interest, exercise of a public authority vested in the controller or the exercise of the controller's legitimate interest.<sup>163</sup> The controller must, therefore, demonstrate that their interest of processing outweighs the data subjects' interest. The provision is mainly targeting lawful processing that the data subject does not wish for the controller to carry out.<sup>164</sup>

Article 22 in the GDPR intends to restrict automated decision making and ensure that the data subjects rights and freedoms are at the forefront.<sup>165</sup> The provision does so by widening the data subject's right to object to include the right for the subject to negate the controller from subjecting the data subject's personal data to processes that are solely automated.<sup>166</sup>

### **3.6 The Controllers Additional Responsibilities**

The data subject's concrete rights constitute the material requirements for the controller when processing personal data. The controller has additional obligations that are specifically enforced through Chapter four in the GDPR that constitute the controller's organizational requirements. As previously mentioned, Article 5(2) in the GDPR obligates the controller to be accountable for ensuring compliance with the material requirements, as well as providing proof of compliance to an authority. In Article 24 in the GDPR, the controller's obligations are widened by imposing responsibility and liability, on an organizational level, on the controller when processing personal data.<sup>167</sup> The general organizational measures to be taken by the controller are data protection measures, establishing responsibilities in the case of joint controllership, measures to be taken when using a processor, keeping records of processing activities and security measures to be taken when processing.

---

<sup>161</sup> Recital 68 in the GDPR.

<sup>162</sup> Nicolaidou and Georgiades. "The General Data Protection Regulation: A Law for the Digital Age". In: Synodinou, Jougoux, Markou and Prastitou. (eds.), EU Internet Law, p. 47.

<sup>163</sup> Recital 69 in the GDPR.

<sup>164</sup> Ibid.

<sup>165</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 180.

<sup>166</sup> Karegar, F. (2018). Towards Improving Transparency, Intervenability, and Consent in HCI (Doctoral dissertation, Karlstad University Press), p. 29.

<sup>167</sup> Recital 74 in the GDPR.

### 3.6.1 Data Protection Measures

The notion of building an application or service with security and safety measures is not something unique to the GDPR, but is unique in the fact that it is now mandatory to implement such features.<sup>168</sup> Article 25 in the GDPR introduces data protection by design and by default that, as an example, consist of “minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features”.<sup>169</sup> These are merely examples adopted by the GDPR, as the provision itself states that “appropriate technical and organizational measures” must be taken and you must be able to prove so to the supervisory authority.<sup>170</sup> By not including any safety standards the GDPR is not specific to any safety measures but is instead a timeless provision that requires the controller to take “appropriate measures”.<sup>171</sup> Hence, development of safety measures of services and processes is ongoing and highly frequent as technology and security threats evolve.<sup>172</sup>

### 3.6.2 Joint Controllership and Responsibilities

Joint controllership, as discussed in section 3.3, obligates the controllers to, in a transparent manner, determine their respective responsibilities for compliance with the obligations under GDPR, particularly regarding the data subjects right to information.<sup>173</sup> The clear distinction between each controller’s responsibilities is required to ensure that the data subject’s rights and freedoms are at focus, not putting them in a worse position by allocating controllership over several organizations.<sup>174</sup> The controllers can also equally determine the processing of the personal data, which in turn means that the controllers are equally responsible.<sup>175</sup> Regardless of the arrangement of responsibility, the arrangement must be communicated to the data subject and the data subjects may exercise their rights under the GDPR against each of the controllers, regardless of the arrangement.

---

<sup>168</sup> Calder, A. (2016) EU GDPR: a pocket guide. (n.p.): It Governance Pub., p. 52.

<sup>169</sup> Recital 78 in the GDPR.

<sup>170</sup> Twobirds.com. (2018). *Guide to the General Data Protection Regulation*. [online], p. 6. Available at: <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en> [Accessed 19 Apr. 2018].

<sup>171</sup> Bygrave, Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, p. 114.

<sup>172</sup> Calder, EU GDPR: a pocket guide, p. 53.

<sup>173</sup> Article 26 in the GDPR.

<sup>174</sup> Recital 78 in the GDPR.

<sup>175</sup> Voigt and Busche, The EU General Data Protection Regulation, p. 34.

### 3.6.3 Processor Measures

The processor is also imposed with a responsibility to comply with the GDPR.<sup>176</sup> The processor's organizational responsibilities are regulated under Article 28 of the GDPR and are, as discussed in section 3.4, applicable to situations where the controller has a processor process personal data. The processor is required to fulfill requirements specific to terms of knowledge, reliability and resources, and must be able to implement appropriate security and technical measures.<sup>177</sup> It is the controller's responsibility to make sure that the processor meets such standards. However, the processor is in fact, through the implementation of the GDPR, directly responsible for certain criteria to be fulfilled regarding the processing of personal data, such as security measures and that the processor merely processes the data in accordance with the instructions given by the controller.<sup>178</sup> It is required by the GDPR that the relationship between controller and processor, as well as the processing by the processor, is governed by a contract.<sup>179</sup> The contract dictates the instructions and framework for the processor's responsibilities and authority regarding the task and is referred to as a Data Processing Agreement (DPA).

### 3.6.4 Keeping Records of Processing Activities

According to Article 30 in the GDPR, the controller and processor must keep records of their processing activities. These are kept as proof of compliance and are thereafter given to the appropriate supervisory authority.<sup>180</sup> Maintaining such records increases transparency towards the data subject and improves the possibility of satisfying the data subject's right to request information. The regulation lays forth extensive criteria for what information that is to be documented regarding the processing and naturally sets a greater responsibility on the controller as they bare the primary responsibility regarding compliance and a certain level of security.<sup>181</sup>

### 3.6.5 Security Measures When Processing

Security measures are not only limited to the implementation of data protection by design and default but must also be implemented on an organizational and technical level through means

---

<sup>176</sup> Hoeren, T. (2018) "*Big Data and Data Quality*". In: Hoeren T. and Kolany-Raiser B. (eds.), *Big Data in Context*. SpringerBriefs in Law. Springer, Cham, p. 1.

<sup>177</sup> Recital 81 in the GDPR.

<sup>178</sup> Voigt and Busche, *The EU General Data Protection Regulation*, p. 83.

<sup>179</sup> Article 28(3)(a) in the GDPR.

<sup>180</sup> Recital 82 in the GDPR.

<sup>181</sup> Article 30 in the GDPR.

of computer security in events of processing.<sup>182</sup> Article 32 in the GDPR sets non-exhaustive minimum-security standards, for controllers and processors, that are relevant for the safeguard of data protection.<sup>183</sup> The provision requires the implementation of pseudonymizing and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.<sup>184</sup>

In doing so the controller and processor can mitigate security risks that have been assessed, by ensuring appropriate levels of security, considering the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected.<sup>185</sup>

### **3.7 GDPR Conclusion**

This concludes the section on the GDPR and its key provisions regarding personal data and responsibilities imposed on those that process such data. The GDPR aims to increase transparency and empower the data subject to be in control of their own personal data by imposing certain rights on the data subject that translate into obligations for the controller and processor. These obligations take two separate forms. The first set of obligations are the controller's responsibility in being able to provide the above-mentioned material to the data subject, i.e. the right to information and data portability. These rights are aimed at increasing the transparency and provide insight for the data subject. The second set of obligations are the organizational measures which the responsible controller/processor must implement. They are meant to increase security and the protection of the personal data, i.e. the securing of processes and personal data. The next chapter will discuss the balance between blockchain technology and these key provisions.

---

<sup>182</sup>Softcat.com. (2018). *GDPR – A guide to key articles for security & privacy professionals*. [online] Available at: [https://www.softcat.com/assets/uploads/pdfs/gdpr/whitepaper\\_hunton\\_williams\\_gdpr\\_key\\_articles\\_guide\\_en.pdf](https://www.softcat.com/assets/uploads/pdfs/gdpr/whitepaper_hunton_williams_gdpr_key_articles_guide_en.pdf) [Accessed 19 Apr. 2018].

<sup>183</sup> Voigt and Busche, *The EU General Data Protection Regulation*, p. 39.

<sup>184</sup> Article 32(1)(a-d) in the GDPR.

<sup>185</sup> Recital 83 in the GDPR.

## 4 The Blockchain and the GDPR

When discussing central provisions of the GDPR and having knowledge regarding how the blockchain works, it is inevitable to notice and draw lines between the blockchain and the GDPR. The central principles, rights and obligations apply to the blockchain and it is therefore important to identify the key actors and components on the blockchain in order to be able to assess responsibility and rights as anticipated by the GDPR.

### 4.1 Personal Data

The rights of the individuals are, as stated, the protected property by the GDPR. In identifying potential personal data, and where such data is processed, the data subjects are also identified. When discussing personal data on the blockchain it is important to assess different types of data on the blockchain and their key components. In chapter two above, the reoccurring concepts of public keys, transaction data and nodes are all forms of data that can constitute personal data as per the GDPR. Therefore, each component will be examined considering the GDPR.

#### 4.1.1 Public Keys and Transaction Data

Public keys, as addressed in section 2.2.4, are keys that are handed to every single user on the blockchain to be able to identify a single user by utilizing asymmetric cryptography. Public keys are used to identify and authorize user transactions on the blockchain and each public key points to a specific user.<sup>186</sup> Given that the use of meta-data has enabled corporations to identify consumers by their credit card usage, even though all information has been anonymized except for the habits of the consumer, it must not be ruled out that a public key, when associated with other information, could make it possible for someone to identify the data subject as per Article 4(1) of the GDPR.<sup>187</sup> The GDPR does not set forth requirements for in whose possession the additional information used to identify a data subject must be. So, if someone were to use the blockchain to transfer ownership of a house, such a transfer would be made public, as is the nature of the blockchain. If the persons neighbor would know that such a transfer took place, he/she could view the transfer on the blockchain and associate the public key to the transfer that

---

<sup>186</sup> Maxwell, W. and Salmon, J. (2017). *A guide to blockchain and data protection*. [online] Hlengage.com, p. 7. Available at: [https://www.hlengage.com/\\_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf](https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf) [Accessed 19 Apr. 2018].

<sup>187</sup> Deng, B. (2018). *People can be identified through their credit-card transactions*. [online] Available at: <https://www.nature.com/news/people-identified-through-credit-card-use-alone-1.16817> [Accessed 19 Apr. 2018].

was made. Therefore, it is not impossible that a public key constitutes information that indirectly assists someone in identifying a person.

The blockchain algorithm hashes the transaction data, which in this case is the house, before it is appended to the blockchain-data-structure.<sup>188</sup> The A29WP recognizes hashing as a form of pseudonymization, not as anonymization, since it merely reduces the linkability between a dataset and the original data subject.<sup>189</sup> The blockchain relies on hashing to identify the validity and authentication of transactions and turns the transactions into practically unreadable code to the human eye. Considering what the A29WP stated regarding hashing, a pseudonymized dataset constitutes personal data if the data that is hashed is deemed as personal data.<sup>190</sup> In section 3.1 it was mentioned that each pseudonymizing process must be assessed to be able to conclude if a dataset can be labeled as personal data, weighing in cost and time required for the identification of the natural person. This means that transaction data on different types of blockchains can be labelled differently, depending on the technology, but it does not rule out the possibility of transaction data being labelled as personal data.

Several blockchains encourage users to create new public-private keys for each transaction to ensure integrity, but this has not become common practice.<sup>191</sup> Both public keys and transaction data can therefore be deemed personal data, or at least the possibility of such data being labelled personal cannot be ruled out.<sup>192</sup>

#### **4.1.2 Nodes**

As discussed in section 2.1, the P2P-networks are based on individual nodes communicating with each other. These nodes are identified by their unique addresses and use these addresses to send each other messages and distribute the blockchain-data-structure, namely, the ledger. As mentioned in section 3.1, the GDPR does not rule out digital traces and addresses from falling within the definition of personal data. The question is if the addresses can be used, in combination with other unique identifiers, to identify a person. If the P2P-network uses a

---

<sup>188</sup> See section 2.3.3.

<sup>189</sup> Article 29 Working Party. (2014) Opinion 05/2014 on Anonymisation Techniques, WP216, p. 3.

<sup>190</sup> Maxwell and Salmon, A guide to blockchain and data protection, p. 9.

<sup>191</sup> Dorit, R. and Adi, S. (n.d.). Quantitative Analysis of the Full Bitcoin Transaction Graph. [online] Eprint.iacr.org, p. 4. Available at: <https://eprint.iacr.org/2012/584.pdf> [Accessed 19 Apr. 2018].

<sup>192</sup> Reid, F. and Harrigan, M. (2012). An Analysis of Anonymity in the Bitcoin System. Security and Privacy in Social Networks. 3. 10.1109/PASSAT/SocialCom.2011.79, p. 26.

standard static IP-address as means of identifying unique nodes, the GDPR explicitly states that such an online identifier constitutes personal data.<sup>193</sup>

In P2P-networks where that is not the case, but a different sort of address is used to identify nodes, it is not as straightforward. In Case-582/14 the CJEU assessed if dynamic IP addresses (temporary IP addresses that change upon each connection session) could constitute personal data.<sup>194</sup> They issued their final judgment and found that dynamic IP addresses could constitute personal data under circumstances where there is another party that can identify an individual based on the changing IP-address (e.g. an internet service provider) and that the party that has the IP-address has legal means of obtaining access to the information that is being held by the other party, the internet service provider in this case. Although this judgement was not judged based on the GDPR, it constitutes an opinion that is in accordance with the GDPR and if online addresses that change can be used to, in some way, aid in identifying someone, it is personal data.<sup>195</sup>

The IP-addresses that are connected to each individual node can, therefore, potentially constitute personal data under the GDPR, which would mean that the P2P-network is not excluded from the GDPR.

## **4.2 Processing**

The conclusion of the previous section, that the blockchain can and does have certain elements that constitute personal data, means that certain events that take place on the blockchain must be assessed to see if these can constitute processing as per the GDPR. As mentioned in section 3.2, processing under the GDPR is any operation or set of operations that is performed on personal data. Since the aim of the GDPR is to ensure the data subjects rights and freedoms regarding the processing of personal data, it is deemed relevant to identify the potential processing of personal data on the blockchain.<sup>196</sup> Whereas processing and personal data directly correlate, as processing is an action performed on personal data, the first step in identifying processing would be to assess what actions are performed on the data that is deemed personal data in the blockchain.

---

<sup>193</sup> Recital 30 in the GDPR.

<sup>194</sup> Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016], 112/16 Luxembourg, Court of Justice of the European Union.

<sup>195</sup> Recital 30 in the GDPR.

<sup>196</sup> Recital 2 in the GDPR.

#### **4.2.1 Processing Public Keys and Transaction Data**

A public key corresponding to an individual private key is given to all users on the blockchain, as mentioned in section 2.2.4. Consequently, for each user on the blockchain, all other users have a public key corresponding that that unique user so they can verify that a transaction was authorized. The verification of transaction data, to secure that such data meets the validation requirements, are automated and performed as instructed by the blockchain algorithm and uses the corresponding public key. The definition of processing under the GDPR is very broad and includes almost all actions performed on personal data. Since the GDPR is autonomous to automated means, which indicates that even if the blockchain algorithm manages the processing, the verification of transactions by using public keys could still constitute processing. It is, therefore, likely that public keys are subject to processing under Article 4(2) in the GDPR.

The labelling of transaction data is very similar to the labelling of public keys and transactions are subject to several different actions. As mentioned in section 2.3.3, transaction data is validated by performing certain validation functions on the data. The transaction data is then stored in a block, in a Merkle tree. That block is then appended to the blockchain-data-structure and distributed to all users on the blockchain. This means that extensive actions, such as structuring, usage and storage are performed on the transaction data. Much like public keys, it is likely that transaction data also is subject to processing under Article 4(2) in the GDPR.

#### **4.2.2 Processing Nodes**

As for the nodes, it was discussed in section 2.3.5 that each node keeps a record of nodes that the node communicates with. That means that each node on the network stores a list containing personal data, as nodes were deemed to potentially constitute personal data in the previous section. Under the GDPR the mere storing of personal data is enough to be considered processing.<sup>197</sup>

Considering what has been discussed regarding personal data, processing and actions performed on sets of data, the blockchain most likely falls within the material scope of the GDPR.<sup>198</sup> Throughout the thesis, the GDPR has been discussed as a regulation that imposes responsibilities on a party that processes personal data. Recognizing the responsible party/parties on a blockchain, that is based on a P2P-system with an algorithm that dictates the

---

<sup>197</sup> Article 4(2) in the GDPR.

<sup>198</sup> Article 1(1) in the GDPR.

rule-set rather than a central authority, is essential for assessing controllership and responsibility according to the GDPR.<sup>199</sup>

### **4.3 Controller**

When identifying the controller under the GDPR, as discussed in section 3.3, the key element is to identify who has the decision-making power regarding the processing of the personal data. However, the blockchain challenges the assumption that centralized responsibility always is imposed, as the core of the blockchain technology is to eliminate middleman services, in other words, the ones that usually are controllers according to Article 4(7) in the GDPR.<sup>200</sup> According to the GDPR, there must be a party that is responsible under the principle of accountability.<sup>201</sup> There has been a lot of speculation surrounding the labelling of users on a blockchain network under the GDPR, either as joint controllers, processors, controller (much like when buying cloud services and the user is labeled the controller) or that each and every user be deemed controller for themselves and processor for other users.<sup>202</sup> To assess if users can be deemed controllers under the GDPR an analysis of the relevant Article 4(7) must be made considering users on the blockchain.

#### **4.3.1 Labelling the User**

As discussed in section 2.3.5, nodes collectively make up the blockchain. They maintain ledgers and append the ledgers with new transactions and blocks, as well as validate the other node's actions. The GDPR identifies a controller as someone that jointly or alone determines the purposes and means for the processing of the personal data. As explained in section 2.3.7, the nodes jointly reach consensus on which ledger represents the truth and collectively validate and append new transactions to the existing ledger. At first glance, this seems like actions that would fall under controllership or joint-controllership. However, as discussed in section 3.3, the key component is being able to have the decision-making power over the processing. The users have, without a doubt, the factual power over the processing as they can choose to connect to the blockchain and therefore provide computing power and also leave when they wish, but the question is if the users are instilled with the power to decide the means and the purpose of the processing. Means refers to how the data is processed, when it is deleted and to whom it is shared. Purpose refers to the aim of the processing and is subjective to each processing activity.

---

<sup>199</sup> Article 24 in the GDPR.

<sup>200</sup> Dulong de Rosnay, M. (2015). Peer-to-peer as a design principle for law: distribute the law. *Journal of Peer Production, Disruption and the Law*, pp.1-9.

<sup>201</sup> Article 5(2) in the GDPR.

<sup>202</sup> Maxwell and Salmon, *A guide to blockchain and data protection*, p. 10.

For the illustrated ownership managing blockchain the purpose of the blockchain would be to manage ownership in a correct and transparent manner. The means, or the how, would be by maintaining a ledger through the instructions set forth by the blockchain algorithm. The purpose of the blockchain-data-structure is to ensure a specific nonfunctional quality of P2P-network, namely ensuring its integrity.<sup>203</sup> Each blockchain does, however, have individual purposes that merely utilize the ensuring of integrity, and the creator of the unique blockchain chooses what the blockchain is to be used for, be it ownership management or as a currency etc. The blockchain algorithm is also something that has been written preemptively to the launching of the blockchain, which is why the users lack the capability of changing the means of the blockchain, as they merely provide processing power for the execution of the blockchain algorithm.<sup>204</sup> Considering the aforementioned, the users cannot be labeled as controllers in an open distributed blockchain as they lack the decision-making power that exemplifies a controller under Article 4(7) in the GDPR. This will, however, widely depend on the nature of the blockchain under discussion, e.g. open source blockchains might assess responsibility in a different manner than the structure that we commonly see today, like the blockchain in the example at hand.

#### **4.3.2 Labelling the Creator(s)**

Even though the users cannot be labelled as controllers, there is a possibility of labelling the creators of blockchains as controllers. The previous section clarified that the creators are the ones that 1) develop the blockchain algorithm, or at least put it to use and 2) decide what the blockchain is to be used for, its purpose. Even though the technology itself, the blockchain, does not have a centralized point of control, the means and purpose were preemptively decided by the creators.<sup>205</sup> That means that the creator/creators are the ones who determine the purpose and means of the blockchain, labelling them as controllers as per Article 4(7) in the GDPR. The creator/creators can be, as mentioned in section 3.3, both natural- or legal persons. In many popular cases, like Litecoin, Ethereum or Ripple, the creators behind the technology are natural persons that collectively contribute to the creation and maintaining of the blockchain.<sup>206</sup> In these cases, the natural persons responsible would jointly be held accountable according to the

---

<sup>203</sup> Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, p. 18.

<sup>204</sup> Ibid., p. 46.

<sup>205</sup> Ibid., p. 59.

<sup>206</sup> Roberts, D. and Finance, Y. (2018). The 11 biggest names in cryptocurrency right now. [online] Finance.yahoo.com. Available at: <https://finance.yahoo.com/news/11-biggest-names-cryptocurrency-2017-110033921.html> [Accessed 19 Apr. 2018].

principle of accountability and would, therefore, have, as mentioned in section 3.3, joint controllership. The same principle applies to companies and other legal persons responsible for the blockchain, where lone responsibility makes that legal person solely the controller, and co-operation to create and manage the blockchain with other legal persons or natural persons leads to joint controllership.<sup>207</sup> According to Article 26, joint controllership obligates the controllers to allocate responsibility regarding the processing of personal data, and not put the data subject in a worse situation by dividing responsibility.<sup>208</sup> The arrangement must be communicated to the data subject, to secure that the transparency imposed by the GDPR is upheld. In some cases, the original creator of the blockchain is unknown to the public, like the creator of Bitcoin, Satoshi Nakamoto, who is still unknown to this day.<sup>209</sup> This would be, to some extent, impossible under the GDPR, as there cannot be an anonymized controller since this would undermine the purposes of transparency and trust imposed by the GDPR and interferes with the data subjects' rights, e.g. the right to information under Article 13 and 14 in the GDPR.<sup>210</sup>

To summarize the aforementioned, even though the user(s) were excluded from being labeled as the controller(s) the discussion resulted in the labelling of the creator of the blockchain as the controller under Article 4(7) in the GDPR. The user does, however, factually process personal data as discussed in section 4.2.1 and 4.2.2, which requires assessing whether the user(s) are to be labelled as processors under Article 4(8) in the GDPR.

#### **4.4 Processor**

As mentioned in section 3.4, a processor is someone who processes personal data on behalf of the controller. Like the controller, the processor can take any legal form and are identified by them performing a certain activity of data processing for the data controller.<sup>211</sup> Given that a controller's decision to delegate, all or part of, the processing activities to external actors is the main factor attributing to the existence of a processor as per the GDPR, a decision that leads to the controller delegating the processing activities to external actors on a P2P-network indicates that the nodes are to be labelled as processors under the GDPR. According to the GDPR, a processor is a separate legal entity and processes personal data on the controller's behalf. Everyone connected to the P2P-network constitutes a single user, as discussed in section 2.1,

---

<sup>207</sup> Voigt and Busche, *The EU General Data Protection*, p. 18.

<sup>208</sup> See section 3.6.2.

<sup>209</sup> Hodge, M. (2018). Who is Satoshi Nakamoto? Bitcoin inventor whose identity remains a secret. [online] The Sun. Available at: <https://www.thesun.co.uk/news/5037060/satoshi-nakamoto-bitcoin-inventor-richest-world/> [Accessed 19 Apr. 2018].

<sup>210</sup> Article 5 in the GDPR.

<sup>211</sup> A29WP, Opinion 1/2010, p. 25.

motioning the fact that everyone, excluding the controller, is a separate legal entity. Each node also processes personal data, as concluded in section 4.2.1 and 4.2.2. Given these circumstances, the nodes undeniably fall within the reach of the provision processor under Article 4(8) in the GDPR and are, therefore, to be labelled as processors.

The labelling of controller and processor is done to impose responsibility on those that are held responsible for the processing of personal data.<sup>212</sup> Therefore, it is of interest to assess if the fundamental principles and rights of the data subject can be upheld in a scenario where the controller is the creator of the blockchain and the processors are the individual nodes on the blockchain.

## **4.5 Responsibilities**

Given that the primary responsibility has been imposed on the creator of the blockchain they are the ones to provide proof of compliance according to the principle of accountability.<sup>213</sup> This does not mean that the processors are free from responsibility, as discussed in section 3.5. Therefore, the organizational and material measures on the blockchain must be analyzed and assessed to answer whether they provide adequate means for complying with the GDPR.

### **4.5.1 Organizational Measures**

The controllers and processors material requirements, as discussed in section 3.6 i.e. responsibility and liability, are imposed on the controller regarding certain measures that an organization must implement to be compliant with the GDPR.

#### **4.5.1.1 Data Protection**

As discussed in section 3.6.1, the GDPR obligates organizations to apply certain data protection measures to ensure a level of security. As the GDPR does not provide any specific standards, only examples, it is individual for each technological solution if the taken measures are adequate under the GDPR. Article 25 in the GDPR specifically targets how personal data is protected and it is therefore of interest to assess how such data is protected on the blockchain. One of the greatest challenges of the blockchain is that generic blockchains do not let the controller nor processor know when they are processing personal data, meaning that every single element that possibly can contain personal data must be adjusted to fit the requirements of the GDPR.<sup>214</sup> The blockchain is also public by nature, which means that all transactions are

---

<sup>212</sup> Article 1(1) in the GDPR.

<sup>213</sup> Article 5(2) in the GDPR.

<sup>214</sup> Maxwell and Salmon, A guide to blockchain and data protection, p. 14.

visible to everyone, i.e. also potential personal data. Data protective measures are also hard to assess since they are unique to a certain time and depend on the sensitiveness, underlying technology and are individual. The examples laid forth are not exhaustive but give a basic idea of how an organization is measured regarding data protection and will therefore be used as a starting point in assessing if processors and controllers are compliant.

### *Transaction Data*

Transaction data is, as mentioned in section 4.1.1, pseudonymized at first contact since the nodes start hashing transaction data as soon as they receive such data, to be able to create new blocks. That means that the pseudonymization takes place as soon as possible, automatically fulfilling one of the examples laid forth by the GDPR.<sup>215</sup> When discussing how blockchains distribute transaction data it became clear that such data is distributed to the entire network in a gossip fashion and then hashed and structured in a Merkle tree, by the individual nodes, before being distributed as completed blocks to the other nodes. This entails that personal data is not only potentially distributed to every user on the blockchain, but is also potentially processed by every single user. Since the security and validity of the blockchain originates from the calculation power of the masses, it does not cohere with the GDPR's example of ensuring protection through minimizing the processing of personal data.<sup>216</sup> This much can be said though, the factual processing of personal data is minimized by having nodes move on and process new transactions and blocks as soon as the appended block has been validated, as introduced in section 2.3.6. Also, under Article 25 in the GDPR, the emphasis is on appropriate technical and organizational measures. If the blockchain can ensure the integrity and transparency of data through utilizing the computing power of the masses, while also enabling the data subject to monitor the data processing and enabling the controller to create and improve security features, which will depend on the individual blockchain algorithm and architecture of the blockchain, the controller could possibly be deemed compliant under Article 25 in the GDPR.

### *Public keys and nodes*

Public keys and IP-addresses of nodes are of similar nature when assessing processing. These are only used to identify and maintain a relationship between the users on the blockchain. Also, they are not collected excessively, as each user only gains one public key and address.<sup>217</sup> The

---

<sup>215</sup> Recital 78 in the GDPR.

<sup>216</sup> Ibid.

<sup>217</sup> See section 2.1 and section 2.2.4.

keys are distributed to every other user while the addresses are only distributed to a selected few. These distributions are, however, necessary for the entire concept to work, since digital fingerprinting is dependent on the distribution of public keys and the maintaining of an address register is required for the distribution of ledgers and communication among nodes.<sup>218</sup> The nature of public keys and addresses entails that they are initially pseudonymized since they cannot be attributed to a specific data subject without additional information.<sup>219</sup>

The anonymization and pseudonymizing of personal data is perhaps the most important part of the provision imposing data protection by design and default.<sup>220</sup> However, like transaction data, these are not factually kept to a minimum but is necessary for the functionality. The principle of minimization and storage limitation under Article 25 in the GDPR might not conform with the excessive distribution of public keys and addresses.<sup>221</sup> However, much like when dealing with transaction data, the GDPR lays forth the requirement of applying appropriate measures to ensure that the requirements of the regulations are met. The communication between nodes is strictly open, the public key is derived from one's private key, the processing functions and monitoring of the personal data is as transparent as processing can be and the data is pseudonymized from the start. Therefore, it is possible that the data protection measures taken are the necessary ones, proving compliance.<sup>222</sup>

#### **4.5.1.2 Processor Measures**

Processors are not excluded from compliance, entailing that each user on the blockchain individually bears responsibility for the processing taking place on their own computer.<sup>223</sup> One of the most interesting points when assessing a processor in the blockchain is that they do not have the factual power to alter or impact the system unless managing the majority of all users on the entire network.<sup>224</sup> And even so, the users on the blockchain are not manually acting on the creators' instructions, they are automatically acting out the instructions written in the blockchain algorithm. This is an anomaly in the eyes of the GDPR since the GDPR assesses the processor as someone being 'hired' to provide a technical solution or addition of the processing.<sup>225</sup>

---

<sup>218</sup> See section 2.1 and section 2.2.4.

<sup>219</sup> Article 4(5) in the GDPR.

<sup>220</sup> Voigt and Busche, *The EU General Data Protection Regulation*, p. 64.

<sup>221</sup> Maxwell and Salmon, *A guide to blockchain and data protection*, p. 14.

<sup>222</sup> Recital 78 in the GDPR.

<sup>223</sup> See section 4.4.

<sup>224</sup> See section 2.3.7.

<sup>225</sup> Recital 81 in the GDPR.

The GDPR requires for these processors to provide guarantees regarding knowledge, reliability and resources, to implement technical solutions to meet the requirements set by the GDPR. It is noteworthy that the technical solution and guarantee already is provided to the processor by the controller through the blockchain algorithm. This, in turn, means that the users are imposed with responsibility without any real way of altering the technical measures to ensure compliance, except for leaving the blockchain. However, that does not necessarily have to be in the user's disfavor, since the most direct responsibilities of the processor do not involve the processing of data in any other way than in accordance with the instructions given by the controller and security measures.<sup>226</sup> These instructions and security measures are implemented in the blockchain algorithm, meaning that the responsibility to follow instructions are automatically met and the security measures are the ones implemented by the controllers. Consequently, if the controller is compliant, so is the processor.

As presented in section 3.6.3, the parties must have a contract between them, a Data Processing Agreement. This means that signing up to acquire the status of 'user' on the blockchain requires that the controller presents each person with a Data Processing Agreement that dictates the instructions and framework of the processing to take place. In such a Data Processing Agreement the controller can take responsibility for the processor's security measures, as a controller's non-compliant security measures could result in all the processors failing to comply with the GDPR.<sup>227</sup> Unless the processor is able to prove that they are not in any way responsible for the event giving rise to the damage, they are to be held liable under Article 82(3) in the GDPR.<sup>228</sup> In a blockchain scenario, it is probable that the processors are able to prove that they are not responsible for events giving rise to the damage as the nodes have no factual way of altering the security measures and a breach would be out of their control.

#### **4.5.1.3 Keeping Records of Processing Activities**

The GDPR also imposes that records be kept of processing activities that take place under Article 30.<sup>229</sup> According to Article 30(1) and (2) in the GDPR, this responsibility is imposed on both the controller and processor regarding any processing.<sup>230</sup> By nature, the blockchain maintains records of all processing activities, as the ledgers and the blockchain algorithm are

---

<sup>226</sup> See section 3.6.3.

<sup>227</sup> Article 28(1) in the GDPR.

<sup>228</sup> Voigt and Bussche, *The EU General Data Protection Regulation*, p. 208.

<sup>229</sup> Nicolaidou and Georgiades. "*The General Data Protection Regulation: A Law for the Digital Age*". In: Synodinou, Jogleux, Markou and Prastitou. (eds.), *EU Internet Law*, p. 9.

<sup>230</sup> See section 3.6.4.

transparent and anyone can see how and what is processed.<sup>231</sup> However, the record that the controller maintains must contain information regarding contact details and name, purposes, categories of processed personal data and data subjects and categories of recipients to receive data.<sup>232</sup> Such a record is not difficult for the controller to maintain since purposes and categories of recipients are readable from the blockchain algorithm and data-structure. Categorizing data subjects and personal data can, however, be more difficult since the controller can never know with certainty what sort of data that will be maintained on the blockchain.<sup>233</sup> Hence, the blockchain has the potential of processing every category of personal data of every possible data subject, and the controller should, therefore, assume that it does. The processor, i.e. the user on the blockchain, on the other hand, needs only maintain a record containing their name and contact details of themselves and the controller as well as a list of categories processed on behalf of the controller.<sup>234</sup> All information, except for the name and contact details of the processor, is provided by the controller and since this register is only to be made available on request to a supervisory authority, it must be deemed doable from a blockchain perspective.<sup>235</sup>

#### **4.5.1.4 Security of Processing**

As discussed in section 3.6.5, the GDPR also requires certain security implementations when processing personal data. The pseudonymizing is not enough in itself, as this only assesses how the data is stored, and organizational measures must also be assured to comply with the GDPR. The integrity and security of the blockchain is dependent on the mass of the computing power being attributed to the blockchain by the nodes.<sup>236</sup> However, that means that the blockchain becomes physically one of the securest data-structures known.<sup>237</sup> The biggest risk factor to the blockchain on an organizational level is that the controller commits faulty changes that have not been properly tested leading to security flaws in the code or forks the blockchain into two

---

<sup>231</sup> See section 2.3.7.

<sup>232</sup> Article 30(1)(a-d) in the GDPR.

<sup>233</sup> For example, child pornography has been found on the Bitcoin blockchain. See: Gibbs, S. (2018). Child abuse imagery found within bitcoin's blockchain. [online] the Guardian. Available at: <https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content> [Accessed 19 Apr. 2018].

<sup>234</sup> Article 30(2) in the GDPR.

<sup>235</sup> Article 30(4) in the GDPR.

<sup>236</sup> Miles, C. (2018). Blockchain security: What keeps your transaction data safe? - Blockchain Unleashed: IBM Blockchain Blog. [online] Blockchain Unleashed: IBM Blockchain Blog. Available at: <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/> [Accessed 11 Apr. 2018].

<sup>237</sup> Lee, D., Chuen, K. and Deng, R. (2017). Handbook of blockchain, digital finance, and inclusion. Academic Press, p.185.

separate blockchains, potentially opening up for several unpatched vulnerabilities.<sup>238</sup> The most prominent third-party threat to the blockchain data-structure and architecture, other than threats generated by the controller, is if the majority of the CPU power is used to attack the network, ultimately leading to the truthful ledger not outpacing the attackers.<sup>239</sup> Such an attack is the equivalent of millions of computers contributing processing power to taking down data centers and are unavoidable, but very unlikely.

The blockchain ensures certain security measures imposed by Article 32(1) in the GDPR. It provides integrity, availability and resilience of the processing systems through its immutable data-structure. Complete confidentiality, on the other hand, is not made possible due to the open nature of the blockchain. The blockchain must also be restored and made available to data subjects in case of a physical or technical incident. The ledgers will remain, but in the event of the P2P-network, e.g. going offline, the controller must have available measures to make the network available to its users. This problem is not something unique to the blockchain, all organizations run the risk of running into network problems, rendering their services unavailable for the data subjects and must, therefore, under the GDPR, have procedures to restore the availability and access.<sup>240</sup> As for avoiding the aforementioned organizational threats, the controller can do so by implementing processes for regular testing and assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing and then patching the vulnerabilities and keeping an up-to-date and securely tested blockchain algorithm.<sup>241</sup> By doing so the controller can increase their security of processing under Article 32 in the GDPR. However, it is still probable that such measures do not make up for the inability to ensure the confidentiality of data, which in turn can be of significance regarding compliance with the regulation.

#### **4.6 Rights of the Individual**

By assessing the core responsibilities of the controller and processor, compliance on an organizational level is examined. Under the GDPR the controller and processor must also fulfill certain requirements and duties towards the individual data subject, which can turn out to be quite troublesome due to the nature of the blockchain.

---

<sup>238</sup> Lee, Chuen and Deng, Handbook of blockchain, digital finance, and inclusion, p. 251 ff.

<sup>239</sup> Kiran, M. and Stannett, M. (2014). Bitcoin risk analysis. Nemode.ac.uk: Research Councils UK, p. 5.

<sup>240</sup> Article 5 in the GDPR.

<sup>241</sup> Article 32(1)(d) in the GDPR.

#### **4.6.1 Right to Information**

The right to information consists of, first and foremost, providing information to the data subject regarding the processing and storage of their personal data.<sup>242</sup> Compliance under such a provision is not dependent on the underlying technology, but rather on the information that the controller chooses to communicate to the data subject. The right to information is expanded by the right to access, through which the data subject can gain in-depth information regarding the lawfulness of processing and how their personal data is handled so that he/she can exercise his/her rights under Articles 16-22 in the GDPR.

#### **4.6.2 Right to Erasure, Rectification and Restriction of Processing**

The GDPR enforced right to erasure gives the data subject the right to request the deletion of their personal data.<sup>243</sup> This fundamental right is in direct conflict with the blockchain. Since the key security feature of the blockchain-data-structure depends on previous transaction data to be stored, removing a piece of data from the structure would render the rest of the data useless.<sup>244</sup> Also, due to the mathematically imposed structure, the processing power required to remove something from the ledger is nearly technologically impossible, making it close to unfeasible for any controller or processor to do so. By the blockchain, you can always append a new transaction that overrides the old transaction data, but the old transaction data will always be a part of the ledger. Regardless of the grounds for which the data subject requires the controller or processor to erase the personal data, it is simply not possible, which in turn means that the obligations of the GDPR cannot be fulfilled and the data subject loses control of their own personal data.<sup>245</sup>

The same conditions apply when the data subject requires that his/her personal data be rectified. Rectification means that data is updated to be accurate. Like previously mentioned, a new transaction can always remedy a wrongdoing in a previous transaction but the previous transaction will remain and cannot be removed. According to Article 16 of the GDPR, it is not made clear if the incorrect data must be deleted for compliance. However, the blockchain does not function like a regular register where new data takes the old data's place, the only way to rectify information is by adding a layer that renders the old data outdated. By blockchain standards, the data has been rectified and corrected and the data subject has the power to be able to request the rectification which in turn means that a literal interpretation could possibly

---

<sup>242</sup> See section 3.5.2.1.

<sup>243</sup> See section 3.5.2.2.

<sup>244</sup> Maxwell and Salmon, A guide to blockchain and data protection, p. 15.

<sup>245</sup> See section 3.5.2.2.

result in the provision being fulfilled. However, a strict interpretation would most likely require that the outdated data be removed, which is technically impossible on the blockchain. The right to restriction of processing is also a fundamental right imposed on the data subject under the GDPR. Since the transaction data consists of an immutable ledger whose purpose is to maintain an accurate depiction of the transaction history, or else the blockchain becomes obsolete, it is not possible to restrict certain data in the ledger from being subject to processing.

In section 4.2.1 when assessing what kind of processes take place on the blockchain, the conclusion was that there are at least three different kinds of processing of data that handle personal data. The two previous paragraphs touched upon the restriction, rectification and erasure of transaction data but the processing of public keys and nodes was not discussed. The rectification of nodes and public keys are not similar to rectification of transaction data. They cannot be factually faulty as they merely are unique combinations of numbers that correlate to a unique user. Also, they cannot become outdated since they are maintained until the user either leaves the network or reconnects and potentially receives a new unique address.<sup>246</sup>

The processing of nodes is done in the register being maintained by the other nodes. If a user wishes to be erased from such a register, or restrict the processing, he/she must leave the P2P-network.<sup>247</sup> Rectification can technically be done by reconnecting to the network if the node is given a new unique address. However, the controller cannot institute or delete addresses as they have no centralized control over how the P2P-network communicates and handles the registers. This leads to the data subjects not being able to practice their individual rights under the GDPR unless the controller embeds automated functionality into the network that fulfills such criteria, while not compromising the nature of P2P-network. The public keys are also unique addresses that are distributed to other users on the blockchain. The erasure of these public keys would undermine the principle of validating transactions through cryptography as the corresponding private key would have no pair and all future transactions would be deemed invalid by the other nodes.<sup>248</sup> However, if an owner of a private key no longer wished to use the key, they could, if implemented in the blockchain algorithm, erase such a key and all related public keys, since they are relevant when validating transactions, but not retroactively. The restriction of processing is made possible by the user not posting any transactions using their private key but

---

<sup>246</sup> See section 2.2.5 and 2.3.5.

<sup>247</sup> See section 2.3.5.

<sup>248</sup> See section 2.3.6.

not possible by requiring the controller to restrict their processing as the use of the public key is entirely dependent on the user's own habits.

#### **4.6.3 Data Portability**

Under Article 20 in the GDPR, the data subject must be able to withdraw their personal data from one system and easily transfer it into another without the controller preventing such an action. However, Article 11(2) in the GDPR states that a controller does not need to fulfill the obligation of data portability if the controller can demonstrate that they are not able to identify the unique data subject. What the legislator means by identifying the unique data subject and if it refers to the legal identity or not has been subject to discussion.<sup>249</sup> First and foremost, data portability only applies to data concerning the data subject which was provided to the controller by him/her.<sup>250</sup> Public keys and nodes are not provided by the data subject but are automatically created by the blockchain algorithm, exempting public keys and nodes from the right to data portability.<sup>251</sup>

As for transaction data, the raw transaction data, before being processed, is most likely committed by the data subject to the blockchain and then processed, pseudonymized and changed into a rather small element of a larger structure.<sup>252</sup> This transaction data can constitute personal data and therefore constitute personal data regarding the data subject.<sup>253</sup> The A29WP states that the term 'provided by' includes personal data that relates to the data subjects activity and that pseudonymous data can be strongly linked to the data subject, which in turn means that the exception in Article 11 (2) in the GDPR does not apply.<sup>254</sup> This implies that transaction data that constitutes personal data, which is pseudonymized and relates to a data subjects specific activities, must be made portable upon request under Article 20 in the GDPR if the processing of such data is automated and based on consent or a contract to which the data subject is part of. The blockchain, by its nature, processes personal data by automated means.<sup>255</sup> However, lawfulness according to the GDPR is not only reached through consent, if the blockchain processes these transactions according to Article 6(1)(f) in the GDPR, where the processing is

---

<sup>249</sup> See, for example: Medium. (2018). Comments on Data Portability guidelines – MyData – Medium. [online] Available at: <https://medium.com/mydata/comments-on-data-portability-guidelines-2102d447f73b> [Accessed 13 Apr. 2018].

<sup>250</sup> Art. 29 Data Protection Working Party (2016) Opinion 04/2017, Guidelines on the right to data portability, WP 242 rev.01, p. 9.

<sup>251</sup> See section 2.3.5.

<sup>252</sup> See section 2.3.3.

<sup>253</sup> Article 20(1) in the GDPR.

<sup>254</sup> A29WP, Opinion 04/2017, p. 10.

<sup>255</sup> See section 4.1.1.

necessary for the purposes pursued by the controller or a third party and override the fundamental rights and principles of the individual data subject, the processor need not make the transaction data portable upon request. The model for lawfulness is individual to each approach, but it is probable that the blockchain falls within the scope of Article 6(1)(f), considering that the purpose is to maintain an immutable register. If individuals could freely withdraw data from such a structure, all other data subject's data would be destroyed and the controller's blockchain would fail. In short, this means that cases where the controller relies on consent to achieve lawfulness instead of the necessity provision introduced above, according to Article 6(1) in the GDPR, the controller is obligated to fulfill data portability requests as per Article 20 in the GDPR. Due to the ledger consisting of blocks, that consist of Merkle trees, that consist of hashed transaction data, the controller will most likely be required to take additional steps to make such transactions into a readable format.<sup>256</sup>

#### **4.6.4 Right to Object and Automated Decision Making**

The right to object consists of the data subject being able to, in some instances, require that all processes regarding their personal data cease.<sup>257</sup> The controller can, however, continue such processing if they are able to demonstrate compelling legitimate grounds and that their interest of processing outweighs the data subjects' rights and freedoms.<sup>258</sup> As proposed in the previous section, the purpose is to maintain an immutable register, and if individuals could freely refuse certain elements from being processed in such a structure, all other data subjects' data would be rendered useless and the controller's blockchain would fail. Therefore, the individual's right to object must be weighed against the implications that such an objection would result in. In a blockchain scenario it is probable that such an objection is not possible and even so, if possible, it would cause all other data subjects' data to be rendered useless, why a controller should be able to demonstrate a compelling interest that outweighs the individual's rights and freedoms.

Automated processing is, as discussed, the core functionality of the blockchain.<sup>259</sup> The data subject has the right to not be subject to automated decision making unless this kind of processing is based on the data subjects' explicit consent.<sup>260</sup> Subsequently, if no such consent is given, the controller/processor is required to stop all automated processing on the data

---

<sup>256</sup> Article 21(1) in the GDPR.

<sup>257</sup> See section 3.5.2.4.

<sup>258</sup> Article 21(1) in the GDPR.

<sup>259</sup> See section 4.2.

<sup>260</sup> Article 22 in the GDPR.

subjects' personal data. That is not possible since all individual ledgers are appended with new transactions by automated means, namely the blockchain algorithm. That means that once a transaction has been made on the blockchain, that same set of data will continuously be subject to processing since the ledgers include all transaction data ever committed.<sup>261</sup> Explicit consent must, therefore, be given, which can also be revoked at any time, otherwise compliance under the GDPR is not achieved.

#### **4.7 Fundamental Principles**

Considering the controllers and processors obligations, as well as the rights of the data subject, it is possible to assess whether the fundamental principles of the GDPR can be complied with.

The first set of principles under the GDPR that enforce lawfulness, fairness and transparency as well as a purpose limitation, are related to how the controller acts towards the data subject.<sup>262</sup> This means that these principles are autonomous to technology and depend case-to-case on each controller and how they act towards the data subjects. Consequentially, an assessment cannot be made on whether blockchain technology is compliant under the GDPR but must be assessed by each individual controller.

The second set of principles relate to the kind of personal data that is stored and how.<sup>263</sup> The principle of data minimization regulates that data is to be kept relevant, adequate and limited to what is necessary.<sup>264</sup> On a blockchain, this is a customizable feature, as the blockchain algorithm dictates e.g. what information is necessary for a transaction to be made.<sup>265</sup> Hence, the controller can assess what data is to be deemed relevant and adequate and limit the data according to that, therefore abiding the principle. Again, this is a principle that widely depends on each individual controller's approach, but compliance can most likely be achieved on the blockchain regarding the principle of data minimization.

The principle of accuracy ensures that data be kept up to date and inaccuracies be deleted.<sup>266</sup> As discussed in section 4.6.2 regarding rectification and erasure, it is not physically possible to delete data from the blockchain-data-structure and updating data is only made possible through

---

<sup>261</sup> See for example: Blockexplorer.com. (2018). Bitcoin Block Explorer. [online] Available at: <https://blockexplorer.com/> [Accessed 19 Apr. 2018]. Where all transactions from the Bitcoin ledger are visible.

<sup>262</sup> Article 5(1)(a-b) in the GDPR.

<sup>263</sup> Recital 39 in the GDPR.

<sup>264</sup> See section 3.5.1.

<sup>265</sup> See section 2.3.3.2.

<sup>266</sup> See section 3.5.1.

committing a new transaction that overrides the old one, but does not delete it. Therefore, it is likely that the principle of accuracy cannot be complied with in a blockchain-data-structure.

The principle of storage limitation dictates that the time the personal data is stored must be kept to a very strict minimum and be held in direct correlation with the fulfillment of the purpose of the processing.<sup>267</sup> Given that the original purpose of processing is to validate and guarantee ownership of a transaction and the maintaining of an immutable ledger comes second to that for the data subject itself, it cannot be motivated that the individuals' data is stored forever and processed in a ledger.<sup>268</sup> Consent is not a valid argument as consent should be revocable, and since the blockchain-data-structure is immutable a consent cannot be revoked.<sup>269</sup> The blockchain does not stand in line with the principle of storage limitation and proving compliance with these principles can be troublesome for controllers on the blockchain.

The principle of integrity and confidentiality aims to ensure that the data subjects' personal data is processed in a secure manner, without unauthorized access and loss of data.<sup>270</sup> As previously stated, the controller and processor can be deemed compliant regarding data protection and security of processing, but not guaranteed regarding some cases of confidentiality, due to the nature of an open distributed blockchain.<sup>271</sup> Complete loss of data is very unlikely on the blockchain due to each individual node maintaining their own ledgers, creating many individual reset points in case of an incident.

The principles collectively constitute the core of the GDPR and are a strict requirement for entities processing personal data. Given that the blockchain most likely fails to comply with the principle of accuracy and principle of storage limitation the controller can have a hard time demonstrating compliance with all the above-mentioned principles, resulting in a failure to comply with their accountability obligations under Article 5(2) in the GDPR. In general, it is submitted that large parts of the GDPR are not compatible with the blockchain since the GDPR does not take regard to immutable data-structures.

---

<sup>267</sup> See section 3.5.1.

<sup>268</sup> Maxwell and Salmon, A guide to blockchain and data protection, p. 14.

<sup>269</sup> Article 7(3) in the GDPR.

<sup>270</sup> Article 5(1)(f) in the GDPR.

<sup>271</sup> See section 4.5.1.

## 4.8 Conclusion

As we have seen during recent years, the individuals' rights have suffered at the expense of the excessive monetization of personal data. The GDPR facilitates a move towards data subjects having the conclusive decision-making power over their personal data and is a landmark in clarifying and protecting the individual from privacy intrusions. As a result of the open distributed blockchain falling within the material scope of the GDPR, the utilization of such technology and the failure to comply with the GDPR might result in an illegal operation.<sup>272</sup> Even though the blockchain foundationally contradicts certain principles in the GDPR, such as rectification and removal, the blockchain strongly conforms with the technical data protection principles according to the GDPR, as the blockchain has proven to be one of the most secure structures. The biggest conflict between the blockchain and the GDPR is the blockchain's immutability. However, its biggest strengths originate from this immutability and the purposes of having an immutable object are in line with some of the GDPR's purposes, namely integrity, security and transparency, but does result in the data subject losing the retroactive control over their personal data. The GDPR assesses these principles as absolute but does not discuss if alternative usage would provide the most security for the individual. The blockchain provides one of the highest security standards to date regarding the integrity of data, but at the cost of data being non-removable. It might be required to address if there is a breaking point where security is achievable at the cost of other principles, enter the blockchain.

---

<sup>272</sup> See section 4.7.

## 5 Final Comment

Even though the GDPR was adopted as late as April 27<sup>th</sup>, 2016, by which the initial blockchain craze had passed, the regulation was finalized without any regard to P2P-networks and the blockchain.<sup>273</sup> By not addressing the conflicts between the blockchain and the GDPR, the EU is setting up for complications when the GDPR is implemented on May 25<sup>th</sup>, 2018. Countries, like Liechtenstein, have stated that the blockchain requires a more light-handed approach due to its disruptiveness, and have proposed an act that specifically targets blockchains.<sup>274</sup>

It is argued that there are two separate paths from here. Firstly, adaptation and secondly, a new regulation. The less attractive alternative, adaptation, would render every existing blockchain illegal under the GDPR and instead focus on future blockchains. By assessing the GDPR when developing a blockchain algorithm the responsibilities and measures to be adopted can be assessed and render the technology compliant on a meta-level.<sup>275</sup> The more attractive alternative, a new regulation or an addition to the GDPR, would acknowledge the immutability of the blockchain, yet require the blockchain algorithm to fulfill certain measures in line with the GDPR's goal of strengthening individual's rights and freedoms. Such implementations could, e.g., be that users can mark personal data before that data is transacted, anonymize such data, establish communication between nodes by not communicating personal data and have users generate new private- and public keys for each transaction to reduce the linkability.

This encapsulates a central problem regarding technological innovation, where legislators fail, because it is not foreseeable, to regulate and include technologies in the legislative advancements. Legal advancements are an ever-changing game of cat and mouse where legislators try to fill voids and clarify uncertainties. On the horizon we can see the advancement of quantum computing rendering all existing data security models, even the blockchain, useless.<sup>276</sup> But for now, quantum computing remains a mystery and cannot be legislated, which is exactly how the blockchain was viewed a couple of years ago.

---

<sup>273</sup> See for example: Barford, V. (2013). Bitcoin: Price v hype. [online] BBC News. Available at: <http://www.bbc.com/news/magazine-25332746> [Accessed 21 Apr. 2018].

<sup>274</sup> Maloney, C. (2018). Liechtenstein PM Proposes Friendly Crypto Regulation With New "Blockchain Act". [online] CCN. Available at: <https://www.ccn.com/more-light-regulation-as-leichtenstein-proposes-moderation-in-their-new-blockchain-act/> [Accessed 21 Apr. 2018].

<sup>275</sup> Jordan, D. (2018). Reconciling Blockchain Technology With Europe's GDPR. [online] ETHNews.com. Available at: <https://www.ethnews.com/reconciling-blockchain-technology-with-europes-gdpr> [Accessed 21 Apr. 2018].

<sup>276</sup> Rafaeli, R. (2018). How quantum computing could wreak havoc on cryptocurrency. [online] The Next Web. Available at: <https://thenextweb.com/contributors/2018/04/14/quantum-computing-wreak-havoc-cryptocurrency/> [Accessed 21 Apr. 2018].

## **6 Bibliography**

### **6.1 Statutes, Conventions and Preparatory Works**

#### **6.1.1 European Union**

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.

Charter of Fundamental Rights of the European Union, 18 December 2000, OJ C 364/01 and [2010] OJ C83/389.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 25.1.2011.

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), OJ L 119, 4.5.2016.

#### **6.1.2 Article 29 Working Party Documents**

Article 29 Data Protection Working Party. (2014). Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, WP 169.

Article 29 Data Protection Working Party. (2014) Opinion 05/2014 on Anonymisation Techniques, WP216.

Article 29 Data Protection Working Party (2016) Opinion 04/2017, Guidelines on the right to data portability, WP 242 rev.01.

### **6.2 Cases**

#### **6.2.1 Court of Justice of the European Union (CJEU)**

Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014], ECLI:EU:C:2014:317, Court of Justice of the European Union.

Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016], 112/16 Luxembourg, Court of Justice of the European Union.

### 6.3 Books

Calder, Alan. *EU GDPR: a pocket guide*. (n.p.): It Governance Pub., 2016.

Cormen, T., Leiserson, C. and Rivest, R. *Introduction to Algorithms*. Cambridge: MIT Press, 2014.

Drescher, Daniel. *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress, Berkeley, CA, 2017.

Farrel, Joyce. *A Beginner's Guide to Programming Logic And Design: Comprehensive*. 7th ed. Course Technology, Cengage Learning, 2013.

Finck, Michèle. *Blockchains and Data Protection in the European Union*. Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 2017.

Forgó, N., Hänold, S. and Schütze, B. "The Principle of Purpose Limitation and Big Data". In: Corrales, M., Fenwick, M. and Forgó, N. (eds.), *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation*. Springer, Singapore, 2017.

Greenstein, Stanley. *Our Humanity Exposed: Predictive Modelling in a Legal Context* (Ph.D. dissertation). Department of Law, Stockholm University, Stockholm, 2017.

Hettne, J. and Otken Eriksson, I. (eds.), *EU-rättslig metod*. Stockholm: Norstedts juridik, 2011.

Hoeren, Thomas. "Big Data and Data Quality". In: Hoeren T. and Kolany-Raiser B. (eds.), *Big Data in Context*. SpringerBriefs in Law. Springer, Cham, 2018.

Holtz, Hajo Michael. *Den nya allmänna dataskyddsförordningen — några anmärkningar*, SvJT, 2018.

Jareborg, Nils. *Rättsdogmatik som vetenskap*. Svensk Juristtidning, 1–10, 2004.

Karegar, Farzaneh. *Towards Improving Transparency, Intervenability, and Consent in HCI* (Doctoral dissertation, Karlstad University Press), 2018.

Klamberg, M., Magnusson Sjöberg, C. and Öman, S. "Skydd av personlig integritet och informationsfrihet". In: Magnusson Sjöberg, Cecilia. (ed.), *Rättsinformatik: juridiken i det digitala informationssamhället*. 1st. ed. Lund: Studentlitteratur, 2015.

Kleineman, Jan. "Rättsdogmatisk metod". In: Korling, F. & Zamboni, M. (eds.), *Juridisk metodlära*. 1st. ed. Lund: Studentlitteratur, 2013.

- Lakoff, G. and Johnson, M. *Metaphors we live by*. Chicago: University of Chicago Press, 1980.
- Lee, D. and Deng, R. *Handbook of Blockchain, Digital Finance, and Inclusion*. Volume 2: ChinaTech, Mobile Security, and Distributed Ledger. Academic Press, 2017.
- Menezes, A., Van Oorschot, P. and Vanstone, S. *Handbook of applied cryptography*. Boca Raton: CRC Press, 1997.
- Morabito, Vincenzo. *Business Innovation Through Blockchain The B<sup>3</sup> Perspective*. Cham: Springer International Publishing, 2017.
- Mougayar, W. & Buterin, V. *The Business Blockchain : Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, Incorporated, New York, 2016.
- Nicolaidou, I.L. and Georgiades, C. *The General Data Protection Regulation: A Law for the Digital Age*. In: Synodinou, TE., Jogleux, P., Markou, C. and Prastitou T. (eds.), *EU Internet Law*. Springer, Cham, 2017.
- Olsen, Lena. *Rättsvetenskapliga perspektiv (Perspectives of Jurisprudence)*, SvJT, 2004.
- Paar, C. and Pelzl, J. *Understanding cryptography*. Berlin: Springer, 2010.
- Reichel, Jane. "EU-rättslig metod". In: Korling, F. & Zamboni, M. (eds.), *Juridisk metodlära*. 1st. ed. Lund: Studentlitteratur, 2013
- Romano, D. and Schmid, G. *Beyond Bitcoin: A Critical Look at Blockchain-Based Systems*. *Cryptography*, 1(2), 2017.
- Sandgren, Claes. *Är rättsdogmatiken dogmatisk?*. *Tidsskrift for Rettsvitenskap*, TfR, 118(4–5), 2005.
- Smart, Nigel. *Cryptography Made Simple*. Cham: Springer International Publishing, 2016.
- Sobolewski, M., Mazur, J. and Paliński, M. *GDPR: A Step Towards a User-centric Internet?*. *Intereconomics*, 52(4), 2017.
- Solove, Daniel. *The Digital Person: Technology and Privacy in the Information Age*. New York University Press, New York, 2004.
- Voigt, P. and Bussche, A. *The EU general data protection regulation (GDPR)*. Cham: Springer International Publishing, 2017.
- Winter, Steven. *A clearing in the forest*. Chicago: University of Chicago Press, 2001.

## 6.4 White Papers

Nakamoto, Satoshi. *Bitcoin: A peer-to-peer electronic cash system* [White paper]. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 18 Apr. 2018], 2008.

Okupski, Krzysztof. *Bitcoin Developer Reference Working Paper* [White paper]. Available at: [https://lopp.net/pdf/Bitcoin\\_Developer\\_Reference.pdf](https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf) [Accessed 19 Apr. 2018], 2016.

## 6.5 Journals and Articles

Barford, Vanessa. *Bitcoin: Price v hype*. [online] BBC News, 2013. Available at: <http://www.bbc.com/news/magazine-25332746> [Accessed 21 Apr. 2018].

Bygrave, Lee. *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*. Oslo Law Review, Volume 4, No. 2, 2017.

Dorit, R. and Adi, S. *Quantitative Analysis of the Full Bitcoin Transaction Graph*. [online] Eprint.iacr.org, (n.d.). Available at: <https://eprint.iacr.org/2012/584.pdf> [Accessed 19 Apr. 2018].

Dulong de Rosnay, Melanie. *Peer-to-peer as a design principle for law: distribute the law*. Journal of Peer Production, Disruption and the Law, 2015.

Icann.org. *Beginner's Guide To Internet Protocol (IP) Addresses*. Internet Corporation for Assigned Names and Numbers (ICANN), 2011. Available at: <https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf> [Accessed 19 Apr. 2018].

Jordan, Daniel. *Reconciling Blockchain Technology With Europe's GDPR*. [online] ETHNews.com, 2018. Available at: <https://www.ethnews.com/reconciling-blockchain-technology-with-europes-gdpr> [Accessed 21 Apr. 2018].

Kiran, M. and Stannett, M. *Bitcoin risk analysis*. Nemode.ac.uk: Research Councils UK, 2014

Maloney, Conor. *Liechtenstein PM Proposes Friendly Crypto Regulation With New "Blockchain Act"*. [online] CCN, 2018. Available at: <https://www.ccn.com/more-light-regulation-as-leichtenstein-proposes-moderation-in-their-new-blockchain-act/> [Accessed 21 Apr. 2018].

Maxwell, W. and Salmon, J. *A guide to blockchain and data protection*. [online] Hlengage.com, 2017. Available at: [https://www.hlengage.com/\\_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf](https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf) [Accessed 19 Apr. 2018].

Merkle, Ralph. "Protocols for public key cryptosystems" In: Symposium on Security and Privacy, IEEE Computer Society, 1980.

Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G. and Herrera-Joancomartí, J. *Double-spending Prevention for Bitcoin zero-confirmation transactions*. [online] Department of Information Engineering and Communications, Universitat Autònoma de Barcelona, 2017. Available at: <https://eprint.iacr.org/2017/394.pdf> [Accessed 12 May 2018].

Reid, F. and Harrigan, M. *An Analysis of Anonymity in the Bitcoin System. Security and Privacy in Social Networks*. 3.10.1109/PASSAT/SocialCom.2011.79, 2012.

Twobirds.com. *Guide to the General Data Protection Regulation*. [online], 2018. Available at: <https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en> [Accessed 19 Apr. 2018].

## 6.6 Electronic Sources and Web Pages

Bits on blocks. *A gentle introduction to immutability of blockchains*. [online], 2018. Available at: <https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/> [Accessed 19 May 2018].

Blockchain-basics.com. *Hashing*. [online], 2018. Available at: [http://blockchain-basics.com/Hashing.html?hash\\_input=Hello+everyone%21](http://blockchain-basics.com/Hashing.html?hash_input=Hello+everyone%21) [Accessed 16 Apr. 2018].

BlockchainHub. *Blockchains & Distributed Ledger Technologies*. [online], 2018. Available at: <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/> [Accessed 19 Apr. 2018]. [www.tutorialspoint.com](http://www.tutorialspoint.com).

Blockexplorer.com. *Bitcoin Block Explorer*. [online], 2018. Available at: <https://blockexplorer.com/> [Accessed 19 Apr. 2018].

Coinmarketcap.com. *Global Charts / CoinMarketCap*. [online], 2018 Available at: <https://coinmarketcap.com/charts/> [Accessed 19 Apr. 2018].

Cox, T. and Solomon, A. *Block chain: Is the GDPR out of date already?* | Lexology. [online] Lexology.com, 2018. Available at: <https://www.lexology.com/library/detail.aspx?g=d4c0481a-c678-4748-80cb-4ab917e66207> [Accessed 19 Apr. 2018].

Deng, Boer. *People can be identified through their credit-card transactions.* [online], 2018. Available at: <https://www.nature.com/news/people-identified-through-credit-card-use-alone-1.16817> [Accessed 19 Apr. 2018].

European Data Protection Supervisor. *A - European Data Protection Supervisor.* [online], 2018. Available at: [https://edps.europa.eu/data-protection/data-protection/glossary/a\\_en](https://edps.europa.eu/data-protection/data-protection/glossary/a_en) [Accessed 20 Apr. 2018].

European Data Protection Supervisor. *Guidelines on the protection of personal data in IT governance and IT management of EU institutions.* [online], 2018. Available at: [https://edps.europa.eu/sites/edp/files/publication/it\\_governance\\_management\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf) [Accessed 19 May 2018].

Gibbs, Samuel. (2018). *Child abuse imagery found within bitcoin's blockchain.* [online] the Guardian, 2018. Available at: <https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content> [Accessed 19 Apr. 2018].

Hodge, Mark. *Who is Satoshi Nakamoto?* Bitcoin inventor whose identity remains a secret. [online], 2018. The Sun. Available at: <https://www.thesun.co.uk/news/5037060/satoshi-nakamoto-bitcoin-inventor-richest-world/> [Accessed 19 Apr. 2018].

Medium. *Comments on Data Portability guidelines – MyData – Medium.* [online], 2018. Available at: <https://medium.com/mydata/comments-on-data-portability-guidelines-2102d447f73b> [Accessed 13 Apr. 2018].

Medium. *Merkle Tree Introduction – Evan Kozliner – Medium.* [online], 2018. Available at: <https://medium.com/@evankozliner/merkle-tree-introduction-4c44250e2da7> [Accessed 19 Apr. 2018].

Medium. *The Meaning of Decentralization – Vitalik Buterin – Medium.* [online], 2018. Available at: <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274> [Accessed 18 Apr. 2018].

Miles, Curtis. Blockchain security: *What keeps your transaction data safe?* - *Blockchain Unleashed*: IBM Blockchain Blog. [online] Blockchain Unleashed: IBM Blockchain Blog, 2018. Available at: <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/> [Accessed 11 Apr. 2018].

Oxford Living Dictionaries. (2018). [online] Oxford University Press. Available at: <https://en.oxforddictionaries.com/definition/integrity> [Accessed 11 May 2018].

Rafaeli, Raz. *How quantum computing could wreak havoc on cryptocurrency*. [online] The Next Web, 2018. Available at: <https://thenextweb.com/contributors/2018/04/14/quantum-computing-wreak-havoc-cryptocurrency/> [Accessed 21 Apr. 2018].

Roberts, D. and Finance, Y. *The 11 biggest names in cryptocurrency right now*. [online] Finance.yahoo.com, 2018. Available at: <https://finance.yahoo.com/news/11-biggest-names-cryptocurrency-2017-110033921.html> [Accessed 19 Apr. 2018].

Rouse, Margaret. *Confidentiality, integrity, and availability (CIA triad)*. [online] WhatIs.com, 2018. Available at: <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> [Accessed 20 May 2018].

Softcat.com. *GDPR – A guide to key articles for security & privacy professionals*. [online], 2018 Available at: [https://www.softcat.com/assets/uploads/pdfs/gdpr/whitepaper\\_hunton\\_williams\\_gdpr\\_key\\_articles\\_guide\\_en.pdf](https://www.softcat.com/assets/uploads/pdfs/gdpr/whitepaper_hunton_williams_gdpr_key_articles_guide_en.pdf) [Accessed 19 Apr. 2018].

TutorialsPoint. *Perl Basics: Perl References*. [online], 2018. Available at: [https://www.tutorialspoint.com/perl/perl\\_references.htm](https://www.tutorialspoint.com/perl/perl_references.htm) [Accessed 16 Apr. 2018].

Web.archive.org. *All Currencies / Crypto-Currency Market Capitalizations*. [online], 2018. Available at: <https://web.archive.org/web/20170115051728/http://coinmarketcap.com/all/views/all/> [Accessed 19 Apr. 2018].