

Protection of Personal Data in Blockchain Technology

*An investigation on the compatibility of the General Data Protection Regulation
and the public blockchain*

Amelia Wallace

Department of Law
Master's Thesis, 30 HE credits
Area: Law and Informatics
Master's Program in Law (270 HE)
Autumn term 2018
Group mentor: Johan Axhamn
Swedish title: Personuppgiftsskyddet i Blockkedjeteknik
– En utredning om förenligheten av dataskyddsförordningen och
den publika blockkedjan



**Stockholm
University**

Abstract

On 25 May 2018 the General Data Protection Regulation, GDPR, came into force in the EU. The regulation strengthened the rights of the data subjects' in relation to the data controllers and processors and gave them more control over their personal data. The recitals of the GDPR state that it was the rapid development in technology and globalisation that brought new challenges for the protection of personal data. Private companies and public authorities were making use of personal data on an unprecedented scale in order to pursue their own activities. The protection should be technologically neutral and not dependant on the technique used. This leads to questions on whether the protection that is offered through the GDPR is de facto applicable on all technologies. One particular technology which has caught interest of both private companies and public authorities is the blockchain. The public distributed blockchain is completely decentralized, meaning it is the users who decide the rules and its content. There are no intermediaries in power and the transactions of value or other information is sent peer to peer. By using asymmetric cryptography and advanced hash algorithms the transactions sent in the blockchain are secured. Whilst the interest and use of blockchain is increasing and the GDPR attempting to be applicable on all techniques, the characteristics of the public blockchain must be analysed under the terms of the GDPR. The thesis examines whether natural persons can be identified in a public blockchain, who is considered data controller and data processor of a public blockchain and whether the principles of the GDPR can be applied in such a decentralised and publicly distributed technology.

Keywords

General Data Protection Regulation, Blockchain, Transparency, Technology Neutrality, Personal Data, Data Controller, Data Processor.

Sammanfattning

Den 25 maj 2018 trädde den nya dataskyddsförordningen, GDPR, i kraft i EU vilken slog hårdare mot personuppgiftsansvariga och personuppgiftsbiträden än vad det tidigare dataskyddsdirektivet gjort. Med reformen ville EU stärka personuppgiftsskyddet genom att ge de registrerade mer kontroll över sina personuppgifter. I skälen till förordningen anges att det var den snabba tekniska utvecklingen och globaliseringen som skapat nya utmaningar för skyddet då privata företag och offentliga myndigheter använder personuppgifter i en helt ny omfattning idag. Skyddet bör således vara teknikneutralt och inte beroende av den teknik som används. Detta öppnar upp för frågor om huruvida skyddet som GDPR erbjuder faktiskt är applicerbart på samtliga tekniker. En särskild teknologi som fångat intresse hos såväl privatpersoner som företag och offentliga myndigheter är blockkedjan. Den öppet distribuerade blockkedjetekniken är helt decentraliserad, vilket innebär att det är dess användare som styr och bestämmer över innehållet. Några mellanmän finns inte, utan värdetransaktioner och andra överföringar av information sänds direkt mellan användare. Genom asymmetrisk kryptografi och avancerade hash algoritmer säkras de överföringar som sker via blockkedjan. Något som uppmärksammas under den ökande användningen och intresset för blockkedjan samt ikraftträdandet av GDPR är hur personuppgifter bör hanteras i en sådan decentraliserad teknologi, där inga mellanmän kan bära ansvaret för eventuell personuppgiftsbehandling. Flera av den publika blockkedjeteknikens egenskaper bör problematiseras, framför allt dess öppenhet och tillgänglighet för varje person i världen, samt dess förbud mot rättelse och radering av inlagda data. Denna uppsats behandlar frågorna huruvida fysiska personer kan identifieras i en publik blockkedja, vem som kan anses vara personuppgiftsansvarig och personuppgiftsbiträde i en publik blockkedja, samt om de principer och krav som uppställs i GDPR kan efterlevas i en sådan decentraliserad och öppet distribuerad teknologi.

Nyckelord

Dataskyddsförordningen, Blockkedja, Transparens, Teknikneutralitet, Personuppgift, Personuppgiftsansvarig, Personuppgiftsbiträde.

Abbreviations

Art 29. WP	Article 29 Data Protection Working Party
BTC	Bitcoin
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
EU	European Union
GDPR	General Data Protection Regulation
i.e.	Id est (Latin), that is
IT	Information Technology
TFEU	Treaty of the Functioning of the European Union

Table of Contents

- 1 Introduction 1**
 - 1.1 Background 2
 - 1.2 Legal Issues 3
 - 1.3 Aim and Legal Questions..... 4
 - 1.4 Delimitations 4
 - 1.5 Method & Material 5
 - 1.6 Outline..... 7

- 2 Basics of Blockchain Technology 9**
 - 2.1 Creating Bitcoin and the Blockchain..... 9
 - 2.2 Peer-to-Peer Networks and Software Architecture 10
 - 2.3 Concept of the Blockchain 11
 - 2.4 Structure of the Blockchain..... 12
 - 2.5 Hashing the Block 13
 - 2.6 Merkle Tree 15
 - 2.7 Data Miners 15
 - 2.8 Block Reward Schedule 16
 - 2.9 Proof-of-Work 17
 - 2.10 Block Header 17
 - 2.11 Accessing the Blockchain 19
 - 2.12 Different Types of Blockchains..... 19
 - 2.13 Summary 20

- 3 General Data Protection Regulation..... 21**
 - 3.1 Scope of the GDPR 21
 - 3.2 Subject of the GDPR..... 22
 - 3.3 Complying with the GDPR..... 24
 - 3.3.1 Personal Data 25
 - 3.3.2 Lawfulness 26
 - 3.3.3 Principles 26
 - 3.3.4 Rights of the Data Subject..... 27
 - 3.3.5 Adequate Level of Security 28
 - 3.4 Summary 28

- 4 Identifying Personal Data in the Blockchain 29**
 - 4.1 Anonymised Data 29
 - 4.2 Direct or Indirect Personal Data 30
 - 4.3 Identifiers 31
 - 4.4 Transaction Data 32

4.5 Summary	33
5 Data Controller and Processor of the Blockchain.....	35
5.1 Founder of a Blockchain.....	36
5.2 Users of a Blockchain	37
5.3 Miners of a Blockchain	39
5.4 Summary	40
6 Applying the GDPR Principles in Blockchain Technology	42
6.1 Purpose Limitation.....	42
6.2 Lawfulness, Fairness, Transparency and Accountability.....	42
6.3 Data Minimisation, Accuracy and Storage Limitation	44
6.4 Integrity and Confidentiality	45
6.5 Summary	46
7 Discussion and Conclusions.....	48

1 Introduction

“Everything that can be invented has been invented” is a famous quote claimed to have been expressed by Charles H. Duell in 1899 during his tenure as the US Commissioner of Patents. The quote is often referred to, although its truthfulness is debated, since it reflects our faith in the present as the obvious and the future as something elaborate and abstract.¹ In fact, and far more inspiring, Duell said in 1902 *“In my opinion, all previous advances in the various lines of invention will appear totally insignificant when compared with those which the present century will witness. I almost wish that I might live my life over again to see the wonders which are at the threshold.”*²

The words of Duell brings to mind the time when internet was in its infancy and only a few believed its ability. Nowadays the internet is used frequently even though the technology behind it is still difficult for some to grasp. And today, a fairly new technology is here, by some called the next generation of the internet, and it is called blockchain.³

The blockchain technology in itself is not as known and discussed as its first implementation, the Bitcoin blockchain. Bitcoin is a digital currency and is by many acknowledged as being the most secure and stable blockchain, since it has been operating constantly since 2009 and not failed once.⁴ However, the blockchain technology is now starting to move past cryptocurrencies and closer to companies and organisations in the world. In fact, 26 member states of the European Union (EU) including Norway signed a declaration on 10 April 2018 creating the European Blockchain Partnership to cooperate in the establishment of a European Blockchain Services Infrastructure supporting the delivery of cross-border digital public services, with the highest standards of security and privacy.⁵ The European Commission have already invested more than 80 million euro in projects supporting the use of blockchain in technical and societal areas and approximately another 300 million euro is estimated to be allocated to blockchain by

¹ Lovén, Linus, Bitcoin – en finansiell revolution, page 37.

² The Friend: a religious and literary journal, episode 76 (1902), page 28.

³ Singh, Prakhar, Blockchain: Next Generation of the Internet, 2 October 2018.

⁴ De Geer, Christoffer, Bitcoin och blockkedjan - En begriplig överblick, s. 47.

⁵ News on 'Digital Single Market', webpage of the European Commission, 10 April 2018, Digibyte, available on <https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership> (accessed on 4 January 2019).

2020.⁶ Safe to say is that the EU is interested in learning more about the new technology and its possibilities.

Not only is the EU interested in joining the technology development, but also in making sure the member states' law on information and communication technology are harmonized and up to date. On 25 May 2018 the General Data Protection Regulation (GDPR) came into force as part of the data protection reform.⁷ The GDPR replaced the previous data protection directive⁸ and became applicable in all member states in order to harmonize data protection law and strengthen the rights of the data subjects in relation to the processing of their personal data.⁹ At the very core of the GDPR is the vision of transparency towards the data subjects which is a fundamental principle for the data controller when processing personal data.¹⁰ As the EU focuses on transparency through legislation, developments in technology are moving faster and faster. The blockchain offers also transparency by creating a user-based database where anyone can trade information or value with whomever they want and verify these transactions publicly. The difference is that the GDPR focuses on the obligations and responsibilities of a data controller and processor, whereas the blockchain uphold transparency by giving people back control over their assets and offering a transaction database without intermediaries.

Briefly explained, the blockchain is a distributed database processing an unlimited amount of transactions, possibly filled with personal data. Even though the transactions are secured through advanced cryptography making the record of transactions immutable, the question remaining is whether the blockchain or the transaction data contain personal data, and, if so, is who would be the data controller and processor of such decentralised database, and, is it at all possible to be compliant with the GDPR?

1.1 Background

The blockchain allows transactions of assets without any intermediaries and has the potential to entirely change the way we trade with each other. The technology is new, however its origin and development rests on a very human story.¹¹ Mankind developed trade to exchange

⁶ Ibid.

⁷ 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).

⁸ 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.

⁹ Recital 11 of the GDPR.

¹⁰ Recital 39 and Article 5(1)(a) of the GDPR.

¹¹ De Geer, page 9 ff.

necessities with each other. Trading a horse with two cows had its obvious problems which led to different symbols representing value, such as runestones, gold or silver. As trades became more complex and distance grew between the trading parties, both public and private institutions like governments and banks were born. Industries started evolving to keep people's assets safe and secure, while earning a fair share on the deals. When the internet came, some of these intermediaries were put online. Platforms such as eBay and Amazon are even faster and more efficient than we could have imagined in a time before the internet. By publicly rating the seller on eBay or our Uber driver we reduce or increase the credibility of the counterparty in order to create trust when trading without intermediaries.

Going from more informal rules to using institutions as a tool in economics, humans have found a way of lowering uncertainty and mistrust by giving the responsibility to governments, banks and other companies to be able to trade assets.¹² However, as these intermediaries have grown larger and stronger, our personal control over our assets have decreased. The GDPR is a proof of the fact that individuals lack sufficient control over their personal data in relation to the intermediaries acting as data controllers. Technology is now allowing us to trade without intermediaries and still keeping trust, control and safety of our own assets. The blockchain technology can be like an open book filled with transactions, similar to a bank's database, only it is available for everyone, similar to the Internet, and it is controlled by everyone who is using it, like on Wikipedia or in a shared Google Drive document.¹³

1.2 Legal Issues

With the GDPR in force and the data protection directive repealed, the protection of personal data has been extended to reflect changes in technology and the ways organisations collect personal data.¹⁴ Since the GDPR is strictly focused on responsibilities of the data controller and its processors, the question rises on how to protect personal data kept in the blockchain when no intermediaries are in control. As the public distributed blockchain is constructed today there is a risk that the technology is incompatible with the objectives and fundamental principles of the GDPR as all data processed in the blockchain are available for an unlimited amount of people. However, the GDPR and the blockchain share the same purpose which is essential for their very existence, namely the focus on transparency, security of data and giving natural persons more control in relation to intermediaries. If the technology would comply with the

¹² Ibid.

¹³ De Geer, page 16.

¹⁴ Recital 6 of the GDPR.

GDPR, the possibilities of blockchain could rather strengthen the protection of personal data than threaten it. It is therefore of great importance that the technology is explained and analysed in a legal perspective. Furthermore, the GDPR aims to be technologically neutral and should not depend on the techniques used, in order to prevent creating a serious risk of circumvention in the protection of natural persons.¹⁵ This concludes that the GDPR, indirectly, aims to be applicable on the blockchain.

One could argue that the public blockchain is still in its infancy and that we yet do not know entirely how or if the technology will be used further than the implementations of cryptocurrencies that we have seen. It is correct that a lot of experiments will take place and probably fail before we can see the useful cases for the technology. However, there are a lot of organisations working on blockchain and its areas of usage, such as financial institutions, tech companies, start-ups and universities.¹⁶ It is not only an economic revolution but also an innovation in computer science.

1.3 Aim and Legal Questions

The aim of the thesis is to describe and clarify the legal challenges in protecting personal data in a public blockchain and analyse whether the objectives of the GDPR can be upheld in such a decentralized technology. The following questions will therefore be answered:

1. Under which circumstances can a natural person directly or indirectly be identified in a public blockchain in accordance with the GDPR?
2. Who, if anyone, constitute the data controller and, if applicable, processor of the processing of personal data in a public blockchain according to the GDPR?
3. Is it possible to comply with the principles related to Article 5 of the GDPR in a public blockchain?

1.4 Delimitations

The target audience of the thesis are lawyers with a basic understanding of the discipline of information technology (IT) law. Therefore, the technology will not be explained in detail but only to the necessary extent. The blockchain is interesting in many ways. The purpose of the

¹⁵ Recital 15 of the GDPR.

¹⁶ See for example the investigation under Swedish government on blockchain technology as a tool for digitalization, SOU 2018:25 Juridik som stöd för förvaltningens digitalisering. Read also article on how blockchain can change the art market; What Does Blockchain Mean for the Art Market?, MutualArt, 8 november 2018.

thesis, however, is to analyse the legal perspective of the blockchain and not its technical structure or economic use. Further, the thesis targets only distributed blockchains, which are made public and available to anyone, in order to keep the thesis focused on the legal aspect of a network where each user is treated equal and where the purpose is to have no central controller held responsible. The thesis may however be relevant to permissioned or private blockchains where there are a limited number of users with access, since the GDPR would apply on such technology as well. The technology is mainly the same in private blockchains as in public ones, however what sets them apart is the rules on who is allowed access the blockchain and who validates the transactions. In some extent the private blockchain will inevitably be analysed in comparison with the public blockchain in order to highlight the characteristics and architecture of the public blockchain.

The Bitcoin blockchain in particular will not be described in detail or analysed since it would limit the thesis to a blockchain that is currently up and running and only deals with transferring a digital currency. The thesis focuses rather on the technology *behind* Bitcoin and aims to frame the legal issues possible to arise in the future, regardless of what kind of value or information is transferred in the blockchain. By only describing the Bitcoin blockchain the reader would not understand the abilities of the blockchain and how it can be used in other organisations outside of the cryptocurrency market. However, the Bitcoin blockchain is a great example of a functioning blockchain and it will be used as a practical example regularly in the thesis as there are a lot of material to study regarding the Bitcoin blockchain and how its protocol is programmed. The thesis will not explain how to buy Bitcoin, get a Bitcoin wallet, the value of Bitcoin or any other topic related to cryptocurrencies.

Other topics that will not be dealt with in the thesis are questions regarding smart contracts, since the focus of the thesis is rather data protection law than contract law. Questions on national security or information security in general will not either be dealt with, which would be relevant for example in governmental use of the blockchain.

1.5 Method & Material

The method used when working and writing on the thesis is in general a legal analytical method, and due to the subject of the thesis, the legal informatic method in particular, where focus lies on the relationship between law and IT. The legal informatic method is inter alia about practically joining the development of IT architecture with legal competence, in order to comply

with legal demands.¹⁷ Accordingly, the thesis will start off with clarifying established EU law and other sources of law on the area of personal integrity and personal data privacy using a legal dogmatic method where the established sources of law are examined. Thereafter, the law and its underlying principles and means will be analysed with the perspective and in regard of the digital era we are currently exploring, to what extent the law and existing technology comply, and which legal challenges are to be solved.

There is reason to shortly state that IT law is not a traditional area of law and not by everyone acknowledged as a separate legal discipline.¹⁸ Nevertheless, IT law concerns the principles of how IT is used and how established law is functioning in digital environments.¹⁹ The legal dogmatic method is mainly focusing on describing the law as it is with guidance of the established sources of law, by interpreting and clarifying the structure of the law.²⁰ By applying the legal dogmatic method, the aim of the thesis will not be achieved, since a mere clarification of established law would not answer the research questions of the thesis since the technology is fairly new and has not been ruled on in the courts of the EU. With the legal analytical method however, the thesis will analyse the law from a technical perspective where the writer will criticize it with a starting point that the law and technology might not cooperate. From that perspective, the legal analytical method is more advantageous since it allows basically all types of sources, in comparison with the legal dogmatic method.²¹ Arguments from non-traditional rules and foreign sources of law create a possibility to criticize the law without necessarily determining what is established or clarified, but rather how it works and how it can be improved. By looking at the law from an analytical perspective it can be reviewed without necessarily giving one right answer or the best answer.²²

Regarding the material, the thesis processes a great variety of sources in order to answer the research questions. Mainly articles of the GDPR and legal cases from the Court of Justice of the European Union (CJEU) will be processed. Due to the subject of the thesis landing in the border between law and technology, some non-legal sources will be used to describe the blockchain technology and how it works such as literature on how the Bitcoin blockchain functions. Non-established sources of law are also used such as guidelines from data protection authorities, legal publications or opinions and suggestions from practising lawyers in the IT law

¹⁷ Magnusson Sjöberg, Cecilia, *Rättsinformatik: Juridiken i det digitala informationssamhället*, page 27.

¹⁸ *Ibid.*, page 27 f.

¹⁹ *Ibid.*, page 23.

²⁰ Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare: ämne, metod, material och argumentation*, page 48–50.

²¹ *Ibid.*, page 50.

²² *Ibid.*, page 51.

field. Any news articles or other debating publications are used only to highlight various issues and to convey trends, perceptions or events of matter.

A great amount of soft law material is collected from the guidelines of two specific data protection regulators, namely the Article 29 Working Party (Art. 29 WP) and Commission Nationale de l'Informatique et des Libertés (CNIL). When writing the thesis, the GDPR was applicable only a few months ago, and the CJEU and other courts or data protection authorities in the EU have not yet brought many new leading cases or recommendations to help clarify the new regulation and its application on decentralized data architecture, neither have the legal doctrine had much to say about it. In this sense, soft law material such as guidelines are of great relevance when interpreting the GDPR. The Art. 29 WP was an organisation consisting of representatives from the data protection authorities of each EU Member State, the European Data Protection Supervisor and the European Commission. It had an advisory status and acted independently.²³ It was set up due to Article 29 of the data protection directive and its tasks are described in Article 30 of the same directive.²⁴ Although it was replaced by the European Data Protection Board under the implementation of the GDPR, the guidelines are still of relevance because of its great knowledge on the area and since it represented the member states authority powers.²⁵ Their guidelines are still frequently used by IT lawyers when interpreting the GDPR and will therefore be used in the thesis. The CNIL is the French data protection authority who on 6 November 2018 became one of the first data protection authorities in the EU to issue written guidance on the intersection of the use of blockchain technology and the GDPR. The guidance provides some clarification on certain addressed issues, although it leaves a great amount of questions unanswered for further response at European level, in particular when it comes to public blockchains.²⁶

1.6 Outline

The next chapter will describe the basics of the blockchain technology, to the extent that is needed to understand and answer the research questions. The chapters where the research questions are clarified and analysed, i.e. chapter two to six, will begin with an introduction and end with a summary. Chapter three will go through the main structure and content of the GDPR

²³ About Article 29 Data Protection Working Party, 12 December 2017, available on (http://ec.europa.eu/justice/article-29/documentation/index_en.htm) (accessed 3 January 2019).

²⁴ 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.

²⁵ About EDPB, available on https://edpb.europa.eu/about-edpb/about-edpb_en (accessed 3 January 2019).

²⁶ Commission Nationale de l'Informatique et des Libertés, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, 6 november 2018.

in more general terms. Chapter four will address the first research question regarding the direct or indirect identification of personal data in the blockchain. Chapter five will continuously analyse who may constitute the data controller and data processor where personal data is processed in the blockchain. Chapter six will bind the technology together with the objectives of the GDPR in order to analyse whether the GDPR can be upheld in such a decentralised technology. Finally, there will be a discussion and conclusion chapter in chapter seven where the research questions will be answered more concrete and some other, more general, questions arising throughout the thesis will be dealt with finally, in particular regarding EU's view on integrity and movement of data. However, some analysis will take place along the analysis.

2 Basics of Blockchain Technology

There is no established definition of a blockchain in EU legislation or regulation as it is a fairly new phenomenon. However, some governments and authorities within the EU are realizing that the technology is increasing in its use and therefore some explanations can be found in legal context. In the investigation under Swedish government on jurisprudence as a tool for digitalization, the blockchain technology was explained as a combination of known technical building blocks from computer science and cryptography in a new way.²⁷ In the recommendation of the CNIL, a blockchain is somewhat defined as “... a database in which data is stored and distributed to a large number of computers and in which all entries, called “transactions” are visible to all users. A blockchain is not, in itself a data processing operation with its own purpose; it is a technology which can serve in a diverse range of processing operations.”²⁸

The blockchain is thus not in itself a “thing” or a “gadget”, but a collection, development and use of already existing techniques and basic tools. To further understand this technology, where it came from and how it is structured, the basics of blockchain will be explained in the following.

2.1 Creating Bitcoin and the Blockchain

In 2008 Satoshi Nakamoto published the Bitcoin white paper, proposing a system for electronic transactions without relying on trust.²⁹ The nine page document created and deployed Bitcoin’s original reference implementation. The identity of Satoshi Nakamoto is unknown and whether Nakamoto is a he, a she, a company or a group of persons has not yet been revealed.³⁰ Keeping its identity is not such a bad idea, since Nakamoto is said to be sitting on billions of dollars earned in mining Bitcoin.³¹ By implementing Bitcoin, the underlying blockchain database was developed for the first time and has been up and running ever since the first genesis block was verified on the 3rd of January 2009.³² However, not once is the word ‘blockchain’ mentioned in the white paper. The closest Nakamoto came to express the word was in phrases such as

²⁷ SOU 2018:25, Juridik som stöd för förvaltningen, page 151 f.

²⁸ Commission Nationale de l’Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data.

²⁹ Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

³⁰ Hallows, Becca, Who is the REAL Satoshi Nakamoto?, 28 February 2018.

³¹ Wile, Rob, Bitcoin's Mysterious Creator Appears to be Sitting On a \$5.8 Billion Fortune, 31 October 2017.

³² See timestamp of the first Bitcoin block. For example on

<https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

“proof-of-work chain”, “blocks are chained” or “a chain of blocks”.³³ It was only after a few years, around 2015, when the term was more established in investing companies.³⁴ The purpose was to find a new way for people and organisations to trade without needing banks and other intermediaries to trust for the safety and validity of the transactions. Nakamoto came up with a protocol, using already existing techniques, that offered a peer-to-peer network which decentralized trading and solved the so-called double-spending problem. Double spending can be described as a potential flaw mainly in a digital cash system, where the same digital token can be spent more than once due to the fact that digital files can be duplicated or falsified.³⁵

2.2 Peer-to-Peer Networks and Software Architecture

The blockchain is a *peer-to-peer* network. According to the Cambridge Dictionary, a *peer* means an equal. Someone who has the same abilities as other people in a group.³⁶ Like the wording, a peer-to-peer network refers to a non-hierarchical network, a sort of architecture within computer science where participation and tasks are divided equal between peers.³⁷ When it comes to computer science, each system component is called a computer *node*. A node represents either devices or data points. A computer acts as a node since it has an IP address, but also every link that is clicked on, for example on a company’s webpage, since it holds part of a larger data structure.³⁸ A peer-to-peer network is an example of nodes acting in a *decentralized* software architecture. Decentralized system architecture is what it sounds like, a system where the power or responsibility is allocated to each individual node. The opposite is a *centralised* system architecture where the functions are carried out through a central element.³⁹ It is important for the reader to understand at this point that there are two major ways of organizing software systems.

³³ Nakamoto, page 1, 3 and 7.

³⁴ Burniske, Chris, and Tatar, Jack, *Cryptoassets - The Innovative Investor’s Guide to Bitcoin and Beyond*, page 24–25.

³⁵ Dreschder, Daniel, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, page 51.

³⁶ Cambridge Dictionary, viewed on 24 november 2018. Available on <https://dictionary.cambridge.org/dictionary/english/peer>

³⁷ Dreschder, page 14 f.

³⁸ Ibid.

³⁹ Dreschder, page 11.

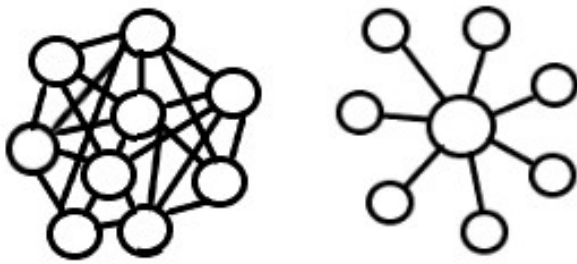


Image 1: This figure illustrates the difference of decentralized (left) and centralized (right) software architecture. The circles represent the nodes and the lines between them represent the connection between them.

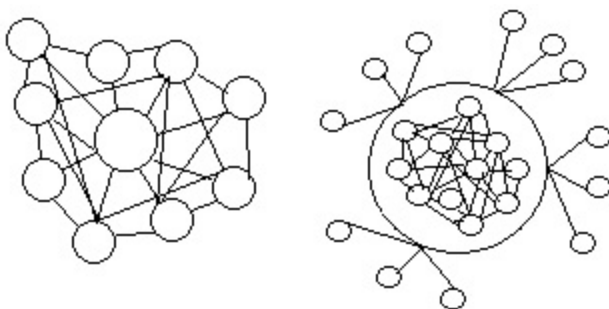


Image 2: This figure illustrates two examples where the two types of architecture have been mixed. On the left-hand side the architecture looks decentralized at first glance but by taking a closer look at the lines connecting the circles you might see that it is actually a centralized architecture. On the right-hand side the architecture looks centralized at first, but really represents a decentralized architecture as well since the central component contains a decentralized system inside.

In the blockchain each node represents a user of the network. No user has a specific role and all users interact on the same terms, meaning they are both suppliers and consumers of resources.⁴⁰

2.3 Concept of the Blockchain

The blockchain is often referred to as a public ledger.⁴¹ A ledger is traditionally a book or a computer file for recording economic transactions in accounting. It can also be a database which describes the blockchain well since it allows anyone to view the transactions made in it. Therefore, the blockchain can be described as a tool for achieving integrity in a decentralized software architecture.⁴² Keep in mind the reference of the blockchain as a public ledger when

⁴⁰ Dreschder, page 11.

⁴¹ Lovén, page 58.

⁴² Drescher, page 34 ff.

understanding the *concept* of blockchain. However, from now on the thesis will be referring to it only as ‘blockchain’ to avoid confusion.

2.4 Structure of the Blockchain

The blockchain is structured as a back-linked list of blocks where each block refers back to the previous block.⁴³ It is often visualized as a horizontal chain, as on the image below, where each block contains several transactions. The first block serves as the *genesis block*, which is the first block of transactions ever confirmed in that specific blockchain. When the next block is verified it will be the *parent block* of the previous block. To “link” the blocks together, each block contains a reference to its parent block. Designing the blocks this way, a “chain” is created where, if you change the data of one block, the whole chain will have to change. Finally, the latest block will be referred to as *the most recently added block*.⁴⁴

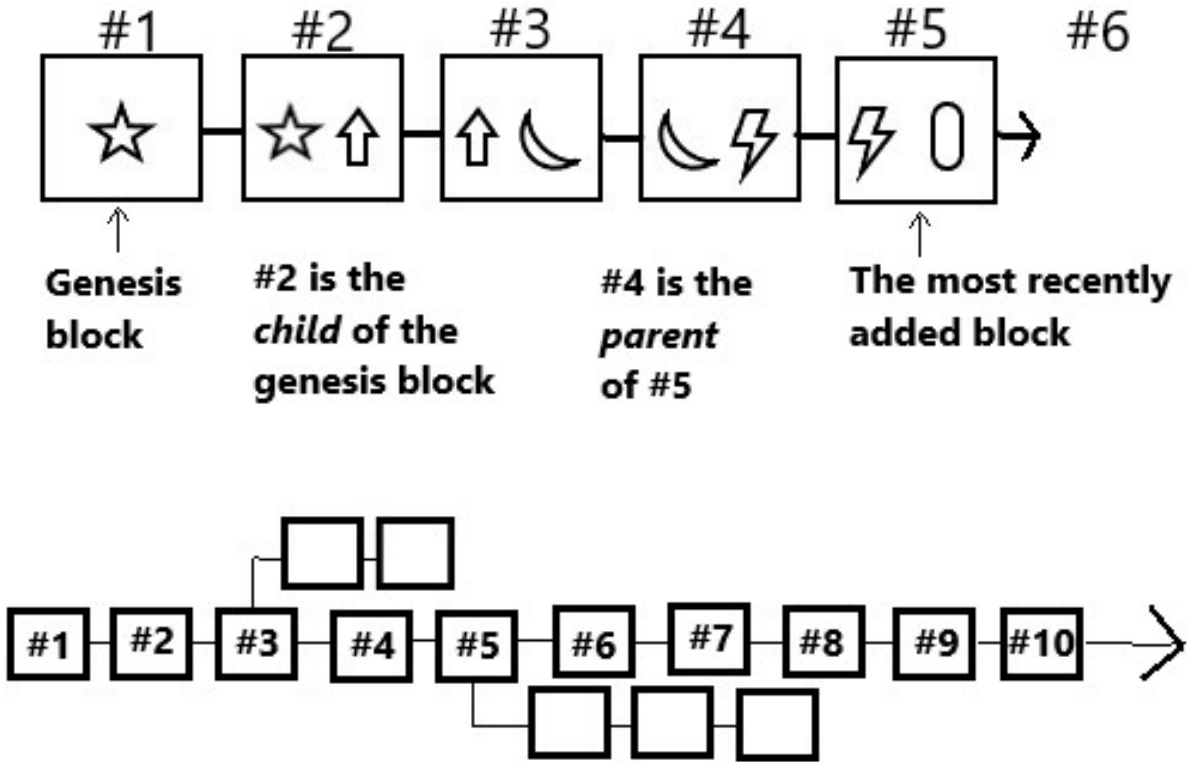


Image 3 and 4: Most often the chain will temporarily look like a “fork”. When verifying the most recently added block all other nodes on the network have to “accept” it, creating a contest on who will verify the block first. Eventually there will always be only one child of each parent block.

⁴³ Antonopoulos, Andreas M., *Mastering Bitcoin – Programming the Open Blockchain*, page 195.

⁴⁴ *Ibid.*

2.5 Hashing the Block

Each block in the blockchain is filled with several transactions made in that particular blockchain network since the last block was validated and added to the chain. The block is identified by its *hash*. One hash for each block. The hash is used as a digital fingerprint, acting as the block's primary identifier and containing a hidden message.⁴⁵ The message can be any information or value. It becomes unreadable by *hashing* it with a computer program, i.e. by using a *hash function* and thereby encrypting the message.⁴⁶ After encrypting the message the output we get is called a *hash value*. The message can later be identified and readable again by decrypting the message by using a cryptographic *hash algorithm*.⁴⁷ This way, data can be transferred without publishing the data itself but only a reference to it. Just as a fingerprint is used as an identifier and has to be verified, for example before entering a secret door to enter a bank vault filled with piles of cash, the hash has the same function in digital environments. It functions as an identifier, which has to be verified, before unlocking the secret message or opening the secret door.



Image 5: By using a hash algorithm, a message or any type of information or value is translated to a fixed length of letters and numbers.



Image 6: The hash functions as a fingerprint, only it is used in a digital environment.

⁴⁵ Antonopoulos, page 197.
⁴⁶ Dreschder, page 71 ff.
⁴⁷ Ibid.

The hash function transforms any kind of data with unlimited length into a fixed length. The cryptographic hash function that the blockchain uses is very advanced, it is considered by many to be secure and impossible to attack. It is a one-way function meaning it is impossible to recover the original input data based on the hash value.⁴⁸ With that being said, even where an advanced algorithm encrypts a message so that it cannot be calculated by its output, the algorithm in itself can always be verified.

SHA256

Message (input)	Hash Value (output)
Hello world	64ec88ca00b268e5ba1a35678a1b5316d212f4f366b2477232534a8aeca37f3c
Hello World	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
Hello World!	7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284add200126d9069
A	559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd
B	df7e70e5021544f4834bbe64a9e3789fbc4be81470df629cad6ddb03320a5c
C	6b23c0d5f35d1b11f9b683f0b0a617355deb11277d91ae091d399c655b87940d
ABC	b5d4045c3f466fa91fe2cc6abe79232a1a57cdf104f7a26e716e0a1e2789df78

Image 7: The cryptographic hash function used in the Bitcoin blockchain is the SHA256. SHA stands for Secure Hash Algorithm which is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). NIST is a physical sciences laboratory and a non-regulatory agency of the US Department of Commerce with a mission to promote innovation and industrial competitiveness.⁴⁹

The block hash is the primary identifier of a block. The first block hash of the first Bitcoin block ever created looked like this:

```
00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
```

By high-performance computers specialized in calculating hard algorithms like this one, the message embedded of the first transaction in the genesis block of the Bitcoin blockchain contained the text “*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.*”. The message was intended to offer proof of the earliest date that block was created, by referencing the headline of the British newspaper The Times.⁵⁰

⁴⁸ Dreschder, page 73 ff.
⁴⁹ Antonopolpous, definitions on page 'xxiii'.
⁵⁰ Antonopoulos, page 197.

2.6 Merkle Tree

Each block hash is a summary of all the transactions in the block. It is calculated using a *merkle tree*.⁵¹ The merkle tree will not be explained further since it is hard to understand and irrelevant for the reader who shall take interest in the legal perspective only. It is important, however, that the reader understands that each block is not one (1) transaction, but several. They are added together, in order to efficiently verify the integrity of a large set of data, and the reason it is called a ‘tree’ is because it is a branching data structure.⁵²

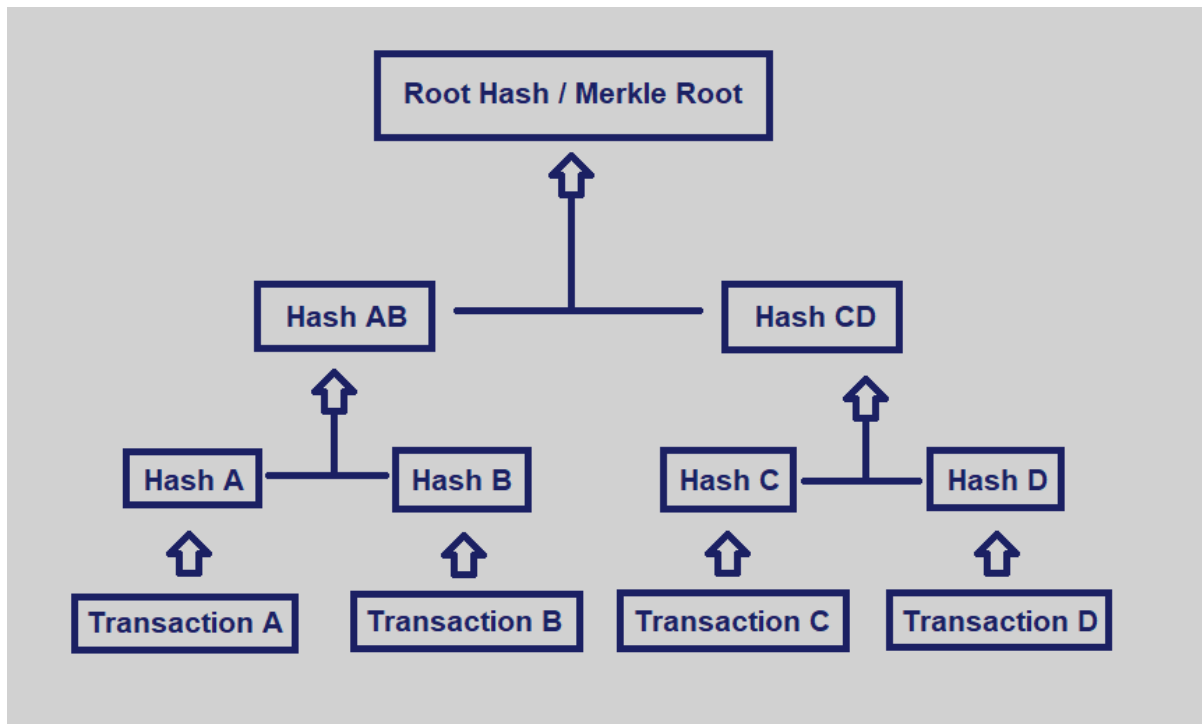


Image 8: A simplified explanation of how all transactions get their own hashes, which is added together until all set of transactions are identifiable with one remaining hash. The remaining hash, i.e. the Merkle Root Hash, is one of the identifiers of each hash.⁵³

2.7 Data Miners

To trade without intermediaries all users have to be equal. Just as in the ideal democratic society, equality in the blockchain is upheld thanks to consensus and by everyone, at least the majority, respecting and acting by the rules that the protocol states. As in any society, there are some people who needs to do the actual work in order to uphold the decided rules. In the

⁵¹ Antonopoulos, page 201 ff.

⁵² Ibid.

⁵³ Image 8 is borrowed from: Shaan, Ray, Merkle Trees, 15 December 2017. Available on <https://hackernoon.com/merkle-trees-181cb4bc30b4>

blockchain the work consists of solving the hash algorithms in the blocks and thereby validating them.⁵⁴ These actors, who can reach an unlimited amount, are called *miners*. By forming a large global network security is provided and the transactions are accepted and locked into its block. Without the miners the blockchain would not function. They are acting as the accountants of the network and working so fast on verifying the blocks that the chain is nearly impossible to hack or tamper with.⁵⁵

As mentioned, it is impossible to decrypt a hash and directly get the hidden message because of the advanced hash algorithm that is used for encryption. However, a central rule in cryptocurrency blockchains is that each hash starts with a certain number of zeros. If it does not start with zeros, the miners repeatedly change a part of the data inside their block leading to different hash.⁵⁶ Thereby, the miners are allowed to “guess” what the input is by entering some input and hashing it until it matches the original input.⁵⁷ This requires a lot of computational power, money and physical storage. When the protocol was first made by Nakamoto the network was so small that regular computer power could do the mining, but with time and the growth of Bitcoin more computers connected, and the reward was harder to get which led to the need of more computer power to guess more answers to the hash value.⁵⁸ Formally anyone can be a miner, but in practice it is only possible by big companies who can afford to invest in this, at least when it comes to the cryptocurrency blockchains.

2.8 Block Reward Schedule

Why would a person or a company mine? The answer is that they get rewarded for it.⁵⁹ In the Bitcoin blockchain the miners achieve newly produced Bitcoin. Satoshi Nakamoto set *the block reward schedule* when he created Bitcoin.⁶⁰ It is one of the Bitcoin blockchain’s central rules and cannot be changed without agreement between the entire Bitcoin network. The block reward started at 50 BTC at the genesis block and halves every 210 000 blocks. This means for every block up until #210,000 50 BTC is transferred to the miner who first succeeded in confirming the block, and from block #210,001 25 BTC is rewarded. The first block after the genesis block on the Bitcoin blockchain came six days after the genesis block, while today,

⁵⁴ Antonopoulos, page 213 ff.

⁵⁵ Ibid.

⁵⁶ Ibid. The data inside the block that changes is called the ‘nonce’, and will not be explained further here, but available to study further in Antonopoulos’s book on page 231, 247 and forward.

⁵⁷ Antonopoulos, page 230.

⁵⁸ Lovén, page 66 ff.

⁵⁹ Ibid.

⁶⁰ Ammous, Saifedean, *The Bitcoin Standard – the Decentralized Alternative to Central Banking*, page 218.

blocks are mined approximately every 10 minutes. That means 144 blocks are verified each day. In that speed, it will take about four years before the block reward halves.⁶¹

2.9 Proof-of-Work

Whenever someone sends a transaction it is broadcast instantly to the network. The transaction then waits to be picked up by a miner on the blockchain. While it is not picked up, it hovers in something called a *mining pool* of unconfirmed transactions.⁶² The miners start working on these unconfirmed transactions by selecting them and forming them into a new block. The process of mining goes on in every data miner's up-to-date version of the blockchain at the same time, creating a competition on who will construct the new block first and have it accepted by the other miners. The solution of the confirmation of the block is called *Proof-of-Work*, since the winning miner has to prove its solution for the other miners to accept it and add it to their copy of the blockchain.⁶³

2.10 Block Header

Basically, a block is a container of data describing the transactions in the blockchain. Each block consists of three types of metadata (data *about* data). First, it consists of a reference to the parent block. Second, there is data that relates to the mining computation, such as the difficulty and timestamp of the block. Third, is the merkle tree root, i.e. data structure used to efficiently summarize all the transactions in the block.⁶⁴ On the website of any block explorer you can get information on a block if you search for its block hash.⁶⁵ For example, on the crypto company called *Blockchain* you can get information on every block in the Bitcoin blockchain, from the genesis block to the most recently added block. For example, by entering <https://blockchain.info/block/> followed by the block hash you will get a description of the contents of the *genesis* block in the Bitcoin blockchain.⁶⁶

⁶¹ Antonopoulos, page 215.

⁶² Antonopoulos, page 250 ff. The mining pools are more complex than described here, which can be studied further in Antonopoulos's book on page 250 and forward.

⁶³ Antonopoulos, page 214.


⁶⁴ Antonopoulos, page 197 ff.

⁶⁵ Ibid., page 199.

⁶⁶ Read more on <https://www.blockchain.com/about>.

These images below show us some information about the genesis block of the Bitcoin blockchain. As a digital public ledger, the information is revealing information about the transactions been made. Here, you can tell that:

- (1) it is the genesis block of the blockchain
- (2) the block contains only one transaction
- (3) the “height” of the block is the number of the block visualized in a stack,
- (4) it was confirmed at 6.15 pm on the 3rd of January 2009,
- (5) it was confirmed by a miner unknown (Satoshi Nakamoto)
- (6) the size of the data stored in the block is 0,285 kB big, and
- (7) the reward obtained by “unknown” was 50 BTC.

Blockera #0  1







Sammanfattning	
Antal transaktioner	1 
Output Total	50 BTC
Beräknad transaktionsvolym	0 BTC
Transaktionsavgifter	0 BTC
Höjd	0 (Huvudkedjan) 
Tidsstämpel	2009-01-03 18:15:05 
Mottagen tid	2009-01-03 18:15:05
Relayed By	Unknown 
Svårighet	1
bits	486604799
Storlek	0.285 kB 
Vikt	0.896 kWU
Version	1
nonce	2083236893
Blockbelöning	50 BTC 

Image 9: Data of the genesis block of the Bitcoin blockchain.



hashes	The block hash
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Föregående block	00  Hash of the parent block (in this case also the genesis block)
Nästa block (er)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048  Hash of the child block
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Image 10: Data of the genesis block of the Bitcoin blockchain.

2.11 Accessing the Blockchain

The blockchain uses asymmetric cryptography, also described as public-key cryptography. This means that the cryptographic system requires two sets of keys. One public key to encrypt data and one private key to decrypt such data.⁶⁷ Anyone who joins the blockchain network generates a public address, which is similar to an email address or bank account number, and a private key, similar to the password needed to that specific email address or bank account.⁶⁸ All other users in the network are given a key-pair to that specific user's private key. A person gets access to their own information and assets by logging on to their account with their private key. With this public-key infrastructure anyone can encrypt and send information by using the receiver's public key, whilst that encrypted message can be decrypted, and accessed, only by the receiver using its private key.

Say a person, Anna, would want to send a message to her friend, Ben, on a blockchain. Anna first logs on to her account⁶⁹, by using her private key. Anna then sends the message to Ben's public address. When doing so, it is the public key (in pair with Ben's private key) which encrypts the message.⁷⁰ By using his private key, Ben can decrypt the message and get the message from Anna.

2.12 Different Types of Blockchains

The use of blockchain technology varies, depending on who can access it and enter data. The classifications used further in the thesis are the ones used by the CNIL in its recommendation. They are as following. *Public blockchains* are accessible to all, anywhere in the world. Anyone can record a transaction, take part in the validation of the blocks or access a copy of them. *Permissioned blockchains* have rules that set out who can take part in the validation process or even register transactions. They can, depending on the case, be accessible to all or be restricted. *Private blockchains* are controlled by a unique actor who alone oversees participation and validation. According to some experts, these parameters do not respect the traditional properties of blockchains, such as decentralisation and shared validation. According to the CNIL, the private blockchains do not raise specific issues regarding their compliance with the GDPR. They are merely "traditional" distributed databases.⁷¹

⁶⁷ Lovén, page 57 ff.

⁶⁸ Ibid.

⁶⁹ In the Bitcoin blockchain called a "wallet".

⁷⁰ Ammous, page 217.

⁷¹ Commission Nationale de l'Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data.

2.13 Summary

- Satoshi Nakamoto founded the cryptocurrency Bitcoin and thereby implemented the technology behind it, called blockchain.
- The public blockchain is a peer-to-peer network. The architecture of the technology is decentralized, meaning there are no intermediaries in power, but it is all users-centric.
- The blockchain functions as a public ledger, why the history in the blockchain is central.
- Each transaction is “hashed” when entered into the blockchain.
- When “mining” the latest transactions, all those hashes form one single hash (the merkle tree root), which serves as the primary identifier of that block.
- The miners work after a protocol. The mining consists of solving mathematical puzzles. The miner who first solves the puzzle and validate the new block gets a reward.
- The blocks of transactions are structured as a chain, where each new block contains the hash of its parent block. This makes the chain immutable, since the whole chain would have to change its data in order to change a single detail in a block.
- The blockchain uses public-key cryptography. To access the blockchain each participant receives a public address, similar to an email address or bank account number, and a private key, similar to a password.
- A blockchain can be public (open for all to see and enter data into), permissioned (where one needs permission to get access to it) and private (a unique actor controls it, which in practice is not a decentralised network).

3 General Data Protection Regulation

The protection of personal data is a fundamental right established in Article 8(1) of the Charter of Fundamental Rights of the European Union (Charter) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).⁷² It was previously implemented through the data protection directive.⁷³ However, in a time where technology develops rapidly and globally new challenges were brought forward regarding the protection of personal data and the need of strengthening the protection of natural persons' integrity grew bigger.⁷⁴ The result of this was a data protection reform, introducing the GDPR, which came into force on 25 May 2018. The aim of the regulation was to strengthen the data subjects' rights in relation to data controllers processing their personal data, but also to take a step forwards in the Digital Single Market strategy - increasing trust in and the security of digital services in the EU in order to allow the development of the digital economy across the internal market.⁷⁵ Going from a directive to a regulation the member states' data protection laws were harmonized to a greater extent and established EU case law was codified.⁷⁶

3.1 Scope of the GDPR

The GDPR applies, with only a few exceptions, to the processing of personal data, wholly or partly by automated means, and to the processing other than by automated means of personal data which form part or intend to form part of a filing system.⁷⁷ Regardless of whether the processing takes place in the EU or not, the GDPR applies in the context of the activities where the controller or processor is established in the EU or in a third country where a member state's law apply by virtue of public international law, or, when the controller or processor is *not* established in the EU but process personal data by offering goods or services in the EU.⁷⁸

Processing personal data is basically any operation performed on personal data whether it is wholly or partly automated. The GDPR lists a few examples such as the collection, recording,

⁷² Recital 1 of the GDPR.

⁷³ 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.

⁷⁴ Recital 6 of the GDPR.

⁷⁵ Recital 7 of the GDPR, and Policy of the DSM Strategy, adopted by the European Commission on 6 May 2015, last updated on 24 August 2018. Available on <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> (accessed on 6 January 2019).

⁷⁶ Recital 3, 53, 150 and 152 of the GDPR for example mentions the aim to harmonise certain rules in the member states.

⁷⁷ Article 2 of the GDPR.

⁷⁸ Article 3 of the GDPR.

organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.⁷⁹ *Personal data* is any information relating to an identified or identifiable natural person.⁸⁰ These definitions combined provide a comprehensive scope where the GDPR becomes applicable on almost all kinds of contact of all types of data relating to a natural person in a digital environment.

3.2 Subject of the GDPR

The GDPR applies to the person or group of persons who process personal data. The correct term used in the GDPR is the *controller* of personal data, who is the one, a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.⁸¹ The *processor* of personal data is also subject of the GDPR, who is the person who processes personal data on behalf of the controller.⁸² If the data controller uses a processor, for example a market research company or a payroll company, the GDPR require a contract or other legal act between the two of them governing the subject-matter.⁸³ It is therefore crucial to analyse the relationship between the controller and a potential processor in each case in order to determine who will be responsible for complying with the GDPR, which national law will apply and which data protection authority will monitor the compliance. However, the roles of the involved entities can be complex since there are often many parties processing the same personal data simultaneously or jointly. In order to clarify the definitions and roles the Art. 29 WP adopted an opinion in 2010 on the concept of controller and processor of personal data.⁸⁴ The opinion states that the concept of controller is autonomous, meaning it should be interpreted mainly according to data protection law and in a sense where it is intended to allocate responsibilities where the factual influence is, based on a factual rather than a formal analysis.⁸⁵ Three main building blocks characterizes the concept of controller, namely, (1) the personal aspect, (2) the possibility of pluralistic control and (3) the essential elements to distinguish the controller from other actors.

⁷⁹ Article 4(2) of the GDPR.

⁸⁰ Article 4(1) of the GDPR.

⁸¹ Article 4(7) of the GDPR.

⁸² Article 4(8) of the GDPR.

⁸³ Article 28 of the GDPR, in particular Article 28(3).

⁸⁴ Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010.

⁸⁵ Opinion 1/2010, page 1.

1. The personal aspect ("*the natural or legal person, public authority, agency or any other body*") focuses on who can be a controller in subjective terms. By the broad definition such as "any other body" one can tell that it aims to cover every influential actor on the market. The opinion states that it is important to stay as close as possible to the practice established both in the public and private sector by other areas of law, such as civil, administrative and criminal law.⁸⁶
2. The possibility of pluralistic control ("*which alone or jointly with others*") aims to protect personal data in cases where there are multiple actors involved in the processing of such data regardless of if these operations take place simultaneously or in different stages.⁸⁷
3. The essential elements to distinguish the controller from other actors ("*determines the purposes and the means of the processing of personal data*"), determines what qualifies for a person to be a controller. The *purposes* of processing relate to the specified, explicit and legitimate decisions made in regard to the processing of the data. Whoever makes these decisions is the de facto controller. The *means* of the processing concerns more technical or organisational questions, such as decisions on which data shall be processed, which third parties shall have access to the data, how long data shall be stored or which hardware or software shall be used. Overall, the controller decides the *why* and *how* of each processing activity. Questions such as 'would an outsourced company process the data if they were not asked by the controller?' or 'would a contractor have an influence on the purpose and carry out the processing also for its own benefit?' can be analysed when determining who qualify as the controller. In this perspective, it is well possible that the technical and organisational means are determined exclusively by the data processor.⁸⁸

An interesting and fairly new case ruled by the CJEU, *Wirtschaftsakademie*, dealt with the possibility to process personal data jointly with others. The case concerned an administrator of a fan page on Facebook, who argued it was not the data controller of the personal data collected on the fan page. The administrator obtained statistical information on visitors of the fan page via a Facebook function.⁸⁹ There was no doubt that Facebook was a data controller of the

⁸⁶ Opinion 1/2010, page 15 ff.

⁸⁷ Opinion 1/2010, page 17 ff.

⁸⁸ Opinion 1/2010, page 12 ff.

⁸⁹ C-210/16, *Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 June 2018.

processing since they placed cookies and structured personal data collected from those cookies.⁹⁰ The CJEU stated the following. The concept of controller should be defined broadly, not necessarily referring to a single entity, to ensure effective and complete protection of the persons concerned.⁹¹ The administrator had entered a specific contract with Facebook, subscribing to the conditions of use of the page, including the cookie policy.⁹² Through this contract Facebook's advertising system was improved and the administrator obtained statistics from the visits of the page for the purpose of the promotion of its own activities.⁹³ When creating a fan page, Facebook is given the opportunity to collect the personal data. The administrator had an actual influence on the processing since it had the possibility to define the criteria in accordance with which the statistics, designate the categories of persons whose personal data is collected and request the processing of data relating to its target audience, such as trends in terms of age, sex, relationship, occupation, information on the lifestyles and centres of interest of the target audience.⁹⁴ Consequently, the administrator was considered jointly responsible, by contributing to the determining of the purposes and means of the processing. It is not required that each processor have access to the personal data concerned where several operators jointly responsible for the same processing. And further it does not matter if the statistics are compiled by Facebook in an anonymised form.⁹⁵ However, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. Operators may be involved at different stages and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.⁹⁶ In this case, the CJEU confirmed the broad definition of controller, how the mere influence contributes to the determining of the purposes and means of the processing and that the level of responsibility of each controller must be assessed on a case-by-case basis.

3.3 Complying with the GDPR

When determining whether or not a processing activity is lawful and GDPR compliant, a few steps has to be taken into consideration. First, the data which is being processed has to be personal.⁹⁷ Second, the processing has to be lawful.⁹⁸ Third, the principles relating to the

⁹⁰ Ibid., para 15 and 18.

⁹¹ Ibid., para 26–29. See also C-131/12, Google Spain, 13 May 2014 and C-212/13, Ryněš, 11 December 2014.

⁹² Ibid., para 30-32.

⁹³ Ibid., para 34.

⁹⁴ Ibid., para 37.

⁹⁵ Ibid., para 35–39.

⁹⁶ Ibid., para 43.

⁹⁷ Article 4(1) of the GDPR.

⁹⁸ Article 6 of the GDPR.

processing has to be fulfilled.⁹⁹ Fourth, the rights of the data subject have to be met (including the obligations implied on the controller and processor).¹⁰⁰ Fifth and finally, the security of the personal data has to be assured.¹⁰¹ In the following, these steps will be described.

3.3.1 Personal Data

Personal data is defined as any information relating to an identified or identifiable natural person, also referred to as a *data subject*. A natural person is identifiable if he or she directly or indirectly can be identified, in particular by reference to an identifier. For example, an identifier can be a name, identification number, location data, online identifier or factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.¹⁰² In the recitals of the GDPR internet protocol addresses (IP-addresses) and cookie identifiers are listed as examples of online identifiers. These may leave traces used to create profiles of the data subjects, especially when combined with unique identifiers and other information received by the servers.¹⁰³

In 2007 the Art. 29 WP adopted an opinion on the concept of personal data.¹⁰⁴ Concerning what a *direct* identifier is, the name of a person is mentioned as the most common identifier. A very common family name may not be sufficient to single someone out from a group of several people, however if that family name appears on a list of pupils in a classroom together with the name of the street that the person lives on, the addressed person surely is identified. Even ancillary information such as “the man wearing a black suit” may identify a certain person when looking at a surveillance camera in a shopping mall. The assessment must, however, be made on a case-by-case basis.¹⁰⁵ When it comes to *indirect* identifiers, the Art. 29 WP mentions all “unique combinations” of information allowing the individual to be distinguished from others. In some cases, the information in itself may not single out an individual, but that information combined with other pieces of information might do so.¹⁰⁶ An example of this is a classroom of pupils, where information on the gender of a person is not enough to single out one pupil, but together with the person’s hair colour the pupil might be identified.

⁹⁹ Article 5 of the GDPR.

¹⁰⁰ Articles 12–23 of the GDPR.

¹⁰¹ Articles 32–36 of the GDPR.

¹⁰² Article 4(1) of the GDPR.

¹⁰³ Recital 30 of the GDPR.

¹⁰⁴ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007.

¹⁰⁵ Opinion 4/2007, page 12 f.

¹⁰⁶ Opinion 4/2007, page 13.

3.3.2 Lawfulness

When processing personal data, the controller is responsible for doing so on at least one lawful ground. The processing is lawful if (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (*'consent'*), (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (*'contract'*), (c) processing is necessary for compliance with a legal obligation to which the controller is subject (*'legal obligation'*), (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person (*'vital interests'*), (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (*'public interest'*) or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (*'legitimate interests'*).¹⁰⁷

3.3.3 Principles

The GDPR further require compliance with the principles relating to the processing of personal data.¹⁰⁸ The personal data must be (a) processed lawfully, fairly and transparent in relation to the data subject (*'lawfulness, fairness and transparency'*), (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (*'purpose limitation'*), (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*'data minimisation'*), (d) accurate and kept up to date, meaning also that in relation to the purposes, inaccurate personal data is erased or rectified without delay (*'accuracy'*), (e) kept for no longer than necessary for the purposes (*'storage limitation'*) and (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*'integrity and confidentiality'*).¹⁰⁹ The controller is responsible for fulfilling these principles and shall be able to demonstrate compliance with the principles (*'accountability'*).¹¹⁰

¹⁰⁷ Article 6(1) of the GDPR.

¹⁰⁸ Article 5 of the GDPR.

¹⁰⁹ Article 5(1) of the GDPR.

¹¹⁰ Article 5(2) of the GDPR.

3.3.4 Rights of the Data Subject

The principles are reflected and expressed more concrete in the following set of rights of the data subject. The data subject has *the right to get information* on the processing of his or her personal data regardless of wherefrom such data was collected.¹¹¹ This right reflects on the principle of transparency and gives the data subject more control over its data. The data subject also has the *right to access* such data by getting a copy of the personal data undergoing processing.¹¹² Where personal data is inaccurate the data subject have *the right to rectification*, meaning such data shall be completed.¹¹³ *The right to restriction of processing* allows the data subject to have his or her personal data restricted in some cases.¹¹⁴ The data subject also have *the right to erasure*, also referred to as *the right to be forgotten*, meaning the controller must delete personal data in some cases, for example where it is no longer necessary in relation to the purposes or if the data subject withdraws his or her consent.¹¹⁵ The right to be forgotten is a clear expression of the importance of the principles of data minimisation and storage limitation. It was included already in the data protection directive, established by the CJEU in *Google Spain* case, but was later codified in the GDPR.¹¹⁶

Where the processing is based on consent and carried out by automated means, the data subject also have *the right to data portability*, meaning the controller is obliged to provide the data in a structured, commonly used and machine-readable format and transmit those data to another controller, directly from one controller to another, without hindrance from the controller to which the personal data have been provided.¹¹⁷ And finally, regarding automated individual decision-making, profiling and direct marketing purposes, the data subject has *the right to object* at any time to such processing on grounds relating to his or her particular situation and not be subject to a decision based solely on automated processing which produces legal effects concerning him or her. The controller shall then stop such processing unless legitimate grounds overriding the interests, rights and freedoms of the data subject for the processing is demonstrated.¹¹⁸

¹¹¹ Article 12–14 of the GDPR.

¹¹² Article 15 of the GDPR.

¹¹³ Article 16 of the GDPR.

¹¹⁴ Article 18 of the GDPR.

¹¹⁵ Article 17 of the GDPR.

¹¹⁶ C-131/12, *Google Spain*, 13 May 2014.

¹¹⁷ Article 20 of the GDPR.

¹¹⁸ Article 21–22 of the GDPR.

3.3.5 Adequate Level of Security

After fulfilling the principles, processing on a lawful ground and meeting the data subject's rights, the controller and processor have to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such safety measures include, among other, to pseudonymize and encrypt personal data, to assure confidentiality, integrity, availability and resilience of processing systems and services, to restore availability and access to personal data in the event of a physical or technical incident, and, to regularly test, assess and evaluate the effectiveness of the safety measures.¹¹⁹

Organisational measures indicate for example that the controller should establish safety policies and educate its employees whereas technical and physical measures could be to redesign IT systems and services and restrict physical access to personal data.¹²⁰ Regarding transfers of personal data to a third country, the GDPR allows processing only where the controller and processor reach the same level of security as the conditions laid down in the GDPR.¹²¹ Other than that, the European Commission has the power to determine which countries provide an adequate level of security of personal data.¹²²

3.4 Summary

- The protection of personal data is a fundamental right. As the previous data protection directive was repealed and replaced with the GDPR the data subjects' rights were strengthened.
- The GDPR applies to the processing of personal data where the controller or processor is established, or where services and goods are offered, in the EU.
- The controller is a natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data. The processor is the natural or legal person who processes personal data on behalf of the controller.
- In order to comply with the GDPR, personal data has to be processed on a lawful ground and according the principles. The rights of the data subject have to be fulfilled, including the obligations implied on the controller and processor, and the processing has to achieve an adequate level of security.

¹¹⁹ Article 32 of the GDPR.

¹²⁰ Datainspektionen, Säkerhet för personuppgifter (Swedish Data Protection Authority, guidelines on security of personal data), November 2008.

¹²¹ Article 44 of the GDPR.

¹²² Article 45 of the GDPR.

4 Identifying Personal Data in the Blockchain

If a blockchain process personal data, the GDPR will apply. In order to find out if it does, the data has to be reviewed under the terms of the GDPR. For the data to be personal, a natural person has to be directly or indirectly identified. If found that the data does not, or does not any longer, identify a natural person, the GDPR does not apply since such data is anonymous.¹²³ This chapter will first examine the actual possibility to anonymise data, since the blockchain encrypts all entered data, and where the line is drawn between anonymous data and indirect personal data. Second, two categories of data in the blockchain will be examined in which personal data may occur. The identifiers of the blockchain, i.e. in the private and public key or in the public address, and the additional data, i.e. the transaction data.

4.1 Anonymised Data

In 2007 the Art. 29 WP concluded in its opinion on the concept of personal data, that data would be anonymous if it previously referred to an identifiable person, but where such identification is no longer possible.¹²⁴ In 2014 the Art. 29 WP adopted another opinion on anonymisation techniques, where the effectiveness and limits of existing anonymisation techniques were analysed against the EU legal background of data protection.¹²⁵ The opinion provided recommendations to handle the techniques by taking account of the residual risk of identification inherent in each technique and clarified a few misconceptions, such as pseudonymisation not being a method of anonymisation but rather a method of reducing the linkability with the original identity of a data subject.¹²⁶ The 2014 opinion state, in contrary to the 2007 opinion, that even though the potential value of anonymisation is acknowledged and it remains a decision on a case-by-case basis, it is difficult to create a truly anonymous dataset.¹²⁷ It is all dependant on several elements taken into consideration by data controllers, having regard to all the means likely reasonably to be used for identification. For example, it is not sufficient to write numbers instead of names in a list to make it anonymous if someone, including a third party, still has access to the key to the original raw data. However, would the

¹²³ Recital 25 of the GDPR.

¹²⁴ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007.

¹²⁵ Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.

¹²⁶ *Ibid.*, page 3.

¹²⁷ *Ibid.*, page 3.

data controller delete the raw data and only provide general data, such as statistics provided to third parties on a high level say ‘on Mondays on trajectory X there are 160% more passengers than on Tuesdays’, that would qualify as anonymous data.¹²⁸

4.2 Direct or Indirect Personal Data

The blockchain does not directly reveal the identity of a natural person since all data is encrypted. When it comes to indirect identifiers the limit extends to whatever allows a person to be recognized. In *Scarlet Extended* the CJEU held that IP addresses is considered personal data since it allows the internet users to be precisely identified.¹²⁹ This was later codified in the recitals of the GDPR.¹³⁰ The CJEU did not mention whether IP addresses are direct or indirect personal data, only that it *precisely identifies* the user. In the later *Breyer* case the CJEU ruled on whether a dynamic IP address constitute personal data.¹³¹ A dynamic IP address is a provisional address which is assigned for each internet connection and replaced when subsequent connections is made, in opposite of a static IP address which is invariable and allow continuous identification of the device connected to the network.¹³² The website provider needed additional data from the internet service provider to identify the user. The CJEU held that it is common ground that a dynamic IP address in itself does not constitute information relating to an identified natural person since such an address does not directly reveal the identity of the natural person owning or using the computer.¹³³ By interpreting the word ‘indirectly’ the CJEU stated that it is not necessary that information alone allows the data subject to be identified.¹³⁴ Account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person, meaning that it is not required that *all* the information enabling the identification of the data subject must be in the hands of one person.¹³⁵ The need of additional data is not sufficient to escape the GDPR and it does not matter if the controller of the data and the additional data is the same or two different persons. However, the CJEU emphasizes that it does need to be determined if the possibility to combine the data constitute a mean likely reasonably to be used to identify the data subject. That would not be the case if the identification was prohibited by law or practically impossible on account of the fact that it

¹²⁸ Ibid., page 9.

¹²⁹ C-70/10, *Scarlet Extended*, 24 November 2011, para 51.

¹³⁰ Recital 30 in the GDPR.

¹³¹ C-582/14, *Breyer v. Bundesrepublik Deutschland*, 19 October 2016.

¹³² Ibid., para 36.

¹³³ Ibid., para 38.

¹³⁴ Ibid., para 40–41.

¹³⁵ Ibid., para 42–43.

requires a disproportionate effort in terms of time, cost and manpower, so that the risk of identification appears in reality to be insignificant.¹³⁶

The criteria, all measures likely reasonably to be used, literally focuses on what is or can be *used*, which correlates to what we *know* about technology, its *capacity* and *how* we use it. Identifiers must therefore be expanding in relation to technology, which corresponds with the fact that the Art. 29 WP somewhat changed its opinion on anonymisation techniques between 2007 and 2014. Only seven years passed between the opinions, which says something about how fast we get new knowledge on existing techniques and how to use and develop it.

4.3 Identifiers

Each user of the blockchain generate a public address and a private key as identifiers and tools for decryption and authorization. The identity of the user is not directly singled out by the key or address, just as the identity of an internet user is not directly revealed by an IP-address. However, for someone to send a message to another person through a blockchain, that other person's public address is used, just as an email address or bank account number. It functions as a post box or wallet, which must therefore precisely identify *a* person. Even if it is not available for everyone to see who that person is, for example the anonymity of Satoshi Nakamoto, at least the person who sends the message will know that it got sent to the *right* person. On a case-by-case basis, it must therefore be determined whether the identity of the sender or receiver is known, or if it is simply a public blockchain network where all users remain anonymous and have no clue to whom they send information or value to when trading. However, that would be unlikely in practice, since it would require that no one ever mentions that they are the owner of that public address and private key. Say all email addresses in the world were random letters and numbers combined, for example akjr489fdn3@gmail.com, and no names or other identifiers would be allowed. Would it be possible to keep such anonymity in real life? Or is it simply a "human factor" that we sometimes accidentally reveal our identities. As mentioned on anonymisation techniques, the Art. 29 WP recognizes that all means likely to be used must be taken into consideration. The CJEU state that information in combination with additional information may be personal data. So regardless of the intention of creating a truly anonymous dataset, if the key, together with additional information, reveals the user, it may be considered personal data. Furthermore, the CNIL recognizes that the identity of participants and miners can be identified through the public keys which are linked

¹³⁶ C-582/14, Breyer, 19 October 2016, para 45–46.

to the private keys, known only by the participant. These identifiers are always visible, as they are essential for the proper functioning of the blockchain. This data is, according to the CNIL, in line with the blockchain's duration of existence.

Say a transaction is made in the network by person A. A sends a book manuscript to person B at a certain date and time due to a contract they had signed in a publishing house earlier that week. Person B sends one million dollars in return, also in accordance with the contract. Both transactions are made public in the blockchain. Person C, who was the witness to the contract signed between A and B, see the transactions in the network. C recognizes that the transactions belong to person A and B, since C saw the size of the transactions as well as the timestamp. The key of A and B is therefore personal data, since the identity of A and B was revealed with the additional data related to the transaction.

4.4 Transaction Data

Besides the identifiers, personal data may consist in additional data stored on the blockchain, i.e. the actual content of the transactions. When encrypting the data, hashing is a one-way measure. It is not possible to derive the hash back to its original data and decrypt the message. However, when validating the block and all its transactions, the miners have to “guess” the input until it matches the output.¹³⁷ Perhaps in 2007 the transaction data of blockchain would not be considered personal data, since anonymised data then would be anonymous if it previously referred to an identifiable person, but where such identification is no longer possible. However, times change, and technology develops rapidly. Interpreting the 2014 opinion it sounds unlikely that it is possible to anonymize personal data at all, if the original raw data is not completely erased. The Art. 29 WP holds that it is a case-by-case assessment, although it cannot be excluded that the transaction data may identify natural persons. Since there are no exact answers on whether a public blockchain identifies a natural person in the transaction data, three arguments may be presented.

First, one could argue that there are no personal data in the hash but rather “underneath” it. The personal data cannot be found even by the miners, since it is too well hidden by the advanced hash algorithm, and therefore the data is not personal at all or at least it has gone anonymous after encrypting it. The data should rather be viewed as “metadata”, meaning the hash is data with mere references to the raw data.

¹³⁷ Mentioned in chapter 2, section 2.7.

Second, one could argue that the hash in itself is personal data since it *directly* identifies a natural person. This would be in line with the fact that the hash is sometimes referred to as a digital fingerprint, which precisely identifies a person even though it does not directly single out the person. Just as a fingerprint one can look at it and compare it with others, by doing the miner's work, and thereby identify the person.

Third and finally, one could argue that the hash is not in itself personal data, i.e. it does not directly single out an individual since it is pseudonymised by the hash function as a measure of encryption. However, with the use of additional information the hash may reveal the identity of the natural person. The hash should therefore be viewed as *indirect* personal data. Such additional information could either be each "guess" that the data miners enter to figure out the original data, or perhaps there are other qualities in the transaction such as the timestamp or the size of it that could reveals the identity of the sender. To determine whether means are reasonably likely to be used all objective factors should be looked at, for example the costs of and the amount of time required for identification, but also the available technology at the time of the processing and technological developments.¹³⁸ The cost of the high-speed computers is for a common person incredibly expensive and would not at all be considered, however there are many companies investing in these computers in order to mine in exchange of Bitcoin or other reward. The amount of time required for the mining is not either that long. As mentioned, the approximate time to mine a block in the Bitcoin blockchain is ten minutes today. As technology is way ahead of the data protection law, it is not unlikely that such technology will be used in order to identify natural persons.

4.5 Summary

- The Art. 29 WP clarified in 2014 that pseudonymisation is not a method on anonymisation, but rather reducing the linkability with the original identity of a data subject. It is therefore difficult to create anonymous data without completely erasing the original data.
- The CJEU said it is not necessary that information alone identifies a person for it to be considered personal data, but all the means likely reasonable to be used should be taken into consideration. The need of additional data is not sufficient to escape the GDPR, not even if such data is held by another person. However, the possibility of

¹³⁸ Recital 26 of the GDPR.

such combination of information must be analysed, based on the effort required in terms of time, cost and manpower.

- The identifiers of the blockchain, the key-pairs and public address, is most probably personal data. Such data is in line with the blockchain's duration of existence.
- The additional data, the content of the transactions, may be considered personal data depending on how one argues. Due to the fast development of technology, it is likely that natural persons may be identified in the blockchain.

5 Data Controller and Processor of the Blockchain

After stating that the blockchain may, at least in certain cases, contain personal data, the data controller must be identified in order to have a person responsible for the processing under the GDPR. In the blockchain all users trade information and value on equal terms. Who can be responsible for the purposes and means in a network where everyone acts and is treated equal? The GDPR claims the protection of natural persons should be technological neutral and not dependant on the techniques used, meaning that where there is processing of personal data of data subjects in the EU there must be a responsible person.¹³⁹ It is not mentioned in the GDPR, neither in the recitals nor in the articles, what applies in cases where there exists no controller or processor or when these cannot be identified and held accountable. The GDPR rather states the importance of imposing obligations on the controller and, if applicable, the processor.

The CNIL observe that the GDPR was designed in a world in which data management is centralised within specific entities. The decentralised data governance model, such as the blockchain technology, holds a multitude of actors involved in the processing of data, which leads to a more complex definition of their role.¹⁴⁰ The CNIL points out that it is the participants, and in some cases the miners, who have the right to enter data on the chain and who decide to send data for validation by the miners, who can be considered as data controllers. Since the CNIL recommendations are aimed at actors who wish to use it when processing personal data within their own business activities, it is more useful in the context of a permissioned or private blockchain. The recommendations are therefore only useful to some extent when analysing the data controller and processor in a public blockchain.

The target groups identified in the public blockchain, and who's role as data controller or processor will be analysed further, are the founder, the miners and the users. In this chapter, their role will be analysed through the three criteria in the Art. 29 WP opinion of 2010:¹⁴¹

¹³⁹ Recital 15 of the GDPR.

¹⁴⁰ Commission Nationale de l'Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data, page 1.

¹⁴¹ Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010.

1. The personal aspect (*"the natural or legal person, public authority, agency or any other body"*).
2. The possibility of pluralistic control (*"which alone or jointly with others"*), and
3. The essential elements to distinguish the controller from other actors (*"determines the purposes and the means of the processing of personal data"*).

5.1 Founder of a Blockchain

Can the founder of a particular blockchain be the data controller? Take for example Satoshi Nakamoto who was the actual founder of the Bitcoin blockchain. Though Nakamoto might not have had the intention of developing the blockchain technology further, the blockchain was founded when applying the Bitcoin protocol for the first time. Naturally, a founder of a technology in general cannot be held responsible. That would mean the founders of the internet would be chased down each time a personal data breach would take place on the internet. The CNIL acknowledges also that blockchain is a technology on which personal data processing can rely, but it is not a data processing operation with its own purpose.¹⁴²

However, Nakamoto did found the Bitcoin blockchain in particular for some purposes and by some means, even if Nakamoto might not have had the intention of letting the network grow as big as it did. The GDPR does not directly proscribe that the controller nor processor has to have an actual intention when determining the purposes and means of the processing. The GDPR must therefore assume, naturally, that the intention lies within the determination criteria, which applies to most common cases.

Looking at the personal aspect of the data controller, Nakamoto fulfil the criteria by acting as a natural or legal person or group of persons. Regarding the possibility of pluralistic control, Nakamoto wrote the white paper alone or as an exclusive group. As of the essential elements to distinguish the controller from other actors, Nakamoto does determine the purposes and means in the white paper by setting up the Bitcoin protocol. By studying the abstract and introduction of the white paper, the purpose is to offer an electronic cash system, where online payments are allowed to be sent without going through a financial institution and the double-spending problem is solved. The means of the Bitcoin blockchain is the use of a peer-to-peer

¹⁴² Commission Nationale de l'Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data, page 1.

network, digital signatures and the hash-based proof-of-work record.¹⁴³ Based on the terms of GDPR, Nakamoto is qualified for a person to be the controller of the Bitcoin blockchain.

Would it be a reasonable solution to hold the founder of a particular blockchain responsible? When thinking about the structure and potential of the technology, it would not be proportionate. Comparing the blockchain technology with something similar, take for example Wikipedia, it would be unfair to hold the person or the group of persons accountable for founding Wikipedia when in fact it is the users who fill the database with content. As long as the founders of Wikipedia are not the ones confirming each text being written. Wikipedia, and the blockchain, are considered databases, which are user-centric and expand and take new shapes along the way. Of course, each case of processing of personal data has to be analysed uniquely, i.e. case-by-case studies are required. Say a public blockchain is founded by a natural person to collect money from its closest relatives. In that case, there would be no problem in pointing out who qualify as controller more than others. However, what happens if that blockchain grew bigger and bigger? Does the concept of controller stay unchanged as more personal data is being collected, or does the fact that some databases grow uncontrolled make the assessment harder? Safe to say is that there are no clear answers on whether the founder of a particular blockchain may constitute the controller. The general answer would be probably not, but a case-by-case assessment is required.

5.2 Users of a Blockchain

It is the majority of the blockchain users who actually uphold the blockchain by agreeing on the rules, as a model of democracy, saying it is the truth. No one is in more control than any other actor. Could it be the users of blockchain who are accountable? It would not be a problem seen to the personal aspect nor the possibility of pluralistic control. There's no limit in the GDPR on how many data controllers or processors there can be in each processing, and the term 'jointly' is interpreted extensively as seen in the *Wirtschaftsakademie* case, making room for as many controllers as needed. *Wirtschaftsakademie*, however, states also that the operators may be involved at different stages and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.¹⁴⁴ By holding the consensus as the very core and purpose of the blockchain every user could fit as a data controller, jointly with other users. Overall, the three

¹⁴³ Nakamoto, page 1.

¹⁴⁴ C-210/16, *Wirtschaftsakademie Schleswig-Holstein GmbH*, para 43.

criteria could be argued they are fulfilled here as well. The “determination” criteria would be criticised though, since a user of a technology should not determine its purposes and means merely by accepting it and using it. The assumption also has its other obvious problems. The difficulty in holding every user accountable lie for example in the issue of identifying the user at first place and in the struggle of restricting the amount of data controllers since the network has the potential to reach as many users as there are living people on this planet with access to a computer device and some sort of computing competence. Also, there would be a distorted relationship between the data subject and data controller if these were the same person. Not to mention the amount of fines the Commission would have to impose on each user of the blockchain. In reality, *every* user cannot be the data controller of every case.

The CNIL also recognizes that not every user is the data controller, but there are two ways a user, or as they choose to call it, a “participant”, can be the data controller. Either where the participant is a natural person and the personal data processing operation is related to a professional or commercial activity, i.e. when the activity is not strictly personal, or where the participant is a legal person who register personal data in a blockchain. As an example, a notary who records his or her client’s property deed on a blockchain is the data controller, or, a bank who enters its clients’ data onto a blockchain as part of its client management processing. A natural person who buys or sells Bitcoin on his or her own behalf is not data controller, according to CNIL, unless that person carries out these transactions as part of a professional or commercial activity, on behalf of other natural persons.¹⁴⁵

To sum it up, it is not fair that every user of the blockchain is counted as data controller or processor. At least some distinction has to be made. At the minimum, a natural person using the blockchain for his or her own private activity is not a data controller, which is in lines up with the fact that purely personal or household activities are not regarded as processing of personal data subject to the GDPR.¹⁴⁶ A legal person who uses the blockchain as part of its business, should be the data controller for the personal data entered into the blockchain in that particular processing, however such argument is more in line with permissioned and private blockchains rather than a public one.

¹⁴⁵ Commission Nationale de l’Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data, page 2.

¹⁴⁶ Article 2(2) c of the GDPR.

5.3 Miners of a Blockchain

After stating that not all users are data controllers, perhaps there are certain users who have somewhat more interest in the upholding the blockchain network than every other “ordinary” person using the blockchain. The miners obtain a certain reward for mining each block, as a compensation for investing time, energy and highly expensive computer power. Without the miners and their proof-of-work system where altering blocks are rejected, there would be no blockchain, mainly since the miners together prevent hackers and interference from others wanting to take control over the blockchain. By obtaining reward, the miners could be designated as being more determined to uphold the blockchain than every other user and therefore are more likely to be the data controllers. However, that assumption will not either remain uncriticised.

The miners have no actual interest in identifying the data subjects. They just want to get the reward. In practise, there are big computers doing the mining for them, and the actual persons behind it do not see the personal data or take any interest in it. According to the Art. 29 WP opinion of 2014 that does not have any meaning. Regardless of whether the data is actually looked at, the mere collection of personal data constitute processing. As long as the controller, even a single person under its organisation, has access to it, it constitutes processing.

The CNIL state that the miners, by merely validating the transactions submitted by the participants, are not involved in the object of the transactions made in the blockchain and do not define the purposes and the means of the processing.¹⁴⁷ The CNIL, however, dismisses the possibility of imposing obligations on the miners rather fast, even though they state that users who carry out transactions as part of a professional or commercial activity, regardless of whether the user is a natural or legal person, are considered data controllers. Presumably, the CNIL, again, focuses on private blockchains rather than public ones. When it comes to data processors, the CNIL recognizes that the miners in some cases can be considered data processors, where they follow the data controller’s instructions when checking whether the transaction meets technical criteria, such as a format and a certain maximum size, and that the participant is allowed, according to the chain rules, to carry out its transaction. As an example, the CNIL mentions a situation where several insurance companies decide to create a permissioned blockchain for their processing operations, the purpose of which is compliance with their KYC (“Know Your Customer”) obligations, they may decide that one of them is the

¹⁴⁷ Commission Nationale de l’Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data, page 2.

data controller and the other insurance companies, which validate transactions as miners, are likely to be considered as data processors.¹⁴⁸ This example also focuses on the use of a private blockchain, where the data controller is the person who design or control the protocol and participate in the transactions. The CNIL further state in its guidance that it is still considering the issues raised regarding the miners as processors in a public blockchains, however it is not mentioned whether it is still unclear if the miner is a controller or not.¹⁴⁹

In the Bitcoin blockchain and other cryptocurrency chains, there are companies focused merely on mining Bitcoin. It is the very core of their business — running the network in exchange for the reward. Suppose these companies are the more likely alternative as data controllers. Would they all be processing the personal data jointly in the blockchain, or would they rather be processing the personal data parallel, when competing in who verifies the block first and get the reward? According to *Wirtschaftsakademie* a person can be considered a joint controller even when not collecting and structuring the personal data itself, but merely influencing and requesting the processing and the parameters of such processing. So, the bar is set out relatively low on who may constitute a controller even in cases when someone else is doing the actual gathering and structuring of personal data. This case implies that the miners, in case they would constitute data controllers, would process the personal data jointly rather than separately or simultaneously. The level of responsibility of each miner must therefore be assessed on a case-by-case basis.

5.4 Summary

- The founder of a public blockchain may fulfil the criteria in the Art. 29 WP opinion on the concept of “controller” and “processor”, however, it would be unfair to hold a single person responsible for all data entered into a blockchain since the public blockchain can be used by anyone in the world without hindrance.
- The users of a public blockchain may also fulfil the criteria of being data controllers jointly, since the blockchain is user-centric and all nodes act on equal terms. However, such solution would be practically impossible as the GDPR singles out intermediaries and not an unlimited number of users of a network. Some distinction has to be made between private and household activities and using blockchain as part of a business.

¹⁴⁸ Ibid., page 3–4.

¹⁴⁹ Ibid., page 4.

- The data miners of a public blockchain may also fulfil the criteria of being data controllers jointly, since they get reward for the mining process and therefore have somewhat more purpose in upholding the network and can make a business solely around mining, for example the Bitcoin mining. However, such solution is not either unproblematic.

6 Applying the GDPR Principles in Blockchain Technology

To comply with the GDPR all personal data has to be processed in accordance with the principles of Article 5. Under each principle lies a set of rights of the data subjects and obligations on the data controller and processor, which embodies the principles throughout the regulation. To analyse whether the purposes and functions of the GDPR can be upheld in a blockchain, the technical aspect will be reviewed based on (i) its purpose, (ii) the lawfulness, fairness and transparency of its use together with the ability to demonstrate that the obligations under the GDPR is upheld, (iii) the data subjects' right to rectify or erase data in the blockchain and (iv) the integrity and confidentiality of personal data in the blockchain. In this chapter, these areas will be discussed further.

6.1 Purpose Limitation

Depending on the use of the specific blockchain, the personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This principle depends on who is the data controller, since it is the controller who decides the purposes of the processing. Each blockchain must therefore be reviewed uniquely including the purposes for which it is built. Originally, the blockchain was set up for the purpose of enabling transactions without relying on intermediaries. In order to send transactions peer to peer some data is required, which may constitute personal data. Naturally, it is impossible to control what data is processed in the blockchain since it lacks a sole responsible controller. If the purpose is defined broadly, for example 'upholding a network where any person can send any information to another person without trusting intermediaries', the principle of purpose limitation could possibly be fulfilled. Such purpose would not likely be approved by the CJEU however, since it does not meet up to the requirement of the purpose being specified, explicit and legitimate. It is not therefore guaranteed that the principle of purpose limitation is fulfilled. A case-by-case assessment is required to analyse the compliance.

6.2 Lawfulness, Fairness, Transparency and Accountability

The blockchain is available for everyone to see and access. The data of each transaction is public, and the history of such data is central in order to fulfil the very purpose of blockchain.

The structure of the technology provide transparency towards the users. The GDPR aim also to achieve transparency, by giving more control to the data subject in relation to the data controller with a set of rights. In the Art. 29 WP guidelines on transparency under the GDPR the working party state that transparency is a long established feature of the law of the EU and that it is about engendering trust in the processes which affect the citizen by enabling them to understand, if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter.¹⁵⁰ Transparency is also connected to the principle of accountability, by obliging the controller to always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject. It empowers data subjects to exercise control over their personal data, for example by providing or withdrawing informed consent and actioning their data subject rights. The concept of transparency in the GDPR is, according to the Art. 29 WP, “user-centric” rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles (which outlines in Articles 12 – 14 of the GDPR). However, the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects.¹⁵¹

The CNIL does not analyse the question further than with a few sentences, but it does say that the information right of data subjects is not problematic, neither is the right of access and the right to portability. The exercise of those rights is compatible with the blockchains’ technical properties.¹⁵² The blockchain should therefore not be accused of not complying with the principle of lawfulness, fairness and transparency since all information is made public and easily accessed. The principle of accountability require that the controller shall be responsible for, and be able to demonstrate compliance with, all the principles in Article 5.1. As a recommendation, the CNIL mentions that the governance of changes to the software used to create transactions and to mine should be documented, and technical and organisational procedures should be set out to ensure an alignment between planed permissioned and practical application.¹⁵³

¹⁵⁰ Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, page 5.

¹⁵¹ Ibid., page 6.

¹⁵² Commission Nationale de l’Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data, page 8.

¹⁵³ Ibid., page 10.

Overall, there should be no particular problem in complying with the principal of lawfulness, fairness and transparency nor the principle of accountability, as long as the data controller documents and keeps track of its use of a blockchain solution in its business.

6.3 Data Minimisation, Accuracy and Storage Limitation

Regarding the tampering of personal data, the GDPR and blockchain do not meet as well. GDPR on the one hand require that the data subject can influence the processing of its personal data, by recalling the consent on which the processing relies, having the data rectified or completely erased, etcetera. The blockchain on the other hand require that no data is changed once it is confirmed. It is the very idea of the blockchain that every block refers back to its parent block, making the chain immutable. In theory data could be erased, but it would require consensus throughout the network and the miners would have to reconstruct the block possibly years back in time. The longer the chain is and as time passes by, it gets harder to rectify the chain. In practise it is impossible to fully comply with the principles of data minimisation, accuracy and storage limitation.

The CNIL also notes that there is tension between the principle of data retention periods and the permanence of blockchain transaction information.¹⁵⁴ Without reaching a conclusion as to whether or not it is impossible for a blockchain to comply with the GDPR, it offers some guidance on data minimization techniques. The CNIL states that there is no data minimization option available when it comes to the identifiers, i.e. the key pair and public address of each participant, due to the technical specifications of blockchains which require that these are always visible as they are essential for its proper functioning.¹⁵⁵ Regarding the transaction data the CNIL consider that personal data should preferably be registered on the blockchain in the form of a commitment. A “commitment” is, according to the CNIL, a cryptographic mechanism that allows one to “freeze” data in such a way that it is both possible – with additional information – to prove what has been frozen and impossible to find or recognise such data by using this sole “commit”.¹⁵⁶ If this is not possible, the CNIL recommends that the personal data is cryptographically secured via encryption or by including only references to the underlying data, for example keeping the cleartext containing personal data on the data controller’s information system and storing only a proof of existence of such data on the

¹⁵⁴ Commission Nationale de l’Informatique et des Libertés, Solutions for a responsible use of the blockchain in the context of personal data, page 8.

¹⁵⁵ Ibid., page 6.

¹⁵⁶ Ibid.

blockchain.¹⁵⁷ The CNIL implies also that no personal data should be stored directly in the blockchain, meaning indirectly that the principle of data minimization, accuracy and storage limitation is practically impossible to comply with in the public blockchain. And not even after leaving recommendations of data minimisation measures can the CNIL leave any guarantees that the principles are fulfilled.

Regarding data minimisation and accuracy, an important article in the GDPR may not be forgotten. Article 11 of the GDPR state that where the purposes for processing do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR. Meaning, in cases where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall, only if possible, inform the data subject accordingly. Articles 15 to 20 shall not then apply unless the data subjects provides additional information enabling his or her identification. This article aims to prevent certain situations. For example, if a data controller receives an e-mail from 123abc@hotmail.com, a person who they cannot identify, they should not be obliged to answer the email and ask for its personal information such as a name or a phone number in order to contact them to inform them on the processing of their data and their associated rights as data subjects. That would mean that the controller would have to collect additional personal data merely in order to comply with the GDPR. In the context of blockchain, this rule also applies. When the data controller cannot identify the data subject, they should not have to gather additional information just to inform the data subjects of the processing and its rights. The right of access, right to rectification, erasure and restriction of processing and the right to data portability would then not apply, which seems fair in the blockchain context. That does not mean, however, that no obligation applies. For example, the controller still needs to notify the supervisory authority on any personal data breach where there is a risk to the rights and freedoms of natural persons which is not unlikely.

6.4 Integrity and Confidentiality

As to the principle of integrity and confidentiality, the blockchain has to process the personal data in a manner that ensures appropriate security of such data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. What was mentioned above on data

¹⁵⁷ Ibid, page 7.

minimisation techniques applies also to the principle of integrity and confidentiality. Further, the CNIL provides some guidance on how individuals and companies might minimize their GDPR risk around blockchain technology. It recommends that companies seeking to process large amounts of personal data using blockchain technology rely on private blockchains over public blockchains.¹⁵⁸ The reason that the CNIL favours private blockchains largely is because of the geographic issues associated with the public blockchain. Most public blockchain nodes can be located anywhere in the world and can be operated by any natural person or entity that has a computer that maintains a copy of the blockchain ledger. This presents problems under the principle of integrity and confidentiality since it restricts the transfer of personal data to countries that do not ensure an “adequate” level of protection without the appropriate legal safeguards in place. The CNIL argues that permissioned blockchains, i.e. private blockchains with restricted access, can allow for tighter control over the jurisdictions in which nodes are operated, which better complies with the geographic limitations imposed by the GDPR.¹⁵⁹

As part of its obligations in Article 25 of the GDPR, data protection by design and by default, the data controller must give prior thought to the appropriateness of choosing this technology when processing personal data. The CNIL reminds that all transactions on the blockchain involve a request to validate the transaction being sent to all miners of the chain, that each update is sent to all participants by adding a new block and that these participants can be located in countries outside of the EU meaning the data controller has no real control over the location of miners in a public blockchain. Further, the CNIL recommends establishing technical and organizational procedures to limit the impact of a potential algorithm failure on the security of transactions, including an emergency plan that allows the underlying algorithms to be modified when a vulnerability is identified.¹⁶⁰

6.5 Summary

- A case-by-case assessment is required to analyse the compliance with the principle of purpose limitation, since each blockchain is set up for a different purpose. This principle is connected to determining who qualifies as the controller, since that person decides the purposes.

¹⁵⁸ Ibid., page 5.

¹⁵⁹ Ibid.

¹⁶⁰ Ibid., page 10.

- The blockchain is public and all information is accessible. It should not be a problem to comply with the principle of lawfulness, fairness and transparency, although the GDPR and the blockchain are transparent in different ways.
- As long as the data controller document its use of the blockchain, the principle of accountability should be able to fulfil.
- It is practically impossible to comply with the principles of data minimisation, accuracy and storage limitation since the blockchain does not allow any data to be tampered with once it is entered into the database. There are, however, some measures that can be taken into consideration to reduce the harm beforehand, such as only storing references to the underlying data on the blockchain. The same applies to the principle of confidentiality and integrity, however some technical and organisational measures can be outlined.

7 Discussion and Conclusions

The public blockchain and the GDPR do not meet well. Since encryption is not a method on anonymisation unless the original data is erased, and the bar is set out low on what constitute indirect personal data, the conclusion must be that natural persons may be identified in the blockchain. Most definitely in the identifiers, and due to the rapid development in technology, probably in the transaction data as well. Therefore, the GDPR is applicable and a natural or legal person must be held responsible in that particular public blockchain. It is demonstrated, however, that it is difficult to determine who qualifies as the controller in the blockchain. All participants, i.e. each user, the founder and miners, act on equal terms as the blockchain is user-centric. Anyone can, at least in theory, become a data miner, and therefore, all participants have more or less the same purposes and means in upholding the blockchain. Some distinction can be made by looking at the miners who create a business around it, or other legal persons who use it as part of their business, which lines up with the fact that the GDPR does not apply on private or household activities. Therefore, the conclusion is that there are yet no clear answers on who is the data controller or the data processor in a public blockchain. Another conclusion is that the GDPR is adapted only for cases where there is at least one actor who holds some sort of power over data subjects and their personal data. Further, the principles of the GDPR cannot either be fulfilled in a public blockchain. The purposes cannot be identified unless there is a controller responsible to begin with, and the principles of data minimisation, accuracy and storage limitation cannot be met since the data entered on the blockchain is practically impossible to tamper with. Nevertheless, the possibility of erasure would undermine the very purpose of the blockchain.

The GDPR might succeed in being implemented where there is someone in power of the personal data or acts and benefits as a middleman. However, it does not succeed in a public blockchain, which concludes that the GDPR fails in its attempt on being technologically neutral. To be fair, the principle of transparency can be fulfilled, and the assessment has to be made on a case-by-case basis. However, even the French data protection authority, the CNIL, seem to avoid giving advice on the public blockchains. The recommendations of the CNIL overall runs counter to the purposes of public blockchains since such networks intend to be borderless. However, it is a strong first step in addressing the blockchain and GDPR issue and the CNIL explicitly admit that it questions its ability to ensure a full compliance with the GDPR which is why a reflection at the European level is essential.

The EU's opinion on blockchain seems to be unclear. On the one hand it favours the rights of the data subjects and on the other hand it invests millions of euros in blockchain projects. EU's intention must logically be that both GDPR and the blockchain investment forms part of the digital market strategy. However, behind the GDPR and blockchain issue lies a tension between something bigger, namely, the balancing of the concept of privacy and the concept of transparency. Privacy within the EU require inter alia that personal data is kept away to some extent whereas thereby the principle of data minimisation, accuracy and storage limitation is fundamental in the GDPR. Transparency on the other hand, is needed to ensure that the authorities who process personal data actually comply with these obligations. The blockchain actually favours transparency wherefore it should not necessarily be a threat on the GDPR, but rather a tool for achieving it. At least parts of it. Perhaps regulators must rethink how to balance data transparency with the right to erasure, especially in cases where a decentralized technology is used. The tension really comes down to an ethical debate on how to balance interests and where to draw the line. Therefore, it is up to the EU to further evaluate its view on transparency versus privacy in the context of decentralized technologies.

Data protection law and blockchain technology will eventually be harmonized. A technology cannot disappear, and the solution is not to prohibit the use of it. One can rethink whether it is necessary to enter personal data in directly the blockchain or if mere references to it is sufficient. Decryption keys can be kept outside the blockchain, to ensure no personal data are processed directly in the blockchain. Thereby, it would still constitute personal data, but by deleting the decryption key and ensuring no one will ever get access to that data again, the right to erasure could be fulfilled. However, the reason this is not done already is because it requires a lot more capacity, and such solution could just as well mean the blockchain is not useful anymore. It would undermine the purpose of blockchain, since it would not be as transparent as it is today. It would also mean a greater risk of personal data breaches, since the keys are in the physical position of someone. If the key is lost and not deleted, that data will be inaccessible and in the wrong hands. Therefore, the solution cannot be on the technology side.

Legal changes have to be made in the EU to solve this conflict. The debate has to continue until balance is found between privacy and blockchain technology. Where we are at now, more recommendations and guidelines from European level is required, and case law from the CJEU, in order to move forwards. That would help organisations at least in fulfilling their accountability obligations, showing that they try to comply with the GDPR. In the long run,

changes must be made in the GDPR or besides it. It is not a question on mere interpretation of the GDPR, but a failure in its objectives. It should not state that it attempts on being technologically neutral if it is not. Studies have to be made on decentralized software architectures and in which areas and for which purposes it is and can be used. Finally, the EU has to make up its mind on whether to change the GDPR or protect personal data in decentralized technologies in other ways.

Bibliography

Statutes, Conventions, Regulations and Directives

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 20 March 2010, OJ C 83/389.

Consolidated version of the Treaty on the Functioning of the European Union, Official Journal of the European Union, 26 October 2012, EUT C 326/47.

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.

Preparatory Works

Sweden

SOU 2018:25, Juridik som stöd för förvaltningens digitalisering, Betänkande av Digitaliseringsrättsutredningen, 27 March 2018.

Recommendations, Opinions and Guidelines

EU

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN, WP 136.

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, 00264/10/EN, WP 169.

Article 29 Data Protection Working Party, Opinion 5/2014 on Anonymisation Techniques, 10 April 2014. 0829/14/EN, WP 216.

Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, as last revised and adopted on 11 April 2018, 17/EN, WP260 rev. 01.

France

Commission Nationale de l'Informatique et des Libertés, Blockchain – Solutions for a responsible use of the blockchain in the context of personal data, 6 November 2018 (English version).

Sweden

Datainspektionen, Säkerhet för personuppgifter, November 2008.

Cases

Court of Justice of the European Union

Case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 24 November 2011, ECLI:EU:C:2011:771.

Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 13 May 2014, ECLI:EU:C:2014:317.

Case C 212/13, František Ryněš v Úřad pro ochranu osobních údajů, 11 December 2014, ECLI:EU:C:2014:2428.

Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, 19 October 2016, ECLI:EU:C:2016:779.

Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, 5 June 2018, ECLI:EU:C:2018:388.

Literature

Ammous, Saifedean, The Bitcoin Standard - The Decentralized Alternative to Central Banking, Wiley, 2018.

Antonopoulos, Andreas M, Mastering Bitcoin - Programming the Open Blockchain. 2nd edition, O'Reilly, 2017.

Burniske, Chris and Tatar, Jack, Cryptoassets - The Innovative Investor's Guide to Bitcoin and Beyond, Mc Graw Hill Education, 2018.

De Geer, Christoffer, Bitcoin och Blockkedjan - En begriplig överblick, Ekerlids Förlag, 2018.

Dreschder, Daniel, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Apress, 2017.

Elgebrant, Emil, Kryptovalutor - Särskild rättsverkan vid innehav av bitcoins och andra liknande betalningsmedel, Wolters Kluwer, 2016.

Frydinger, David and others, GDPR - Juridik, organisation och säkerhet enligt dataskyddsförordningen, Norstedts Juridik AB, 2018.

Korling, Fredric and Zamboni, Mauro (red.), Juridisk Metodlära, Studentlitteratur, 2013.

Lovén, Linus, Bitcoin - En Finansiell Revolution, Tryckfolket Malmö, 2016.

Magnusson Sjöberg, Cecilia and Wolk, Sanna, Juridiken kring E-lärande, Studentlitteratur, 2012.

Magnusson Sjöberg, Cecilia. Rättsinformatik - Juridiken i det digitala informationssamhället, 2nd edition, Studentlitteratur, 2016.

Magnusson Sjöberg, Cecilia; Nordbeck, Peter; Nordén, Anna and Westman, Daniel, Rättsinformatik - Inblickar i e-samhället, e-handel och e-förvaltning, Studentlitteratur, 2011.

Sandgren, Claes, Rättsvetenskap för uppsatsförfattare: ämne, metod, material och argumentation, 4th edition, Norstedts Juridik AB, 2018.

White Papers

Nakamoto, Satoshi, Bitcoin: A peer-to-peer electronic cash system, 2008. Available (PDF) at: <https://bitcoin.org/bitcoin.pdf> (accessed on 3 January 2019).

Journals and Articles

New York Sun, Chances for the Inventor, The Friend: a religious and literary journal, episode 76, 9 August 1902. Available on:

<https://babel.hathitrust.org/cgi/pt?id=hvd.ah6e5w;view=1up;seq=44> (accessed on 3 January 2019).

Singh, Prakhar, Blockchain: Next Generation of the Internet, Data Driven Investor, 2 October 2018, available on: <https://medium.com/datadriveninvestor/blockchain-next-generation-of-the-internet-ec0089ce2b69> (accessed on 3 January 2019).

Hallows, Becca, Who is the REAL Satoshi Nakamoto?, CryptalDash, 28 February 2018. Available on: <https://medium.com/@cryptaldashcoin/who-is-the-real-satoshi-nakamoto-55bacbbe566> (accessed 13 December 2018).

MutualArt, What Does Blockchain Mean for the Art Market?, MutualArt, 8 November 2018, available on: <https://www.mutualart.com/Article/What-Does-Blockchain-Mean-for-the-Art-Ma/408995F2B7144AC9?fbclid=IwAR28NmZE7EB-nssFsqebZGVGa-7h-RT3WXh5btO2mOOyleV4a3OtPj8Ba0E#.W-4FJc6QfeA.facebook> (accessed on 3 January 2019).