Reconciling the conflict between the ‘immutability’ of public and permissionless blockchain technology and the right to erasure under Article 17 of the General Data Protection Regulation

Jani-Pekka Jussila 507230

Re-examining the Foundations of EU Law

Turun yliopiston oikeustieteellinen tiedekunta

8.10.2018

TURUN YLIOPISTO

Oikeustieteellinen tiedekunta

JUSSILA, JANI-PEKKA: Reconciling the conflict between the 'immutability' of public and permissionless blockchain technology and the right to erasure under Article 17 of the General Data Protection Regulation

Pro gradu -tutkielma, XII + 86 s.

Oikeustiede, Eurooppaoikeus

Lokakuu 2018

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check -järjestelmällä.

This thesis focuses on the issues between a blockchain technology and the new European Union General Data Protection Regulation (GDPR). The Blockchain technology is a rather new technology which potential has been recognised only in the recent years. Essentially, a blockchain is a distributed database in which data is stored in blocks, which form a chronological chain of blocks. Blockchains have many types and possible use cases, but this research focuses on public and permissionless blockchains, which primary objective is to enable individuals to transact with each other without centralised intermediaries.

The GDPR entered into force on 25 May 2018. The GDPR was not drafted taking account of distributed ledger technologies, such as the blockchain technology, which has raised several points of tension between the regulation and the technology. The primary focus of this thesis is on the conflict between the 'immutability' of blockchain technology and the right to erasure under Article 17 of the GDPR. One of the main features of blockchains is the immutability, that is to say, data on old blocks is extremely difficult to modify or delete. This feature seems prima facie to conflict with Article 17 of the GDPR that provides data subjects with the right to request erasure of their personal data under certain conditions.

Firstly, this thesis analyses the current state of the conflict. Before analysing the conflict, the research addresses two essential preliminary questions: the question about anonymisation and personal data and the question about allocation of responsibilities on blockchains. After that, different solutions proposed to reconcile the conflict are analysed to understand the current situation. While public and permissionless blockchains currently may infringe Article 17 of the GDPR, there are potential solutions for the conflict in the future.

The second purpose of this thesis is to identify relevant legal problems and propose how to address the problems in the future. Blockchain developers should consider data protection obligations already in the design phase. From the legal side, this research has provided flexible interpretations for the legal problems that could help to comply with the right to erasure. There is a need for a flexible approach to the problems between the regulation and the technology.

Asiasanat: General Data Protection Regulation, data protection, the right to erasure, blockchain technology, blockchain.

Contents

References V
Literature V
Official Material X
Cases XI
Abbreviations XII
1 Introduction 1
1.1 Background 1
1.2 Research problem, scope of the study, and structure 3
1.3 Research method and material 5
2 A brief introduction to blockchain technology 6
2.1 What all the fuss is about? 6
2.2 Different types and use cases of blockchains 8
2.3 Technical properties of blockchain technology 11
3 Regulation of data protection in Europe 14
3.1 History of data protection in Europe 14
3.2 What new the GDPR brought to the field of data protection? 17
3.2.1 The GDPR as a response to the challenges of data protection in the digital age 17
3.2.2 Strengthening the data protection of individuals and enhancing the responsibilities of data controllers and processors 19
4 Relationship between blockchain technology and the GDPR 22
4.1 Decentralisation as the fundamental issue 22
4.2 Blockchain as a tool for enhancing individuals' privacy and data protection 24

4.3 Personal data and traditional blockchains 28
4.3.1 The notion of personal data under the GDPR 28
4.3.2 Personal data on blockchains 35
4.3.3 Technological solutions for better protection of individuals privacy and data protection 41
4.4 Allocation of responsibilities on blockchain networks 44
4.4.1 Main users of personal data under the GDPR 44
4.4.2 Accountability gap and enforcement issues on traditional blockchains 45
4.4.3 Allocation of responsibilities on traditional blockchains 47
5 The conflict between the right to erasure under the GDPR and the immutability of traditional blockchains 50
5.1 History and scope of the right to erasure 50
5.1.1 History of the right to erasure 50
5.1.2 The right to erasure under Article 17 of the GDPR 54
5.1.3 The right to erasure and other provisions of the GDPR 57
5.2 Reconciling the conflict between the immutability and the right to erasure 58
5.2.1 What is the conflict about? 58
5.2.2 Obligation to inform other controllers of the request to erase in traditional blockchains 61
5.2.3 Solutions proposed for reconciling the conflict between the right to erasure and the immutability of traditional blockchains 62
5.3 Taking a review of the current state of play and a look into the future 76
5.3.1 Assessing the current situation of the conflict 76
5.3.2 Building a bridge between the GDPR and blockchain technology 79
6. Conclusions 83

References

Literature

— —, Blockchain and GDPR: How to square privacy and distributed ledgers' (*Chainfrog*, 2017) <http://www.chainfrog.com/wp-content/uploads/2017/08/gdpr.pdf> accessed 27 June 2018

Ateniese G and others, 'Redactable Blockchain - Or - Rewriting History in Bitcoin and Friends' [2017] IEEE European Symposium on Security and Privacy 111 < https://ieeexplore.ieee.org/document/7961975/> accessed 2 September 2018

Bartolini C and Siry L, 'The Right to Be Forgotten in the Light of the Consent of the Data Subject' (2016) 32 Computer Law and Security Review 218

Berberich M and Steiner M, 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers' (2016) 2 European Data Protection Law Review 422

Biryukov A, Khovratovich D and Pustogarov I, 'Deanonymisation of Clients in Bitcoin P2P Network' (Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery 2014) <http://arxiv.org/abs/1405.7418> accessed 19 August 2018

Boucher P, 'How Blockchain Technology Could Change Our Lives' (European Parliamentary Research Service, 2017)

Bygrave LA, *Data privacy law: an international perspective* (Oxford University Press 2014)

Conte de Leon D and others, 'Blockchain: Properties and Misconceptions' (2017) 11 Asia Pacific Journal of Innovation and Entrepreneurship 286

Cryer R and others, *Research Methodologies in EU and International Law*, (Hart Publishing 2011)

De Filippi P, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) 9 Journal of Peer Production <http://peerproduction.net/wp-content/uploads/2016/08/blockchain-technologies-draft.pdf> accessed 30 June 2018

De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law and Security Review 179

Eberhardt J and Tai S, 'On or off the Blockchain? Insights on off-Chaining Computation and Data' in Flavio De Paoli, Stefan Schulte and Einar Broch Johnsen (eds), *Service-Oriented and Cloud Computing - 2017* (Springer, 2017)

Eichler N and others, 'Blockchain, Data Protection, and the GDPR'(Blockchain Bundesverband, 25 May 2018) <www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf> accessed 17 August 2018

El Emam K and Cecilia A, 'A Critical Appraisal of the Article 29 Working Party Opinion 05 / 2014 on Data Anonymization Techniques' (2014) 5 International Data Privacy Law 73

European Data Protection Supervisor, 'Annual Report 2016' (Publications Office of the European Union, 2017)

European Commission, ‘Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union’ COM (2010) 609 final 1

— —, ‘Factsheet on the “ Right to Be Forgotten" ruling (C-131-12)’ (Commission factsheet, 2014)

— —, ’European Commission launches the EU Blockchain Observatory and Forum’ (Press release 2018) <http://europa.eu/rapid/press-release_IP-18-521_en.htm> accessed 26 June 2018

Fabiano N, ‘Blockchain and Data Protection: The Value of Personal Data’ (The 9th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC, Orlando, March 2018) <www.nicfab.it/blockchain-data-protection/> accessed 24 July 2018

Fazlioglu M, ‘Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet’ (2013) 3 International Data Privacy Law

Ferrari V, ‘EU Blockchain Observatory and Forum Workshop on GDPR, Data Policy and Compliance’ (Report on EU Blockchain Observatory and Forum Workshop, Brussels, 8 June 2018) <https://blockchain-society.science/wp-content/uploads/2018/07/blockchain_society_research_nodes_1_GDPR_workshop_03072018.pdf> accessed 17 August 2018

Filippone R, ‘Blockchain and Individuals’ Control over Personal Data in European Data Protection Law’ (Master's Thesis, Tillburg University 2017) <http://arno.uvt.nl/show.cgi?fid=143638> accessed 20 June 2018

Finck M, ‘Blockchains and Data Protection in the European Union’ (2017) 10(1) Max Planck Institute for Innovation and Competition Research Paper Series

Gorzeman L and Korenhof P, ‘Escaping the Panopticon Over Time: Balancing the Right To Be Forgotten and Freedom of Expression in a Technological Architecture’ (2017) 30 Philosophy and Technology 73

Iansiti M and Lakhani KR, ’The Truth About Blockchain’ (2017) 95(1) Harvard Business Review 118

Ibáñez L, O’Hara K and Simperl E, ‘On Blockchains and the General Data Protection Regulation Brief Introduction to Blockchain Technologies’ (University of Southampton 2018) <https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf> accessed 20 September 2018

Information Commissioner Office, ‘ICO Analysis of the Council of the European Union Text of the General Data Protection Regulation' (*ICO Blog*, 26 August 2015) <https://ico.org.uk/media/1432420/ico-analysis-of-the-council-of-the-european-union-text.pdf> accessed 20 September 2018

Kinnunen T and others, *Applying blockchain technology and its impacts on transport and communications*, (Publication of the Ministry of Transport and Communications 12/2017)

Kuner C and others, ‘Blockchain versus Data Protection’ (2018) 8 International Data Privacy Law 103

Kempe M, ‘The Land Registry in the blockchain’(Report of a development project with Lantmäteriet, Telia Company, ChromaWay and Kairos Future, July 2016) <http://ica-it.org/pdf/Blockchain_Landregistry_Report.pd> accessed 30 June 2018

Markou C, 'The 'Right to Be Forgotten': Ten Reasons Why It Should Be Forgotten' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reforming European Data Protection Law* (Springer 2015)

Michels D, 'Can Blockchain Operators Comply with EU Data Protection Law?' [2018] Binary District Journal <https://journal.binarydistrict.com/can-blockchain-operators-comply-with-eu-data-protection-law/> accessed 19 September 2018

Mourby M and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review 222

Nakamoto S, Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) 1 <https://bitcoin.org/bitcoin.pdf> accessed 29 June 2018

Narayanan A and others, *Bitcoin and Cryptocurrency Technologies*, (Draft version, Princeton University Press 2016) <https://lopp.net/pdf/princeton_bitcoin_book.pdf> accessed 20 September 2018

Neisse R, Steri G and Nai-Fovino I, 'A Blockchain-Based Approach for Data Accountability and Provenance Tracking' in *Proceedings of the 12th International Conference on Availability, Reliability and Securit*y (Association for Computing Machinery, 2017) <http://arxiv.org/abs/1706.04507> accessed 4 September 2018

O'Hara K and Shadbolt N, 'The Right to Be Forgotten: Its Potential Role in a Coherent Privacy Regime' (2015) 1 European Data Protection Law Review 178

Hungarian National Authority for Data Protection and Freedom of Information, 'The Opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in the Context of Data Protection' [2017]

Pacces AM and Visscher LT, 'Methodology of Law and Economics' in Bart van Klink and Sanne Taekema (eds), *Law and Method : Interdisciplinary Research into Law* (Mohr Siebeck 2011)

Pasquale F, *The Black Box Society : The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

Politou E, Alepis E and Patsakis C, Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions' [2018] Journal of Cybersecurity <https://doi.org/10.1093/cybsec/tyy001> accessed 2 September 2018.

Rauchs M and others, 'Distributed Ledger Systems: A Conceptual Framework' (Cambridge Centre for Alternative Finance 2018) <https://ssrn.com/abstract=3230013> accessed 19 September 2018

Rivest RL, Shamir A and Adleman L, 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems' (1978) 21 Communications of the Association for Computing Machinery 120 <http://portal.acm.org/citation.cfm?doid=359340.359342> accessed 30 June 2018

Salmensuu C, 'General Data Protection Regulation and the Blockchains' (2018) 1 Liikejuridiikka 92

Salmon J and Maxwell W, 'A guide to blockchain and data protection' (*Hogan Lovells*, September 2017) 6 <www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf> accessed 30 June 2018

Spindler G and Schmechel P, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 163 <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jipitec7&id=169&men_tab=srchresults> accessed 20 September 2018

Stalla-Bourdillon S, Knight A, 'Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Jouurnal 284

Svantesson DJB, 'A Jurisprudential Justification for Extraterritoriality in (Private) International Law.' (2015) 13 Santa Clara Journal of International Law 517

Swan M, *Blockchain: Blueprint for a new economy,* (O'Reilly Media Inc 2015)

Tarhonen L, 'Pseudonymisation of Personal Data According to the General Data Protection Regulation' in Päivi Korpisaari (ed), *Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2016* (University of Helsinki 2016) 10

Tapscott D and Tapscott A, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*, (Penguin, 2016).

Tikkinen-Piri C, Rohunen A and Markkula J, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34 Computer Law and Security Review 134

European Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor, *Handbook on European Data Protection Law* (2018)

Van Geelkerken FWJ and Konings K, 'Using Blockchain to Strengthen the Rights Granted through the GDPR'(Lviv Polytechnic National University, December 2017) 458 <http://ena.lp.edu.ua/bitstream/ntb/40463/2/2017_F_W_J_van_Geelkerken-Using_Blockchain_458-461.pdf> accessed 30 June 2018

Villaronga EF, Kieseberg P and Li T, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 Computer Law and Security Review 304

Werbach K and Cornell N, 'Contracts Ex Machina' (2017) 67(2) Duke Law Journal 313

Wirth C and Kolain M, 'Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data' in Wolfgang Prinz & Philipp Hoschka (eds), *Proceedings of the 1st ERCIM Blockchain Workshop 2018* (European Society for Socially Embedded Technologies 2018) <https://hdl.handle.net/20.500.12015/3159> accessed 19 August 2018

Wright A and De Filippi P, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015),< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> accessed 29 June 2018

Zanfir G, 'Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reforming European Data Protection Law* (Springer 2015) 227

Zarsky TZ, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47(4) Seton Hall Law Review 995

Zheng Z and others, 'An Overview of Blockchain Technology: Architecture, Consensus, and

Future Trends' (2017 Institute of Electrical and Electronics Engineers 6th International Congress on Big Data, Honolulu, 25-30 June 2017) 557

Online sources

— —, '1 Introduction' (*Swarm Guide*) <https://swarm-guide.readthedocs.io/en/latest/introduction.html> accessed 18 September 2018

— —, 'Blockchain Basics: How Blockchain Works - Digital Signatures' (*Lisk Academy*) <https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/digital-signatures> accessed 20 September 2018

— —, 'Confidential Transactions' (*Elements Project*) <www.elementsproject.org/elements/confidential-transactions/> accessed 14 August 2018

— —, 'Couldn't Everybody Put in Random Private Keys, Look for a Balance, and Send to Their Own Address ?' (*MyEtherWallet FAQ*) <https://kb.myetherwallet.com/faq/couldnt-everybody-put-in-a-random-key-and-send-to-own-address.html> accessed 3 September 2018

— —, 'GDPR encryption: what you should know and what you do not know' (*I-scoop*) <www.i-scoop.eu/gdpr-encryption/> accessed 31 July 2018

— —, Proof of Stake FAQs' (*Github Ethereum wiki*) <http://cryptorials.io/glossary/proof-of-stake/%5Cnhttps://en.bitcoin.it/wiki/Proof_of_Stake> accessed 20 September 2018

— —, 'Ring Signature' (*Monero*) <https://getmonero.org/resources/moneropedia/ringsignatures.html> accessed 14 August 2018

— —, 'Stealth Address' (*Monero*) <https://getmonero.org/resources/moneropedia/stealthaddress.html> accessed 14 August 2018

Ausloos J, 'The Interaction between the Rights to Object and to Erasure in the GDPR' (*KU Leuven Data Protection and Privacy Blog*, 25 August 2016) <www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/> accessed 3 September 2018

Armerding T, 'The 17 biggest data breaches of the 21st century' (*CSO*, January 26 2018) <www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html> accessed 30 July 2018

Bakker D, 'Blockchain in transit?' (*UL Transaction Security Blog*, 2 June 2016) < https://blog.ul-ts.com/posts/blockchains-in-transit/> accessed 26 June 2018

Buterin V, 'A next-generation smart contract and decentralized application platform' (Ethereum White Paper, 2014) 10 < https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> accessed 30 June 2018

— —, 'On Public and Private Blockchains' (*Ethereum Blog,* 6 August 2015) < https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> accessed 30 June 2018

— —, 'Privacy on the Blockchain - Ethereum Blog' (*Ethereum blog*, 15 January 2016) <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/> accessed 14 August 2018

Carson BB and others, 'Blockchain beyond the hype: What is the strategic business value?'

(*McKinsey & Company*, June 2018) <www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value> accessed 30 June 2016

Davis H, 'Ted Cruz using firm that harvested data on millions of unwitting Facebook users' (*The Guardian* 11 December 2015) < www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> accessed 20 June 2018

Di L, 'Why Do I Need a Public and Private Key on the Blockchain?' (*WeTrust Blog*, 29 January 2017) <https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76> accessed 10 July 2018

Greenspan G, 'Blockchains vs centralized databases' (*Multichain*, 17 March 2016) <www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/> accessed 26 June 2018

— —, 'The Blockchain Immutability Myth' (*Coin Desk*, 9 May 2017) <www.coindesk.com/blockchain-immutability-myth/?utm_content=bufferdd3ca&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer> accessed 2 July 2018

Kakouris T, 'Decentralized Wallets : A Need & a Hurdle' (*Medium*, 11 June 2018) <https://medium.com/@tasoskakouris/decentralized-wallets-a-need-a-hurdle-486d3c57b1a9> accessed 17 September 2018

Sherman L, 'Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That' (Forbes, 19 April 2018) <https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#2eee872b1bc8> accessed 30 June 2018

Webpage of DECODE project, <https://decodeproject.eu/> accessed 19 August 2018

Webpage of Ethereum, <https://ethereum.org/> accessed 2 July 2018

Official Material

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) WP 136

Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010) WP169

Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP 216

Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014) WP217

Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2016) WP251

Article 29 Data Protection Working Party, 'Guidelines on Transparency Under Regulation 2016/679' (2016) WP260

Council of Europe

European Convention for the Protection of Human Rights and Fundamental Freedoms [1950] 213 U.N.T.S 221

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No 108

OECD

OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [1980] OECD/LEGAL/0188

Primary Law

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C306/1

Consolidated version of the Treaty on the Functioning of the European Union [2008] OJ C115/1

Charter of Fundamental Rights of the European Union [2012] OJ C/326/02

Secondary Law

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive)

European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1

Cases

Advocate General's Opinions

Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* [2013] EU:C:2013:424, Opinion of AG Jääskinen

European Court of Justice

Case C-101/01 *Criminal proceedings against Bodil Lindqvist* EU:C:2003:596

Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications Marine and Natural Resources and Others and Kärntner Landesregierung and Others* EU:C:2014:238

Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* EU:C:2014:317

Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779

Case C-434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:994

Abbreviations

Charter	Charter of Fundamental Rights of the European Union [2012] OJ C/326/02
Commission	European Commission
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No 108.
DLT	Distributed ledger technology
DPA	Data Protection Authority
DPD	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
GDPR	European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation)
ICO	Information Commissioner's Office
IPFS	InterPlanetary File System
ISP	Internet Service Provider
OECD	Organisation for Economic Cooperation and Development
PoS	Proof of Stake
PoW	Proof of Work
SMPC	Secure Multi-Party Computation
TFEU	Treaty on the Functioning of the European Union
The Court	Court of Justice of the European Union
US	The United States
WP29	Article 29 Data Protection Working Party

1 Introduction

1.1 Background

Data protection and privacy are currently hot topics as the European Union General Data Protection Regulation[1] (GDPR) entered into force 25 May 2018. The GDPR and frequent announcements of data breaches have attracted a lot of attention in the media that has increased individuals' awareness of their rights as data subjects. This is a welcomed trend in the digital world, where personal data has been described as the 'new oil of the internet' or the 'new currency'. A vast amount of personal data is collected, processed, and analysed for different purposes by private companies, governments, researchers, and so forth. The internet has turned into a place where power and control are in the hands of big centralised intermediaries, such as Google, Facebook, and Amazon, instead of individuals.[2] Primarily the centralised intermediaries collect and process personal data for appropriate purposes in order to offer better user-centric products and services and to foster innovation. Despite the positive purposes, several points of tension have been recognised in respect to privacy and data protection of individuals.

The Facebook–Cambridge Analytica data scandal was an illustrative example of the risks related to the collection and processing of personal data by centralised intermediaries.[3] As a response to the issues regarding privacy and data protection, the European Union (EU) regulators drafted the GDPR to give more control for individuals over their personal data by setting obligations for centralised intermediaries regarding collection and processing of personal data. Early blockchain developers also recognised the issues arising from

[1] European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

[2] Roberta Filippone, 'Blockchain and Individuals' Control over Personal Data in European Data Protection Law' (Master's Thesis, Tillburg University 2017) 6-7 <http://arno.uvt.nl/show.cgi?fid=143638> accessed 20 June 2018.

[3] The scandal was about inappropriate collection of personal data of up to 87 million Facebook users by Cambridge Analytica. The data was allegedly used in political campaigns in the US without permission of the data subjects. On the Facebook–Cambridge Analytica data scandal see eg Harry Davis, 'Ted Cruz using firm that harvested data on millions of unwitting Facebook users' (*The Guardian* 11 December 2015) < www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> accessed 20 June 2018.

centralisation although the privacy issues were not the only concern for them.[4] Blockchain developers took a completely different approach for the issues – eliminate the centralised intermediaries, 'the middle-men'. Distributed ledger technologies, such as the blockchain technology, enable individuals to transact directly with each other, peer-to-peer, without the middle-men. Thus, it could be said that regulators and blockchain developers had a common objective *to give individuals more control over their data* although they had entirely different approaches.[5] However, the fundamentally different approaches have resulted in several tensions between the GDPR and blockchain technology.

The GDPR was a necessary reform of which one of the main objectives was to harmonise fragmented national data protection laws in the EU. The GDPR with some new rights and obligations, the extraterritorial effect, and considerable administrative sanctions is a clear statement by the EU that data protection should be taken seriously. On the one hand, companies have started to pay attention to their privacy policies and how to comply with the regulation, and on the other hand, the GDPR has raised awareness among natural persons of their rights as data subjects. As the blockchain technology is a rather new technology, its potential has been recognised only in recent years. That explains why the GDPR was not drafted taking account of this novel decentralised technology. In any case, the GDPR is technologically neutral regulation, and blockchain technology is not an exception.[6] The technology must take data protection of individuals and the GDPR seriously since the regulation risks becoming an obstacle for a broad introduction of this potentially revolutionary technology.

A blockchain is an append-only distributed ledger used to record data of transactions into packages called 'blocks'. The blocks are linked together in a chronological order forming a chain of blocks, thus the name blockchain.[7] The data stored and processed on blockchains may also contain personal data. As the threshold for what constitutes personal data is rather low, blockchain applications might trigger the GDPR more often than blockchain developers had

[4] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) 1 <https://bitcoin.org/bitcoin.pdf> accessed 29 June 2018.
[5] Filippone (n 2) 6-7.
[6] Recital 15 of the GDPR.
[7] John Salmon and Winston Maxwell, 'A guide to blockchain and data protection' (Hogan Lovells, September 2017) 6 <www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf> accessed 30 June 2018.

believed.[8] Processing personal data on blockchain raises many controversial aspects regarding the GDPR, for instance, in relation to the principle of accountability, the principle of data minimisation, and the principle of storage limitation.[9] One of the most fundamental problems is, however, the conflict between the right to erasure under the GDPR and the 'immutability' of blockchain technology.

1.2 Research problem, scope of the study, and structure

Considering that blockchain technology has great potential to change our lives in different areas from casting votes in elections to administering land registries and facilitating machine-to-machine communication[10], to name a few, it is worth examining the issues in relation to the GDPR as they might hinder the development of this possibly revolutionary technology. This master's thesis is focusing on one of the most problematic issues regarding blockchain and the GDPR – the conflict between the right to erasure and the immutability of blockchain. According to Article 17 of the GDPR, data subjects have a right to have their personal data erased under certain circumstances. This right is known as the right to erasure or the right to be forgotten. However, the more accurate term 'right to erasure' is used hereinafter in this thesis.[11] The blockchain technology is in apparent conflict with the right to erasure because one of the main features of blockchains is the 'immutability',[12] which means that removing or altering old blocks is extremely difficult if not practically impossible. The purpose of this research is to study the conflict and solutions proposed to resolve it in order to find out whether the conflict could be reconciled. Based on that purpose, the research questions of this thesis ask: considering different solutions proposed to reconcile the conflict between the right to erasure under Article 17 of the GDPR and the 'immutability' of public and permissionless blockchains, what is the legal situation now and how could potentially remaining issues be addressed?

[8] Luis-Daniel Ibáñez, Kieron O'Hara and Elena Simperl, 'On Blockchains and the General Data Protection Regulation Brief Introduction to Blockchain Technologies' (University of Southampton 2018) 12 < https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf> accessed 20 September 2018.
[9] Filippone (n 2) 32.
[10] More on how blockchain technology could change our lives see eg. Phillip Boucher, 'How Blockchain Technology Could Change Our Lives' (European Parliamentary Research Service, 2017).
[11] The label of Article 17 of the GDPR contains both terms, but the right to be forgotten is in brackets. The term right to be forgotten is more well-known and more used in academic literature, but it has been criticised for being misleading. For instance, Markou has listed ten reasons why the term right to be forgotten should not be used at all. See Christiana Markou, 'The 'Right to Be Forgotten': Ten Reasons Why It Should Be Forgotten' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reforming European Data Protection Law* (Springer 2015).
[12] The term immutable has been criticised as misleading, but it is the most commonly used term to describe this feature, and in the absence of better term it is used hereinafter in this thesis. See n 45.

Some demarcations concerning the scope of this research are in order. It is essential to understand that there are different blockchain types depending on who has access to the blockchain and who can act as a verifier and maintain the blockchain network. This research is limited to the public and permissionless blockchain technology because it represents a more traditional form of the blockchain technology, which is closer to genuine decentralised peer-to-peer networks than other more private blockchain types that require, at least to some extent, the involvement of trusted third party in the operation of the blockchain. Secondly, the public and permissionless blockchain technology is more challenging and interesting regarding privacy and data protection of natural persons than more private blockchain types because many of the problems regarding data protection could be avoided in private and permissioned blockchains by introducing a centralised intermediary in the process.[13] Two most well-known examples of public and permissionless blockchain technology are Bitcoin and Ethereum. The term traditional blockchain is used hereinafter to describe public and permissionless blockchains.

This thesis begins with a brief introduction of the blockchain technology that aims to explain what all fuss is about, what are blockchains used for, and how do they work. Chapter 3 shortly presents the history of data protection in the EU and what changes the GDPR brought. Then, in Chapter 4, the focus shifts to the blockchain technology and data protection at a general level. Before even trying to understand the conflict between the right to erasure and the immutability, it is necessary to analyse whether the GDPR applies to blockchain technology and in case it does, who should be responsible for compliance with the regulation in such decentralised systems. After that analysis, this research moves on to study the right to erasure and the conflict between the right and the immutability of traditional blockchains in Chapter 5. This Chapter seeks to give a proper insight into the right erasure to help to understand the conflict. After that, the thesis moves on to analyse some legal and technological solutions proposed to reconcile the conflict. Based on that analysis, it is considered whether traditional blockchains infringe Article 17 and how to address potentially existing problems to enable further development of traditional

[13] FWJ Van Geelkerken and K Konings, 'Using Blockchain to Strengthen the Rights Granted through the GDPR'(Lviv Polytechnic National University, December 2017) 458, 459 <http://ena.lp.edu.ua/bitstream/ntb/40463/2/2017_F_W_J_van_Geelkerken-Using_Blockchain_458-461.pdf> accessed 30 June 2018; Michèle Finck, 'Blockchains and Data Protection in the European Union' (2017) 10(1) Max Planck Institute for Innovation and Competition Research Paper Series 6 <http://dx.doi.org/10.2139/ssrn.3080322> accessed 30 June 2018.

blockchains without compromising data subjects' right to erasure. Finally, in the last chapter, the findings are summed up, and some concluding remarks are made.

1.3 Research method and material

The primary purpose of this research is to study the conflict between the right to erasure and the immutability of traditional blockchain technology. This research does not settle for identifying issues but instead aims to take an optimistic approach by trying to find ways to address the issues. It is necessary to look into the underlying issue between the problems of the GDPR and the blockchain technology to understand better the conflict between Article 17 and the immutability of blockchain technology. That underlying issue is about balancing between the data protection of individuals and the promotion of innovation. Regarding methodology, this research aims to rely on law and economics approach, which enables to use legal dogmatic approach for identifying the content of the law before moving to assess and criticise the law from the point of view of efficiency.[14] Thus, before considering the efficiency of the new data protection regulation in relation to the traditional blockchain technology, this research relies on legal dogmatic tools to recognise the legal problem. Normative economic analysis of law considers the need for a change, for new policy recommendations, from an economic perspective. The notion of efficiency is used as a framework for assessing whether there is a need for such a change.[15] In the normative economic analysis, so-called Kaldor-Hicks efficiency is generally used to describe that efficiency, 'a social state is efficient if it is no longer possible to increase the total welfare of a society'. In other words, there is a need for change if it is possible to increase 'the total welfare of a society' by creating enough benefits for some individuals while compensating the loss caused to others.[16]

This research balances between the data protection of natural persons and the promotion of innovation and argues that there is a need for change. The change is not about reforming the GDPR or drafting a new blockchain-specific regulation, but instead, the change is about interpretation. The issues cannot be solved by interpreting purely literally the provisions of the

[14] Robert Cryer and others, *Research Methodologies in EU and International Law*, (Hart Publishing 2011) 38.
[15] Alessio M Pacces and Louis T Visscher, 'Methodology of Law and Economics' in Bart van Klink and Sanne Taekema (eds), *Law and Method : Interdisciplinary Research into Law* (Mohr Siebeck 2011) 88.
[16] Pacces and Visscher (n 15) 89.

GDPR. Instead, there is a need for flexible interpretations, which consider the specific characteristics of blockchain technology but also guarantee a sufficient level of protection for data subjects. This research focuses on providing flexible interpretations especially for legal problems in relation to the right to erasure and the immutability of traditional blockchains.

The source material for this research consists of hard and soft law EU instruments, including the GDPR and Article 29 Working Party opinions[17]. As regards to the case law, two most important cases of the Court of Justice of the European Union (the Court) are the *Google Spain*[18] and *Breyer*[19] case. Regarding academic discussion pertaining to the issues between the blockchain technology and the GDPR, there are a few articles written by legal scholars, which are an important source of this thesis. In addition to the legal instruments and academic sources, a relevant source for this research is technological white papers written by blockchain developers.

2 A brief introduction to blockchain technology

2.1 What all the fuss is about?

'The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.'[20]

The story of blockchain began of the white paper of unknown author or group of authors under the name Satoshi Nakamoto.[21] Although the term blockchain was not used in the white paper that described the concept and technical details of Bitcoin, which was the first decentralised cryptocurrency, the white paper can be regarded as a starting point for the development of the blockchain technology. Bitcoin technology combined already existing technological

[17] The European Data Protection Board (EDBP) was set to continue the work of Article 29 Working Party, as from 25 May 2018.
[18] Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* EU:C:2014:317.
[19] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779.
[20] Don Tapscott and Alex Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*, (Penguin, 2016).
[21] Nakamoto (n 4).

innovations in a creative way.[22] The cryptocurrencies are the first and the most well-known use case of blockchain technology. Nevertheless, more on more potential use cases for the technology have been identified.

The next chapter in the story of blockchain was the smart contracts. Blockchain technology has developed in the recent years so that it is possible to create new types of blockchain-based smart contracts. Smart contracts are encoded on blockchain and can automatically enforce and execute predetermined terms of contracts. This enables individuals to make contracts with each other without any middle-men in a cheap and quick manner. Smart contracts can be envisioned, for instance, to enforce wills and other agreements or to enable the Internet of Things devices to operate and share information with each other autonomously.[23] The most well-known platform for smart contract applications is Ethereum, which was released in 2014.[24]

Next focus on the development of blockchain technology is said to be on 'blockchain applications beyond currency, finance, and markets – particularly in the areas of government, health, science, literacy, culture, and art'.[25] The blockchain has potentially disruptive impacts on digital services and existing business models, which has been recognised among others by the European Commission, which has already taken action by launching the EU Blockchain Observatory and Forum and by funding blockchain projects.[26]

Even though the disruptive potential of blockchain technology has been widely recognised, there seems to be a need for some clarifications. Firstly, a blockchain is essentially just a shared database. The blockchain technology is not a magical tool for creating value for any use case, but rather the decision to use blockchain technology should be based on thorough consideration

[22] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015), 5 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> accessed 29 June 2018.
[23] Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina.' (2017) 67(2) Duke Law Journal 313, 335-36 <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj> accessed 29 June 2018 .
[24] Ethereum is 'a decentralized platform that runs smart contracts: applications that run exactly as programmed without a possibility of downtime, censorship, fraud or third-party interference' <https://ethereum.org/> accessed 2 July 2018.
[25] Melanie Swan, *Blockchain: Blueprint for a new economy*, (O'Reilly Media Inc 2015) Preface ix.
[26] Commission, 'European Commission launches the EU Blockchain Observatory and Forum' (Press release 2018) <http://europa.eu/rapid/press-release_IP-18-521_en.htm> accessed 26 June 2018.

of whether blockchain is genuinely necessary and better option than existing ones.[27] Secondly, the technology does not live up to the hype yet. There are still several technical issues that need to be solved before the technology can be adopted as widely as imagined in many descriptions of the potential use cases.[28] However, the technology is developing rapidly, and developers are continuously working to solve these issues.[29] Despite the rapid development, it seems likely that blockchain technology will not suddenly disrupt digital services and business models, but instead 'the blockchain revolution' might be a gradual process, and, as with the development of the Internet, it might take decades to reshape our economies.[30]

2.2 Different types and use cases of blockchains

The blockchain technology can be regarded as disruptive on two fronts. Firstly, the blockchain technology might challenge existing platform economies and be the 'next step in the peer-to-peer economy'.[31] Here, the value of the blockchain technology is at enabling unknown or untrusted parties to transact with each other without a need for middle-men to create trust, but instead, the technology provides the trust between the parties. Bitcoin is the most well-known use case of the traditional blockchain technology, but many other use cases beyond cryptocurrencies can be imagined. For instance, traditional blockchains could disrupt current sharing economies by replacing intermediaries such as Airbnb or Uber with blockchain technology.[32] These disruptive visions of traditional blockchains require a significant further development of the technology before the impacts could be seen in our society and everyday life.[33] As already mentioned, this is more likely a rather long gradual process than a sudden change.

---

[27] The blockchain cannot compete with traditional databases when it comes to confidentiality and performance. However, blockchain might be viable solution, if there is a need for disintermediation and robustness. See eg Gideon Greenspan, 'Blockchains vs centralized databases' (Multichain, 17 March 2016) <www.multichain.com/blog/2016/03/blockchains-vs-centralized-databases/> accessed 26 June 2018; David Bakker, 'Blockchain in transit?' (*UL Transaction Security Blog*, 2 June 2016) < https://blog.ul-ts.com/posts/blockchains-in-transit/> accessed 26 June 2018.

[28] One of the main technical issues is the scalability; current technology does not enable blockchain network to process enough transactions per second (tps) (current maximum being 7 tps). For example, VISA enables to process typically 2,000 tps and maximum is even 10,000 tps. Other issues relate block size and bandwidth, latency, vulnerability to 51-percent attack, and so forth. See Swan (n 25) 81-83.

[29] Swan (n 25) 84.

[30] Marco Iansiti and Karim Lakhani, 'The Truth About Blockchain' (2017) 95(1) Harvard Business Review 118, 121.

[31] Wright and De Filippi (n 22) 4.

[32] Finck (n 13) 9.

[33] Boucher (n 10) 22.

Secondly, the blockchain technology is used by 'mainstream actors' such as companies, banks, and governments to bring operational efficiencies to their businesses.[34] Here, the blockchain is not genuinely decentralised as it is controlled by centralised administrators, but it can be used to reduce operational costs by facilitating record keeping and transaction reconciliation.[35] The value of the permissioned blockchain technology is not at creating trust between unknown parties but instead at providing transparent and immutable databases while maintaining control over the network and databases. For instance, Ripple is a real-time gross settlement system based on blockchain technology that has brought together several financial institutions around the globe to settle their transactions securely, in real-time and at a lower cost compared to current multi-day processing.[36] An excellent example from the government level is the Swedish land registry project, which investigates the possibilities to use permissioned blockchains to create faster and more transparent real estate transactions.[37] Permissioned blockchains offer many advantages compared to their permissionless counterparts in relation to performance, scalability, cost efficiency, and governance.[38] However, permissioned blockchains are criticised for being closer to traditional centralised databases than to the original idea of blockchain as a decentralised database. In the short term, permissioned blockchains are more exciting and offer more value for investors than traditional blockchains because permissioned blockchain technology is technically more mature and ready for companies and governments to adopt.[39]

Above made distinction between permissionless (traditional) and permissioned blockchain technology illustrates important differences between two main blockchain types. There are a great number of terms to describe different types of blockchains; opaque or transparent, open or closed, private or public, and so forth. Essentially there are, however, even four different types of blockchain.[40] The differences between blockchain types depend on who has access to

[34] Boucher (n 10) 5.
[35] Brant Carson and others, 'Blockchain beyond the hype: What is the strategic business value?' (McKinsey & Company, June 2018) <www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value> accessed 30 June 2016.
[36] Finck (n 13) 8.
[37] Magnus Kempe, 'The Land Registry in the blockchain'(Report of a development project with Lantmäteriet, Telia Company, ChromaWay and Kairos Future, July 2016) <http://ica-it.org/pdf/Blockchain_Landregistry_Report.pd> accessed 30 June 2018.
[38] 'What is Permissioned Blockchain Network?' (*Monax*) <https://monax.io/learn/permissioned_blockchains/> accessed 30 June 2018.
[39] Carson and others (n 35).
[40] There are different views of how many blockchain types there are. This research presents four different types as that represents the most exhaustive illustration of different blockchain types. Another common way to present different blockchain types is to divide them into three types; public, private and consortium blockchains. In this

the blockchain and who can act as a validator and maintain the blockchain network (permissioned or permissionless), and whether the blockchain is run on a private network or the Internet (private or public).

Type of blockchain	Description	Examples of the use cases
Permissioned private ledger	The ledger is run on a private network and governed by one or more administrators. Use requires joining to the private network and permission to join granted by the administrator(s).	HR Compliance system
Permissionless private ledger	The ledger is run on a private network governed by one or more administrators. Use does not require permission to join but requires access to the private network.	Whistleblower system of multinational organisation.
Permissioned public ledger	The ledger is run publicly on the Internet and governed by one or more administrators. Use requires joining to the network and permission to join granted by the administrator(s).	A digital rights management system
Permissionless public ledger	The ledger is run publicly on the Internet, not owned or governed by any administrator, and open for anyone to join.	Bitcoin and Ethereum

Table of different blockchain types.[41]

This research focuses on the public and permissionless blockchain technology because it is the most decentralised and 'purest' type of blockchain representing the original objectives of the early blockchain developers – to eliminate middle-men. The permissionless and public blockchain technology is also the most challenging type in respect of data protection because in other types many of the data protection issues can be solved by relying on some trusted third party.[42] The immutability is a concern in particular for traditional blockchains. In more private versions of blockchains, the solutions for erasing old data are much easier to come by because

model public blockchain is used to enable peer-to-peer transaction without a need for a middle-men, private blockchain is controlled by one entity, for instance., multinational company aiming to unify its databases among its subsidiaries, and consortium blockchain is used by group of entities to join together in order to enhance efficiency and reduce transactions costs. See eg Vitalik Buterin, 'On Public and Private Blockchains'(*Ethereum Blog,* 6 August 2015) < https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> accessed 30 June 2018.

[41] The table is based on a table presented in; Tuomo Kinnunen and others, *Applying blockchain technology and its impacts on transport and communications*, (Publication of the Ministry of Transport and Communications 12/2017). The use case examples are from article of Finnish software development company specialising in blockchain technology. See 'Blockchain and GDPR: How to square privacy and distributed ledgers' (*Chainfrog*, 2017) <http://www.chainfrog.com/wp-content/uploads/2017/08/gdpr.pdf> accessed 27 June 2018.

[42] Van Geelkerken and Konings (n 13) 459; Finck (n 13) 6.

in permissioned blockchains the validators could together decide to modify data on old block and collaborate to validate the modifications. While this provides an attractive solution for many business and governmental blockchain projects, it conflicts with the very reason why traditional blockchains are immutable – the users cannot independently affirm that the data is not modified, but instead, they must *trust* the permissioned validators to act honestly.[43] Terms blockchain and traditional blockchain will be used hereinafter when referring to permissionless and public blockchain technology unless otherwise specified.

2.3 Technical properties of blockchain technology

There is no perfect definition of blockchain technology because the definition and the technical features depend on the different types and use cases of blockchains. A blockchain is often confused with distributed ledger technology (DLT). A blockchain is one type of DLT, but unlike in other DLTs, the database is always formed into a chain of blocks.[44] This research is focused on blockchain technology rather than on DTLs in general.

A blockchain is a distributed ledger or database formed into a chain of blocks. Each block is composed of two separate parts; information of transactions (transactional data) and a header. The header contains, *inter alia*, a timestamp, hash value of the block, and a hash value of the previous block.[45] The hash is formed by using a mathematical algorithm that forms a unique string of letters and numbers from the transactional data of the block.[46] If one letter or even accent of the transactional data is changed, the algorithm calculates entirely different hash. As every block also contains the hash of the previous block, the blocks are linked to each other. Further, as only new blocks can be added to the chain, the blockchain forms 'a chronological database'.[47] Even a slight modification of block's data would be detected by other participants of the network because the hash of the next block would not correspond to the data on the

[43] Dave Michels, 'Can Blockchain Operators Comply with EU Data Protection Law?' [2018] Binary District Journal <https://journal.binarydistrict.com/can-blockchain-operators-comply-with-eu-data-protection-law/> accessed 19 September 2018.
[44] Daniel Conte de Leon and others, 'Blockchain: Properties and Misconceptions' (2017) 11 Asia Pacific Journal of Innovation and Entrepreneurship 286, 291 <http://www.emeraldinsight.com/doi/10.1108/APJIE-12-2017-034>.
[45] On more thorough presentation of blockchain architecture see eg Zibin Zheng and others, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends'(2017 Institute of Electrical and Electronics Engineers 6th International Congress on Big Data, Honolulu, 25-30 June 2017) 557, 558.
[46] Conte de Leon and others (n 44) 288.
[47] Salmon and Maxwell (n 7) 6.

modified block. Data on old blocks could only be modified or erased by unbuilding the blockchain, modifying the data, and then rebuilding the whole blockchain again, or by building a new blockchain including the modifications. However, in order to become a valid blockchain, this would require a majority of the network to validate the modifications, which can be extremely difficult to achieve on the blockchain network. This feature enables to verify that data on old blocks are not modified or tampered.[48] In other words, the ledger can be regarded as tamper-proof or immutable. In the absence of a better definition for the feature, the term *immutability* is used in this thesis to refer to this feature of blockchain technology.[49]

A blockchain is a *distributed* ledger, *i.e.*, the ledger that is not stored in a centralised data silo but instead on computers of all participants of the blockchain network, which are called nodes. Nodes that store the whole blockchain are full nodes whereas 'lightweight' nodes store only the part of the blockchain that is relevant to them.[50] A blockchain is also *decentralised* in a sense that there is no need for central authorities to create a trust that the transactions on a blockchain are valid. New transactions are broadcasted on the network and grouped into new blocks. The trust is created by sharing the ledger to every node on the network, who automatically checks whether the transactions in the new block are valid.[51]

How new block is added to the chain depends on the *consensus algorithm* used on the blockchain. The purpose of the consensus algorithms is to ensure that all nodes have the same copy of the ledger, *i.e.*, to confirm consensus of the current state of the ledger.[52] Bitcoin uses a Proof of Work (PoW) consensus in which new blocks are added to the chain by miners who compete against each other by solving mathematical puzzles. The one who first solves the puzzle creates a new block and gets rewarded for the work.[53] PoW consensus mechanism has

[48] Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers' (2016) 2 European Data Protection Law Review 422, 426.
[49] Terms tamper-proof and immutable have been criticized in blockchain literature. It has been argued that true immutability does not exist as data on blockchain can be modified if there is a consensus to modify it. See eg Gideon Greenspan, 'The Blockchain Immutability Myth' (*Coin Desk*, 9 May 2017) <www.coindesk.com/blockchain-immutability-myth/?utm_content=bufferdd3ca&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer> accessed 2 July 2018.
[50] Vitalik Buterin, 'A next-generation smart contract and decentralized application platform' (Ethereum White Paper, 2014) 10 < https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> accessed 30 June 2018.
[51] Boucher (n 10) 8.
[52] Zheng and others (n 45) 559.
[53] Nakamoto (n 4) 3.

been heavily criticised for its energy consumption because solving the puzzles requires a substantial amount of computational power and electricity.[54] There are some other consensus algorithms to verify the consensus of the network, such as Proof of Stake, Delegated Proof of Stake or Practical Byzantine Fault Tolerance. After a block is added to the chain, the new version of the blockchain is distributed to every node of the network, who then updates their versions of the blockchain to correspond with the consensus.[55]

Furthermore, blockchain relies on an asymmetric encryption, also known as the *public-key encryption,* to verify authenticity and author of the transaction. Every user has own private key and public key. The public key can be considered as an account number that hides the true identity of the user. The private key, in turn, can be considered as a password that should not be revealed to others.[56] The public key and the private key are connected to each other by a mathematical algorithm so that the public key is derived from the private key, but it is not possible to reverse the algorithm to derive one's private key of the public key.[57] In addition to public keys and private keys, an essential part of most blockchain protocols is digital signatures. A digital signature is created by an algorithm that combines user's (user sending the transaction) private key and the data to be sent. The user does not have to send his or her private key to the recipient of the transaction, but instead, the transaction made on the blockchain network is signed with a digital signature.[58] A common example of the digital signature and the public-key encryption is a hypothetical situation where Alice wants to send a message to another user Bob.[59] This is a two-step process. First, Alice signs the message with her private key and then sends the message, the digital signature and her public key to Bob. In the second phase, Bob

[54] Bitcoin PoW consensus is estimated to consume same amount of electricity per year (61.4 TWh) than a country like Switzerland. See eg. Lee Sherman, 'Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That' (Forbes, 19 April 2018) <https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#2eee872b1bc8> accessed 30 June 2018.

[55] Boucher (n 10) 5.

[56] Finck (n 13) 4.

[57] Leon Di, 'Why Do I Need a Public and Private Key on the Blockchain?' (*WeTrust Blog*, 29 January 2017) <https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76> accessed 10 July 2018.

[58] 'Blockchain Basics: How Blockchain Works - Digital Signatures' (*Lisk Academy*) <https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/digital-signatures> accessed 20 September 2018.

[59] Alice and Bob are fictional characters used commonly in cryptographic literature. They were originally introduced in an article describing digital signatures and public key cryptosystems. See RL Rivest, A Shamir and L Adleman, 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems' (1978) 21 Communications of the Association for Computing Machinery 120 <http://portal.acm.org/citation.cfm?doid=359340.359342> accessed 30 June 2018.

can verify two things by using the message, Alice's public key and the digital signature; that the message is not altered by anyone and that Alice is the original sender of the message.[60]

Transparency is an inherent feature of blockchain technology.[61] The transparency of the blockchain arises from the publicity of the ledger. Transactions in the ledger are publicly available for anyone in the world to review although the identity of individuals behind the transactions is concealed with public keys. While the transactional data can be encrypted, most decentralised systems are designed in a manner that leaves metadata of the transactions (who are the parties of the transactions, what kind of transaction it is, etc.) visible to anyone.[62] Transparency of transactions and public keys is essential in traditional blockchains as it enables nodes to verify transactions without a centralised party.[63] Despite the fact that the public keys are designed to hide the identity of the user, public keys cannot provide anonymity because it is possible to identify a user from the public key with additional information.[64] This is where data protection issues may arise. The blockchain developers might have misbelieved that the 'anonymity' of blockchain is enough to avoid triggering data protection laws, which is not the case as will be presented in more detail in Chapter 4.[65]

3 Regulation of data protection in Europe

3.1 History of data protection in Europe

Before turning to the history of data protection, it is necessary to bring some clarification to the relationship of the right to privacy (or the right to respect for private life) and the right to data protection. The history of the right to privacy goes much further than the history of the right to data protection. Since the recognition of data protection as a relevant field of law, it has been closely connected to the right to privacy. The right to data protection was subsumed into the

[60] Zheng and others (n 45) 558.
[61] Primavera De Filippi, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) 9 Journal of Peer Production 18 <http://peerproduction.net/wp-content/uploads/2016/08/blockchain-technologies-draft.pdf> accessed 30 June 2018.
[62] De Filippi (n 61) 10.
[63] De Filippi (n 61) 11.
[64] Finck (n 13) 13.
[65] Ibáñez, O'Hara and Simperl (n 8) 7.

right to privacy for a long time, but eventually, the rights developed into two separate fundamental rights under the EU law.[66] This distinction was recognised in the Charter of Fundamental Rights[67] (Charter), which became legally binding in 2009 when the Treaty of Lisbon entered into force. The Charter entails separate Articles for both the right to privacy and the right to data protection.[68] The distinction was later also confirmed by the Court.[69] The right to data protection can be considered as broader right because it is triggered *whenever* personal data is processed, whereas the right to respect for private life requires interference in private life.[70]

Early in the 1970s, different European countries started to draft and adopt their national data protection laws because the development of computation and automated data processing had created a foundation for a new form of society, information society, with new risks for individuals' privacy.[71] The Council of Europe paid attention to the same development of information technology and soon understood that the right to privacy in Article 8 of the European Convention on Human Rights[72] (ECHR) was insufficient to protect individuals from such risks.[73] As a response to that, the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) was adopted in 1981.[74] It is the only legally binding international instrument on the field data protection and still relevant as it went recently through a process of modernisation.[75] The purpose of the Convention 108 was to provide guidance for national legislators within and even outside of the EU because it was

[66] European Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor, *Handbook on European Data Protection Law* (2018) 18-19.
[67] Charter of Fundamental Rights of the European Union [2012] OJ C/326/02. The Charter became legally binding in 2009 when the Treaty of Lisbon entered into force.
[68] Article 7 of the Charter (Respect for private and family life) and Article 8 of the Charter (Protection of personal data).
[69] In *Digital Rights Ireland* the Court held that the directive 2006/24/EC violated both fundamental rights; the right to personal data protection and the right to respect for private life. Joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v. Minister for Communications*
Marine and Natural Resources and Others and Kärntner Landesregierung and Others EU:C:2014:238.
[70] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 19.
[71] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 18.
[72] European Convention for the Protection of Human Rights and Fundamental Freedoms [1950] 213 U.N.T.S 221.
[73] Paul De Hert and Serge Gutwirth, 'Data Protesction in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Sjaak Nouwt (ed), *Reinventing data protection?* (Springer 2009) 3, 5.
[74] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No 108.
[75] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 17.

drafted suitable for universal adoption.[76] The same type of guidelines for national data protection legislators, which have been more important for countries outside Europe, was introduced by the Organisation for Economic Co-operation and Development (OECD) in 1980[77].[78]

Despite the noble efforts by the Council of Europe and the OECD, the most comprehensive and influential data protection instrument was adopted by the EU in 1995.[79] The data protection directive (DPD)[80] was remarkable in many ways. The purpose of harmonising fragmented data protection laws led to some extent to harmonisation even outside of the EU because many non-EU countries used the DPD as a framework for drafting their data protection laws.[81] The DPD had two main objectives. The first objective was based on the need to harmonise national data protection laws and enhance the efficiency of the internal market. The objective of the free flow of data between the Member States was necessary to ensure the efficient functioning of the four fundamental freedoms of the single market.[82] The second objective was the protection of fundamental rights and especially the right to privacy with respect to processing of personal data. The DPD was the first directive to give a prominent role for the protection of fundamental rights. Therefore, it was also a significant step by the EU to protect fundamental rights.[83]

The next important achievement in the field of data protection was the Treaty of Lisbon, which entered into force in 2009.[84] The amendments of the Treaty of Lisbon not only confirmed the role of data protection as an independent fundamental right but also gave a new legal basis for the EU to regulate data protection matters. Even though the DPD had an objective of protecting fundamental rights, it was based on the internal market legal basis. Treaty of Lisbon created a

[76] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 17.
[77] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [1980] OECD/LEGAL/0188.
[78] Lee Bygrave, *Data privacy law: an international perspective* (Oxford University Press 2014) 50.
[79] Bygrave (n 78) 53.
[80] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).
[81] Bygrave (n 78) 53.
[82] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 29.
[83] Bygrave (n 78) 57.
[84] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C306/1.

comprehensive legal basis for data protection that covers all matters of EU competence.[85] The new legal basis, which can be found in Article 16 of the Treaty on the Functioning of the European Union[86] (TFEU), empowered the EU to take a further step in the field of data protection in the Union – the GDPR.[87]

At the beginning of this decade, globalisation and development of data processing techniques had created new challenges for the protection of personal data. The challenges were noticed by the Commission that released its communication of the challenges for the protection of personal data in 2010.[88] After different institutional organs of the EU had given their opinions of the communication, the Commission drafted its proposal for the new data protection regulation in 2012. The proposal was passed to the European Parliament and the Council, which gave their proposals for the new data protection regulation. The legislative 'trilogue' was completed in 2016 when the GDPR was finally approved.[89] The GDPR entered into force on 25 May 2018.

3.2 What new the GDPR brought to the field of data protection?

3.2.1 The GDPR as a response to the challenges of data protection in the digital age

The GDPR is primarily a response to the challenges of the DPD. Globalisation and the development of data processing techniques had led to problems for the DPD. Sharing information with other individuals across the globe had become relatively easy by using different social media services. In the meantime, governmental and commercial operators had developed new more efficient ways to collect and process personal data, which made the monitoring and surveillance of individuals' online behaviour a common practice.[90] The ways of obtaining the consent for data processing had become opaque and controversial as the

[85] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 28.
[86] Consolidated version of the Treaty on the Functioning of the European Union [2008] OJ C115/1.
[87] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 29.
[88] European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final 1.
[89] Paul De Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law and Security Review 179, 181.
[90] European Commission (n 88) 2.

consent was often prerequisite for using the application or the service. Furthermore, how data was processed was often slipped into lengthy and ambiguous terms and conditions that the users most often did not even bother to read. In short, the development had led to a situation where individuals had no actual control over their personal data.[91]

The response of the GDPR to the challenges was to develop data protection definitions, rights, obligations, principles, and so forth, to correspond better with the current data economy and data processing techniques. The GDPR also presented new rights for data subjects and obligations for data controllers and processors where necessary. Another main challenge of the DPD was the unsuccessful harmonisation attempt. Despite the objective of the DPD to harmonise national data protection laws, Member States ended up drafting diverse national laws and, the level of data protection varied between the Member States.[92] Thus, the 'choice of instrument' can also be regarded as one of the main achievements of the GDPR. As the GDPR is a regulation rather than a directive, it is directly applicable in every Member State and leaves much less room for national legislators than the DPD did. A regulation is a more efficient tool for harmonising data protection in the EU than a directive although the GDPR leaves some margin of discretion for the Member States.[93] De Hert and Papakonstantinou have acknowledged, however, that the ultimate level of harmonisation will depend on many factors, such as how the Member States use their margin of discretion and how the consistency mechanism[94] works.[95]

Other challenges of the DPD concerned international data transfers and applicable law, effective enforcement, and coherence of data protection legal framework.[96] Due to the limited scope of this research, it is not possible to go in detail to each challenge and response, but two important aspects that have attracted much attention among different stakeholders from legal practitioners to business communities should be mentioned here. Firstly, one of the most striking aspects of the GDPR have been the severe administrative fines, which can go up to

[91] Filippone (n 2) 5.
[92] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 30.
[93] De Hert and Papakonstantinou (n 89) 182.
[94] Consistency mechanism is laid down in the GDPR under Articles 63-67. The mechanism requires all Member States' DPAs to cooperate with each other, withholds the EDPB the possibility to issue its opinion on the matter if it so decides or is requested to do so, and establishes a dispute resolution system for disputes between DPAs.
[95] De Hert and Papakonstantinou (n 89) 182.
[96] European Commission (n 88) 3-4.

20 000 000 EUR or up to 4 % of the global turnover, whichever is higher.[97] These sanctions provide a strong incentive for companies to comply with the data protection rules beyond any doubt. Another important aspect of the GDPR is the 'extraterritoriality' that has raised controversial discussion among legal scholars.[98] The scope of application of the GDPR is extended to cover also businesses that are not established in the EU but target their products or services to the data subjects in the EU or monitor their behaviour.[99]

The GDPR preserved the two main objectives of the DPD; the free flow of data and the protection of fundamental rights, especially the protection of personal data. As described above, the stronger fundamental rights aspect of the GDPR was empowered by the amendments of the Treaty of Lisbon. The protection of individuals' fundamental rights has been highlighted in an academic discussion. The objective of the free flow of data might have been a bit overshadowed in the discussion by the other objective, which should not diminish the importance of the free flow of personal data. The following chapter gives a brief introduction to how the GDPR aims to strengthen the rights and freedoms of data subjects and enhance the responsibilities of data controllers and processors.

3.2.2 Strengthening the data protection of individuals and enhancing the responsibilities of data controllers and processors

In order to pursue the objective of protection of fundamental rights, the GDPR seeks to strengthen the protection of individuals by increasing transparency of data processing and by giving more control for the individuals over their personal data.[100] The GDPR strengthened the protection of individuals primarily by specifying existing principles, rights and obligations. One of the main clarifications concerned the definition of consent. New additions to the consent requirements and demonstrative examples set out in Recital 32 shall improve the level of data

[97] GDPR Article 83 (5).
[98] The extraterritorial scope of application has been criticised as a 'paper tiger' because the EU lacks the competence to enforce the data protection rules in third countries. On the other hand, the extraterritoriality is considered necessary to prevent companies from circumventing the data protection rules by establishing outside the EU. See Dan Jerker B Svantesson, 'A Jurisprudential Justification for Extraterritoriality in (Private) International Law.' (2015) 13 Santa Clara Journal of International Law 517, 561.
[99] GDPR Article 3 (2).
[100] European Commission (n 88) 6-8.

protection.[101] The GDPR also contains a new data subject right, the right to data portability. According to the right, data subjects have the right to receive the personal data they have given to data controllers 'in a structured, commonly used and machine-readable format'.[102] Data subjects also have the right to have that personal data transmitted to another data controller if it is technically feasible.[103] In practice, this new right seeks to provide data subjects with the right to change service provider in an online environment.[104]

The specified right to erasure, the right this research focuses on, is one of the most noteworthy provisions of the GDPR although it is not a new right *per se*. The right to erasure under the GDPR is, however, more comprehensive detailing the conditions of the right, the obligation of the data controller to inform other controllers and processors of the data subject's request, and the legal grounds for derogating from the right. The right could have been even more astonishing if the Court had not surprised data protection world by stretching the right to erasure under the DPD in its famous *Google Spain* case.[105]

What comes to the obligations of data controllers and processors in the GDPR, the purpose is to enhance the responsibilities of data controllers and processors.[106] Regarding data protection principles, the GDPR introduced two new important principles concerning the obligations of controllers and processors. The principle of transparency requires data controllers and data processors to process personal data transparently. The principle of accountability requires data controllers to be able to prove that their processing of personal data complies with the GDPR provisions.[107] These new principles illustrate a transition from the old notification system of the DPD under which the data controllers were obliged to notify national DPA before the processing operations towards accountability of data controller.[108] New obligations that reflect

[101] According to the GDPR Article 4(11), the consent means 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. The GDPR added a requirement for 'unambiguous' indication and requirement for a 'statement or affirmative action'. De Hert and Papakonstantinou (n 89) 187.
[102] GDPR Article 20 (1).
[103] GDPR Article 20 (2).
[104] De Hert and Papakonstantinou (n 89) 189-190.
[105] De Hert and Papakonstantinou (n 89) 189.
[106] European Commission (n 88) 11.
[107] Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2018) 34 Computer Law and Security Review 134, 139.
[108] De Hert and Papakonstantinou (n 89) 191.

these new principles were set for data controllers.[109] According to the GDPR, data controllers are obliged to maintain records of processing activities and to cooperate with supervisory authority.[110] To increase transparency of data processing, a new obligation to notify supervisory authority and even data subject, in certain circumstances, of personal data breaches was included in the GDPR.[111]

Another important novelty is the introduction of two new principles which aim to encourage developers to consider data protection matters already in the initial stage of development. The principle of data protection by design requires data controllers to implement appropriate technical and organisational measures, which implement data protection principles, such as the principle of data minimisation, by design.[112] The data protection by default, in turn, provides measures that by default ensure that 'only personal data, which are necessary for each specific purpose of the processing are processed'.[113] The objective is to take into account the possibilities of data controllers and processors to comply with their data protection obligations already when designing applications and services.[114]

Other primarily administrative obligations worth mentioning are the obligation for data controllers established outside the EU to designate a representative in the EU[115], the obligation to designate a data protection officer (DPO) in certain cases[116], and the obligation to perform data protection impact assessment (DPIA) prior to data processing if it is likely to result in a high privacy risk[117]. The GDPR has been criticised for causing excessive administrative and financial burden, especially for small and medium-sized enterprises. To counter these challenges, the GDPR specified its provisions of codes of conducts and created a new certification mechanism to facilitate compliance with the provisions of the GDPR.[118]

[109] Tikkinen-Piri, Rohunen and Markkula (n 107) 141.
[110] GDPR Article 30 and 31.
[111] GDPR Article 33 and 34.
[112] GDPR Article 25 (1).
[113] GDPR Article 25 (2).
[114] Recital 78 of the GDPR.
[115] GDPR Article 27.
[116] GDPR Article 37-39.
[117] GDPR Article 35.
[118] De Hert and Papakonstantinou (n 89) 192-193.

To sum up, the GDPR is a tremendous set of provisions codifying already existing data protection practises and rules, but, on the other hand, it also contains several new important aspects. Dealing with all the novelties of the GDPR is, however, way beyond the scope of this research. For example, new provisions regarding international data transfers or the updated roles and functions of DPAs and the EDPB, to name a few, would deserve greater attention.[119] Certain definitions and rights that are essential with respect to blockchain technology are examined in more detail in the following chapters.

4 Relationship between blockchain technology and the GDPR

4.1 Decentralisation as the fundamental issue

The Internet was initially envisioned as a place free of central governance and where strong privacy prevailed. Nevertheless, the development has led to the opposite direction. Lower data storage costs and advanced data processing techniques have increased the power of centralised intermediaries, such as Facebook, Google, Amazon, and so forth, on the Internet.[120] Moreover, in the digital age, it is a common practice for service providers to require users to provide personal data instead of money in exchange for using their digital services. Thus, personal data is also considered to have economic value.[121] Big centralised intermediaries collect huge quantity of data of individuals to monitor and analyse individuals' online behaviour. This enables them to target their products and services more efficiently to customers and to design more personalised services for customers. However, these benefits come at the price of individuals' privacy and data protection.[122] Individuals are encouraged to share more and more personal data and to consent on profiling while the centralised intermediaries keep the underlying processing algorithms secret because disclosing those could give an advantage to competitors.[123] As Pasquale has described the situation, the individuals can be described to live in a 'black box society', where centralised intermediaries are capable to monitor and control

[119] On international data transfers see eg. Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) ch 7; On the roles of DPAs and the EDPB see eg. De Hert and Papakonstantinou (n 89) 190-91 and 193.
[120] Filippone (n 2) 4-5.
[121] Nicola Fabiano, 'Blockchain and Data Protection: The Value of Personal Data' (The 9th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC, Orlando, March 2018) 2 <www.nicfab.it/blockchain-data-protection/> accessed 24 July 2018.
[122] De Filippi (n 61) 2.
[123] De Filippi (n 61) 3.

the behaviour of individuals and to make automated decisions on them without being required to disclose how they do it.[124] This unawareness of how personal data is used and how individuals are profiled give rise to concerns regarding discrimination and stigmatisation.[125]

The strong asymmetry of power between individuals and the centralised intermediaries was recognised not only by the regulators but also by the blockchain developers. Regulatory and technological side share a common objective of giving more control for individuals over their personal data.[126] As described in more detail in Chapter 3, the regulators responded to the challenges arising from centralisation by strengthening the rights and freedoms of individuals and by enhancing the responsibilities of data controllers and processors under the GDPR. Blockchain developers adopted a different approach based on decentralisation.[127] The main idea of decentralisation is to replace centralised intermediaries with decentralised peer-to-peer networks. When there is no centralised intermediary and central point of control, the individuals are in a better position to control their data. Instead of enhancing the responsibilities of centralised operators, decentralisation aims to shift the responsibility over the data from centralised parties to the individuals.[128] Despite the common objective, this extremely different approach of blockchain developers has raised several tensions between the technology and the regulation.

The common problem between law and technology is that technology tends to move extremely fast while legislation moves rather slowly. As a result, legislation is often outdated as it cannot predict how new technologies evolve. That is the case also with blockchain technology and the GDPR. The GDPR was not drafted taking into account decentralised architectures, such as blockchains, where there is no single entity responsible for the data processing. Decentralisation is the fundamental issue behind the tensions between blockchain technology and the GDPR. Essentially, there are three main questions that should be considered to understand the problematic relationship between blockchain technology and the new data protection regulation:

[124] Frank Pasquale, *The Black Box Society : The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
[125] Filippone (n 2) 6.
[126] Filippone (n 2) 6.
[127] Filippone (n 2) 7.
[128] De Filippi (n 61) 15.

1. Does the GDPR apply to blockchain-based applications? (Question about personal data and anonymisation)
2. Who can be a data controller or processor in a traditional blockchain network? (Question about the allocation of responsibilities)
3. What kind of issues the blockchain technology raises in relation to data subjects' rights and compliance with the obligations of the GDPR? (Question about complying with data subjects' rights)

Here, it should be mentioned that the right to erasure is not the only controversial aspect of blockchain technology with regard to compliance with data subjects' rights (Question 3). Therefore, even if the conflict with the right to erasure and immutability could be reconciled, there could still be other issues concerning, for instance, the principle of data minimisation, the principle of storage limitation, or to the right to access would require further attention.[129] However, the scope of this research is not enough to delve into the other issues in more detail. Questions 1 and 2, instead, are essential preliminary questions that need to be considered before assessing the right to erasure and the immutability. Before going in detail into the three questions, it is worth examining the claims according to which the blockchain technology could be used to enhance the privacy and data protection of individuals.

4.2 Blockchain as a tool for enhancing individuals' privacy and data protection

Lack of centralised intermediaries

Despite the several points of tension between blockchain and the GDPR, blockchain has also been regarded as a or tool for enhancing individuals' privacy and data protection. Decentralisation represents the most apparent way in which blockchain pursues to achieve the objective of giving individuals more control over their personal data. Lack of centralised party that is responsible for data collection and processing reflects a shift of control from centralised intermediaries to individuals.[130] Blockchain technology could enable new access authentication systems that give individuals more control over how they store, manage, and use their personal data. The EU has noticed this great potential of blockchain technology to achieve the objectives of the GDPR by alternative means.[131] DECODE is a project funded by the EU that aims to

[129] More on other controversial aspects of blockchain technology in regard to the GDPR see eg Finck (n 13) 20-23.
[130] De Filippi (n 61) 15.
[131] Finck (n 13) 29.

develop and pilot blockchain-based tools that allow individuals to have true control over their personal data.[132] Many other ongoing projects seem to affirm that blockchain technology has potential to strengthen individuals' data sovereignty, so that individuals may independently decide when and how their personal data is processed.[133] As such, the blockchain technology could promote individuals' privacy and data protection by giving more control to the individuals over their personal data.

Decentralisation is also a useful tool for combatting data breaches. Data breaches have become an increasing problem in the digital age because a single vulnerability of application or software can lead to a data breach exposing millions of users' personal data, including home addresses, fingerprint data, or even credential data.[134] As a result of a data breach, data subject might lose availability to the data permanently, which constitutes a serious threat to individuals' data protection.[135] Decentralised data storage and consensus mechanism combined with the immutable ledger provides high security against data breaches. For example, in Bitcoin blockchain, a successful attack would require that the attacker has more mining capacity than the rest of the network, which would be extraordinarily energy-consuming and require enormous computational resources.[136] Even though traditional blockchains are not genuinely immutable as, for instance, the decentralized autonomous organisation (DAO) hack proved[137], one of the most attractive features of blockchain is the effectiveness in preventing data breaches.

[132] More on DECODE project see the project website <https://decodeproject.eu/> accessed 19 August 2018.
[133] For instance, Neisse, Steri and Nai-Fovino have presented in their research three blockchain-based data accountability and provenance tracking models, which enable data subjects to track controllers and processors they have given access to the data and withdraw the consent and disable access to their data anytime. These solutions are considered in more detail in Chapter 5.2.2 because they could be interesting in relation to complying with the right to erasure. Ricardo Neisse, Gary Steri and Igor Nai-Fovino, 'A Blockchain-Based Approach for Data Accountability and Provenance Tracking' in *Proceedings of the 12th International Conference on Availability, Reliability and Security* (Association for Computing Machinery, 2017) <http://arxiv.org/abs/1706.04507> accessed 4 September 2018.
[134] Taylor Armerding, 'The 17 biggest data breaches of the 21st century' (*CSO*, January 26 2018) <www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html> accessed 30 July 2018.
[135] Filippone (n 2) 29.
[136] Greenspan, 'The Blockchain Immutability Myth' (n 49).
[137] The DAO was a decentralised venture capital fund in which investors had, at least in theory, more power as there was no centralised board of directors or equivalent management structure. In the DAO hack, the attacker found a loophole in the code of a smart contract that was built on the Ethereum platform, which allowed the attacker to withdraw 3.6 million ether from the DAO. The attack was noticed by the Ethereum community, but as updating the code would require at least 51 percent of the nodes to support it, it took time and persuasion by community leaders for the majority to agree with the update. As a result of the hack, the Ethereum was split to Ethereum (supported by majority of the nodes) and to Ethereum Classic (supported by the minority disagreeing with the update). Greenspan, 'The Blockchain Immutability Myth' (n 49).

Transparency

Another promising feature of blockchain technology concerning data protection and privacy is transparency. Transparency is an inherent feature of blockchain technology.[138] Transactions in the ledger are publicly available for anyone in the world, even though the identity of individuals behind the transactions are concealed with public keys. Transparency of transactions is essential in traditional blockchains necause it enables validators to verify transactions without a centralised intermediary.[139] However, transparency in traditional blockchains is not limited to publicity of transactions.

On traditional blockchains, transparency also covers the protocol level since traditional blockchain projects are often open source. Even if the source code would not be publicly available, the operations of the code (bytecode) are open for any node in the network to execute and validate. Transparency at the protocol level enables individuals to be better informed what data is collected of them and how the data is processed in contrast to more opaque data processing operations in centralised data systems.[140] While this transparency has been criticised for the fact that most of the individuals cannot truly understand the code and evaluate its modifications, this transparency gives at least the possibility for individuals to be well-informed of the data processing operations and improves individuals' possibilities to exercise their rights as data subjects.[141]

The principle of transparency is one of the new principles introduced in the GDPR. The principle requires that personal is processed transparently.[142] One of the purposes of this principle is to enable data subjects to make better use of their rights.[143] The inherent transparency of traditional blockchains seems prima facie to be in line with the principle of transparency. According to Recital 39 of the GDPR, '(i)t should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.' Despite that blockchain technology seems to be providing transparency to individuals in a manner which the GDPR

[138] De Filippi (n 61) 8.
[139] De Filippi (n 61) 11.
[140] De Filippi (n 61) 8.
[141] Article 29 Data Protection Working Party, 'Guidelines on Transparency Under Regulation 2016/679' (2016) WP260 6; Filippone (n 2) 33.
[142] GDPR Article 5(1)(a).
[143] Article 29 Data Protection Working Party, 'Guidelines on Transparency Under Regulation 2016/679' (n 141) 6.

requires, blockchain technology comes with a more obscure risk for individuals' privacy and data protection. Blockchain-based applications are generally designed so that there is always some metadata relating to the transactions publicly available on the blockchain network.[144] Even though pseudonymisation techniques can hide the identity of the user, there are several methods to indirectly identify individuals from the metadata. This forms a high risk for individuals' privacy as every transaction is publicly available on the ledger and can be possibly linked to a specific individual if additional information to link the metadata to the individual can be acquired.[145] As will be discussed in Chapter 4.3, transparency runs a risk of being rather a privacy issue than a privacy-enhancing feature.

Encryption and pseudonymisation

Blockchain technology uses encryption and pseudonymisation to provide better privacy and data protection for its users. As well described in the Article 29 Working Party's guidelines on the anonymisation techniques, '(p)seudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation'.[146] Pseudonymisation is reaffirmed in the GDPR as a technique that 'can reduce the risks to the data subjects concerned and help controllers to meet their data-protection obligations'.[147]

In traditional blockchains two most commonly used pseudonymisation techniques to obscure the content of the data stored on blockchain are encryption and hashing. Encryption can obstruct the content of the data so that the data can only be decrypted by using a unique private key.[148] Moreover, the public-key encryption is used to hide the identities of individuals transacting with each other. Hashing, on the other hand, is a technique that transforms any size of data to unreadable and fixed size form (hash value), which cannot be reversed back to the original form.[149] As will be discussed in more detail in the following Chapter, encrypted or hashed data may be considered as pseudonymised data and qualify as personal data under the GDPR. It

[144] De Filippi (n 61) 10.
[145] Filippone (n 2) 30.
[146] Article 29 Data Protection Working Party 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP 216 20.
[147] Recital 28 of the GDPR.
[148] Finck (n 13) 4.
[149] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 20.

seems that the state-of-art techniques do not exempt blockchain technologies from the scope of the GDPR but can give some leeway for processing operations.[150]

Pseudonymisation and encryption are mentioned in Article 32 of the GDPR as examples of the appropriate technical and organisational measures for data controllers and processors in ensuring the security of data processing. Encryption, although not mandatory under the GDPR, is mentioned in several parts of the GDPR as an essential data protection measure that could be used to mitigate the risks of data processing activities.[151] Pseudonymisation, in turn, is explicitly mentioned in Article 25 as an appropriate technical and organisational measure that is in line with the obligation of data protection by design. Both are thus useful techniques for reducing the risks related to data processing and facilitating compliance with the provisions of the GDPR. While encryption and pseudonymisation are not unique features of blockchains, they are an essential part of blockchains for achieving compliance with the GDPR. The next Chapter goes on to consider in more detail the encryption and pseudonymisation because they have not only been regarded as important privacy enhancing techniques but also as relevant factors in determining whether the GDPR applies to the traditional blockchains at all or not.

4.3 Personal data and traditional blockchains

4.3.1 The notion of personal data under the GDPR

A layperson might associate personal data only with information that is particularly revealing, such as health records, political opinions, or information on a person's sexual life. All aforementioned particularly revealing and sensitive data constitute personal data, and, in fact, they are mentioned in the GDPR as special categories of personal data, which enjoy an even a higher level of protection than more 'common' personal data.[152] The threshold for personal data under the GDPR may come as a surprise not only for laypersons but also for many stakeholders in data-driven economies. As regards to the blockchain technology, the GDPR seems to have caught blockchain developers off guard. The developers may have misbelieved that blockchain

[150] Ibáñez, O'Hara and Simperl (n 8) 4.
[151] 'GDPR encryption: what you should know and what you do not know' (*I-scoop*) <www.i-scoop.eu/gdpr-encryption/> accessed 31 July 2018.
[152] De Hert and Papakonstantinou (n 89) 183.

projects are exempted from the provisions of the GDPR due to the 'anonymity' of blockchain technologies.[153] Data processed on traditional blockchains is data which has undergone pseudonymisation rather than anonymised data and, in many cases, considered as personal data.

The definition in Article 4(1) and in Recital 26

Personal data is defined in Article 4(1) of the GDPR as 'any information relating to an identified or identifiable natural person'. An identifiable natural person is an essential term when assessing whether the GDPR applies or not. According to Article 4(1), 'identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[154] The GDPR does not require actual identification of the individual as indirect *identifiability* is considered enough for data to constitute personal data.[155] The identifiability forms thus the threshold for what constitutes personal data.[156]

The definition contains a list of attributes that can identify a person directly or indirectly. Direct identifiers, such as name or identification number, can on its own identify a natural person whereas indirect identifiers, such as postal address, phone number or different online identifiers, can identify a natural person only if additional information is provided.[157] Article 29 Working Party has emphasised that besides acquiring name and address, which are the most common attributes used to identify a natural person, there are also other means of identification, including singling out, linkability, and inference.[158] For instance, web traffic surveillance tools and online identifiers, such as IP addresses or cookies, which are explicitly mentioned in Recital

[153] Ibáñez, O'Hara and Simperl (n 8) 7.
[154] GDPR Article 4(1)
[155] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 90.
[156] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) WP 136 12.
[157] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 89.
[158] Other means of identification are defined as follow in the opinion: '*Singling out*, which corresponds to the possibility to isolate some or all records which identify an individual in the dataset; *Linkability*, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (eg. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability; *Inference*, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.' Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP 216 11-12.

30 as attributes that may leave traces that enable to identify individuals on the basis of their online behaviour and habits, can single out individuals without enquiring name or address.[159] Identification thus covers broadly all possible ways to distinguish an individual from other persons.[160]

Particular attention should be paid to the notion of identifiability because it sets the threshold for personal data. If data is not or no longer capable of identifying a natural person, it is considered as anonymised data and out of the scope of the GDPR. In assessing whether the data is capable of identifying a data subject, *all means reasonably likely to be used* by the data controller or by another person to directly or indirectly identify the data subject should be taken into account.[161] The criterion of the means reasonably likely to be used is further clarified in Recital 26, '(t)o ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'

The notion of identifiability requires to assess what is considered as a reasonable effort to link the data to a natural person. There has been a legal debate between two approaches. According to an absolute approach, all possibilities of a data controller to identify a natural person should be taken into account regardless of the likelihood of identification. It is not required that a data controller should be able to link data to a natural person, but it is enough that someone in the world holds the additional information necessary to identify the natural person. On the contrary, a relative approach considers the necessary effort to identify. Thus, a purely theoretical risk of re-identification is not covered by the definition of personal data.[162] The legal scholars have not been unanimous about which approach the GDPR represents. The GDPR can be interpreted to support both approaches, which complicates the assessment of the notion of identifiability.[163]

---

[159] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 156) 14.
[160] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 89.
[161] Recital 26 of the GDPR.
[162] Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 163, 165-66 <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jipitec7&id=169&men_tab=srchresults> accessed 20 September 2018.
[163] On the one hand, the fact that Recital 26 considers not only the possibilities of data controller to identify a natural person from the data but also the same possibility of *another person* (anyone in the world) could support absolute approach as all the necessary information to identify a natural person does not have to be in the hands of

However, some guidance can be found from the case law of the Court and the Opinion of Article 29 Working Party as discussed below.

In *Breyer v. Bundesrepublik Deutschland,* the Court clarified the notion of indirect identifiability and the criterion of means reasonably likely to be used.[164] The case concerned dynamic IP addresses, which are assigned by Internet Service Providers (ISP) to customers and which change every time a customer connects to the internet. Mr Breyer contested practice of German federal institutions to store dynamic IP addresses of persons accessing websites run by the federal institutions. The additional information required to identify individuals accessing the websites was held by a separate ISP.[165]

The Court ruled that identifiability does not require that all information should be in the hands of one person. It considered that dynamic IP addresses could constitute personal data if the website provider 'has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person'.[166] The Court ruled that there were legal means to access the additional information. The national law did not directly allow to transmit the additional data, but in the event of a cyber attack, the website provider could turn to authorities to get access to the additional data in order to initiate criminal proceedings.[167] In addition to the legal means test, the Court referred to the complexity of identification as a relevant factor in determining the level of identifiability. The Court considered that dynamic IP addresses do not constitute personal data if identification is 'practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.'[168]

---

the data controller. Recital 26 makes also a specific reference to singling out as a mean of direct or indirect identification, which could be harmful to a natural person even if it is unlikely that the data can be linked to data subject's name. Further, the Recital 26 states that data which have undergone pseudonymisation should be considered identifiable information that could imply that such data is always personal data regardless of the criterion of means reasonably likely to be used. On the other hand, the GDPR contains also many strong hints of the relative approach, especially the use of the criterion means *reasonably* likely to be used and the list of objective factors. Spindler and Schmechel (n 164) 165-66; Miranda Mourby and others, 'Are "Pseudonymised" Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK' (2018) 34 Computer Law & Security Review 222, 227.

[164] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779.

[165] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 91-92.

[166] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779, para 49.

[167] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779, para 47.

[168] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779, para 46.

The assessment of the legal means test and the complexity of the identification should be carried out on a case-by-case basis.[169] The approach the Court has taken could be seen as a 'balanced approach' because it accepts that third parties hold the additional data, but only if a data controller has legal means to access it. This approach seems to balance the burden on data controllers and the protection of data subjects.[170]

Anonymisation and pseudonymisation

Anonymisation and pseudonymisation are essential terms in understanding the scope of application of the GDPR. As regards what constitutes anonymised data, the GDPR refers to the notion of identifiability. The idea that anonymised data escapes the scope of the GDPR is described in Recital 26 as follows, '(t)he principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.' The GDPR does not give an explicit definition of anonymised data, but some guidance can be found on the opinion issued by Article 29 Working Party on the anonymisation techniques in 2014.[171] Even though the opinion was given in relation to the DPD, it still provides relevant guidance for the GDRP.

The opinion requires that the identification must be prevented *irreversibly*. Thus, the opinion sets out very high standard for identification.[172] This near-zero risk standard has been regarded to be practically unachievable in the digital age.[173] While the opinion acknowledges the potential of anonymisation techniques, it is criticised for failing to provide clear guidance on the risk of re-identification, in other words, what would be an acceptable risk of re-identification to render data anonymous.[174] For instance, Stalla-Bourdillon and Knight have argued that the zero-risk is not attainable in the era of big data and that robust anonymisation techniques could

[169] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 92.
[170] Cagla Salmensuu, 'General Data Protection Regulation and the Blockchains' (2018) 1 Liikejuridiikka 92, 106.
[171] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 156).
[172] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 156) 6.
[173] Khaled El Emam and Cecilia Álvarez, 'A Critical Appraisal of the Article 29 Working Party Opinion 05 / 2014 on Data Anonymization Techniques' (2014) 5 International Data Privacy Law 73, 75.
[174] El Emam and Álvarez (n 173) 74.

provide adequate protection for data subjects even if the risk would be higher than near-zero.[175] In the same vein, El Emam and Álvarez have considered that the acceptable level of re-identification should not be a practically unachievable zero-risk requirement, but more suitable description would be 'a very small risk of re-identification'.[176] Many legal scholars seem to agree that there is a need for a more flexible approach that considers the necessary effort to identify a natural person.

Pseudonymisation has a twofold meaning in the GDPR. As discussed in Chapter 4.2, the pseudonymisation is an important privacy-enhancing technique, which is not necessarily compulsory but is a convenient way for data controllers to demonstrate compliance with the GDPR.[177] Pseudonymisation is a process to disguise individuals' identities by replacing certain attributes, such as name, e-mail address, or sex in the dataset with a pseudonym.[178] Pseudonymisation is defined in the GDPR as 'processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.[179] In practice, pseudonymisation requires that the keys to decrypt the data are kept separate from the data by using different databases for the data and the keys, and by organisational measures by recording and limiting the persons who have access to both the keys and the data.[180]

On the other hand, pseudonymisation has also been considered as a relevant factor in determining what constitutes personal data. According to Recital 26, '(p)ersonal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural

[175] Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Jouurnal 284, 307.
[176] El Emam and Álvarez (n 173) 76.
[177] Laura Tarhonen, 'Pseudonymisation of Personal Data According to the General Data Protection Regulation' in Päivi Korpisaari (ed), *Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2016* (University of Helsinki 2016) 10, 30.
[178] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 94.
[179] GDPR Article 4(5).
[180] Tarhonen (n 177) 19.

person'.[181] This could be interpreted to mean that data which have undergone pseudonymisation always constitute personal data. Article 29 Working Party has acknowledged that pseudonymisation does not suffice to render data anonymised, even though pseudonymisation can reduce the linkability of a dataset with the original identity of an individual.[182] This interpretation would undermine the notion of identifiability and the criterion of means reasonably likely to be used to identify. What comes to encryption techniques, this interpretation would mean that encrypted data could never be anonymised because encryption constitutes a pseudonymisation technique under the GDPR.[183] Before the GDPR was finally approved, the United Kingdom's Information Commissioner's Office (ICO) warned that pseudonymisation should not be linked to the definition of personal data by including it in Recital 26 because that would cause legal uncertainty about the definition of personal data.[184]

Even though there have been different opinions whether pseudonymisation could render data anonymous or not, the opinion that data which have undergone pseudonymisation could be anonymised seem to prevail.[185] De Hert and Papakonstantinou have argued that despite the connection between pseudonymisation and the definition of personal data, it should be possible to render data which has undergone pseudonymisation anonymous because such data is considered as 'information on an identifiable natural person' and subject to the criterion of means reasonably likely to be used to identify a natural person.[186] All in all, there seem to be legal uncertainties about the definition of personal data. The *Breyer* case provided some guidance for the notion of identifiability, but still, the question about anonymisation and the acceptable risk of re-identification remains uncertain. Linking the pseudonymisation to Recital 26 and the definition of personal data further complicates the matter.

[181] In contrast to the Council proposal of the GDPR, the final version of the GDPR does not contain the term pseudonymised data.
[182] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 20.
[183] Mourby and others (n 163) 226-27.
[184] Information Commissioner's Office, 'ICO Analysis of the Council of the European Union Text of the General Data Protection Regulation' (*ICO Blog*, 26 August 2015) 2 <https://ico.org.uk/media/1432420/ico-analysis-of-the-council-of-the-european-union-text.pdf> accessed 20 September 2018 .
[185] See eg Mourby and others (n 163) 226.
[186] De Hert and Papakonstantinou (n 89) 183.

4.3.2 Personal data on blockchains

In considering whether blockchain-based applications process personal data, it must be acknowledged that there are different use cases of blockchain technologies some of which may process personal data while others do not. Salmon and Maxwell have illustrated this by dividing blockchain projects into three categories depending on the use of personal data. The first category covers blockchain projects that process data that is not directly or indirectly related to any individual, *i.e.*, anonymised data. Blockchains could be used for example to store bills of lading or diamond certificates.[187] Here, it should be noted that the GDPR does not protect legal persons, so contact details or even trade secrets of companies could be stored on a blockchain without triggering the GDPR.[188] The other two categories cover blockchain projects that process personal data but to a varying degree. Blockchains could be designed to especially process personal data and even sensitive personal information. On the other hand, some blockchains may process any type of data, which may also contain personal data.[189] For instance, Bitcoin allows writing any information in a separate field of the transaction.[190] The last two categories are in the focus of this research because they could trigger the application of the GDPR.

The broad definition of 'processing' catches different operations performed on personal data including collection, storage, alteration, dissemination, and so forth.[191] As storing is considered processing, all data stored on blockchains are processed.[192] A noteworthy exception to the processing of personal data is that the GDPR does not apply to the processing of personal data that is done 'in the course of purely personal or household activity'.[193] Thus, the regulation requires at least some connection to a professional or commercial activity.[194] The Court has interpreted the household exemption narrowly in the *Bodil Lindqvist* case ruling out the applicability of the household exemption in situations where the data is published on the

[187] Salmon and Maxwell (n 7) 21.
[188] Recital 14 of the GDPR.
[189] Salmon and Maxwell (n 7) 21.
[190] Natalie Eichler and others, 'Blockchain, Data Protection, and the GDPR'(Blockchain Bundesverband, 25 May 2018) 6 <www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf> accessed 17 August 2018.
[191] GDPR Article 4(2).
[192] Ibáñez, Hara and Simperl (n 8) 6.
[193] GDPR Article 2(2)(c).
[194] Recital 18 of the GDPR.

Internet and made accessible to an indefinite number of people.[195] Considering that traditional blockchain applications require certain metadata to be publicly available on the Internet, the household exemption seems not applicable for such blockchains. Further, many use cases seem to involve commercial activities because they are related to different types of commercial transactions.

The data on blockchains can be categorised in two sets of data possibly qualifying as 'information relating to an identified or identifiable natural person', in other words, as personal data.[196] Many blockchain-based applications process transactions between pseudonymous individuals. Transactions may be transfers of cryptocurrencies or, in case of smart contracts, executions of smart contract functions.[197] **Transactional data** refers to a data relating to the content of the transactions, for instance., financial or medical information or information related to digital identities. Transactional data often contains information relating directly or indirectly to individuals.[198] **Metadata** is another category of data processed on blockchains that runs the risk of constituting as personal data. In the context of blockchain, metadata relates to transactions carried out on a blockchain network, for instance, information on who are the sender and receiver of the transaction. In the following paragraphs, these two categories are analysed separately to understand whether they constitute personal data under the GDPR.

Transactional data can be stored in a blockchain in three forms. Firstly, transactional data can be stored in plain text in a blockchain. That is not an efficient way of storing transactional data in a blockchain because storing data in plain text requires a lot of storage capacity. It is not advisable from the data protection perspective either because storing transactional data that contains personal data in plain text to a blockchain constitutes obviously personal data.[199]

Secondly, data can be stored in a blockchain in encrypted form. Traditional blockchains rely on the public-key encryption. Encryption allows storing transactional data in a blockchain so that only the person holding the private key can decrypt the data. Article 29 Working Party has considered in its opinion that encryption of data can provide a high degree of security because

[195] Case C-101/01 *Criminal proceedings against Bodil Lindqvist* EU:C:2003:596, para 47.
[196] Finck (n 13) 10.
[197] Neisse, Steri and Nai-Fovino (n 133) 2.
[198] Finck (n 13) 10.
[199] Finck (n 13) 10.

it renders the data unintelligible for persons that do not have access to the decryption key. However, it has concluded in the same opinion that encryption does not eliminate the possibility to identify a natural person as long as the private key or original data are available (even if held by trusted key escrow service).[200] Furthermore, a brute force attack[201] could be used to decrypt the data.[202] However, it could be contested whether a brute force attack would qualify as means reasonably likely to be used to identify an individual.[203] Article 29 Working Party has considered that encryption cannot irreversibly prevent identification, and, thus, it is rather a pseudonymisation than anonymisation technique.[204] Due to the high threshold for anonymisation, many legal scholars have considered that storing transactional data in a blockchain in encrypted form is likely to constitute personal data under the GDPR.[205]

Lastly, transactional data can be hashed to a blockchain. Hashing data on a blockchain allows subsequent validation of the data by comparing it to the hash. For instance, hashed data could be used in timestamping services to prove that specific document existed at a particular time.[206] Hashed data provide stronger privacy than encryption because hashed data cannot be reverse-engineered.[207] A hash function is, however, also considered as a pseudonymisation technique by the Article 29 Working Party because the hashed data and the original data can be linked together by hashing the original data again (will result in same hash).[208] Therefore, blockchain-based applications should pay attention to storing the original data because if it is leaked or otherwise acquired by third parties, it is rather easy to link transactions to that data by reviewing transaction history.[209] Some legal scholars have considered that the high threshold for anonymisation is likely to trigger the application of the GDPR even if personal data is hashed to a blockchain.[210]

[200] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 29.
[201] Brute force attack consists of adversary systematically trying all possible inputs to find out the right decryption key.
[202] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 29.
[203] For instance, state-of-art brute force attacks against Bitcoin or Ethereum public keys could be beyond the means reasonably likely to be used considering the costs and available technology. See n 392.
[204] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 29.
[205] Salmon and Maxwell (n 7) 7; Finck (n 13) 10.
[206] Finck (n 13) 5; Eichler and others (n 190) 4.
[207] Finck (n 13) 11.
[208] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 29.
[209] Ibáñez, O'Hara and Simperl (n 8) 5.
[210] Salmon and Maxwell (n 7) 11; Finck (n 13) 11.

It seems that on traditional blockchains transactional data cannot be fully anonymised because, if the data is truly anonymised, nodes could not verify transactions.[211] Nevertheless, some legal scholars have considered that even encrypted or hashed data could constitute anonymised data if there are no means reasonably likely to be used to identify a natural person. Particular emphasis should be put on who controls the information necessary to identify an individual. If such information is only held by the user (data subject), it could be argued that encrypted or hashed data is personal data only to the user and anonymised data for everyone else.[212] However, another problem arises in relation to encrypted data. Recital 26 of the GDPR requires to take account of the development of technology when assessing the means reasonably likely to be used to identify. The Article 29 Working Party has clarified that future technological advancements should be considered for 'the period for which the data will be processed'.[213] In the context of blockchain, data is often processed for an unlimited period of time. Thus, technological developments such as quantum computers, which could break even high-level state-of-art encryption, should be considered when assessing the criterion of means reasonably likely to be used to identify a natural person. This could imply that storing personal data in encrypted form in a blockchain could not constitute anonymised data if the data is stored for an unlimited period. On the other hand, blockchain developers are already developing solutions for quantum computers.[214]

Another set of data stored in blockchains that may qualify as personal data is metadata. Transparency of metadata is an inherent feature of traditional blockchains. Certain metadata must be publicly available on the blockchain to enable validators to verify transactions. In other words, the transparency of metadata is a necessity on blockchain networks to coordinate the behaviour of unrelated individuals and create trust between the individuals without centralised intermediaries.[215] Blockchain technologies rely on the public-key encryption to mitigate the apparent privacy issues stemming from such transparency. Public keys are essential elements of the metadata that is used for validating transactions.[216]

[211] Salmensuu (n 172) 112.
[212] Ibáñez, O'Hara and Simperl (n 8) 5-6.
[213] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (n 156) 15.
[214] Ibáñez, O'Hara and Simperl (n 8) 12.
[215] De Filippi (n 61) 11.
[216] Finck (n 13) 14.

The public keys are used on blockchains to enable pseudonymous identification for transactional purposes.[217] Even though users' real-world identities are disguised with pseudonyms, blockchains cannot provide transactional privacy. Every public key is linked to a published transaction, and values of all transactions and balances of every public key are publicly available on a blockchain for anyone to observe.[218] Due to the pseudonymous nature of the public keys, they cannot directly identify a natural person. However, public keys may indirectly identify a natural person if additional information can be attained and combined with the public key.[219] Here, the notion of identifiability and the criterion of means reasonably likely to be used are relevant in considering whether the public keys are considered as personal data. As explained above, the Court clarified the notion of indirect identifiability in the *Breyer* case. Applying the ruling on the case of public keys, public keys can be considered as personal data if a data controller holding the public key has legal means (not prohibited by the law) to acquire additional information to identify the individual, and such means are not too complicated, *i.e.*, in reality, the risk of re-identification is not insignificant considering the necessary effort in time, cost and manpower to identify the individual.[220]

There are various means for acquiring additional information that could identify a natural person when combined with the person's public key. Anyone transacting with a user, be it e-commerce website, cryptocurrency exchange or just a friend, will get to know at least one of the user's public keys.[221] It has become more and more common to use different service providers, such as online wallets or cryptocurrency exchanges, which collect information that enables to link public keys to users' real-world identities. These service providers may be obliged to collect the additional information in order to comply with Know Your Customer and Anti Money Laundering obligations.[222] Some users even publish their cryptocurrency addresses voluntarily online to receive donations, which may link their address to their real-world identity.[223] In addition to the different forms of collection and voluntary disclosures of additional information, various data analysis techniques have been developed to deanonymize especially cryptocurrency transactions. Researchers have found out for example that Bitcoin addresses could be linked to the users' IP addresses, which in turn could be linked to the users'

[217] Finck (n 13) 12.
[218] Zheng and others (n 45) 562.
[219] Salmon and Maxwell (n 7) 7.
[220] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* EU:C:2016:779, para 46.
[221] Arvind Narayanan and others, *Bitcoin and Cryptocurrency Technologies*, (Draft version, Princeton University Press 2016) 175 <https://lopp.net/pdf/princeton_bitcoin_book.pdf> accessed 20 September 2018.
[222] Ibáñez, O'Hara and Simperl (n 8) 7.
[223] Narayanan (n 221) 175.

real identities.[224] Law enforcement agencies have already proved that they can identify individuals behind Bitcoin transactions.[225]

Here, the criterion of means reasonably likely to be used to identify becomes crucial again. Ibáñez, O'Hara and Simperl have underlined that attention should be paid to who holds the additional information necessary to identify the individual from public keys.[226] Finck has considered that the *Breyer* case affirms the interpretation that public keys qualify as personal data because all the data necessary to identify a natural person does not have to be in the hands of one person, but instead it suffices that information exchanges or other service providers hold the additional information.[227] Ibáñez, O'Hara and Simperl have taken a more flexible approach by arguing that if the users themselves generate and manage their public and private keys as initially envisioned for traditional blockchains, the public keys will not constitute personal data. Nonetheless, a common practice is that users rely on centralised third parties for key management. These wallet services collect information that enables to link the public key to a natural person. If a situation similar to *Breyer* case arises, additional information to identify an individual from the public key could be acquired from the wallet service provider by legal means, which are not too complicated.[228] In other words, when users rely on key management services or other service providers, which collect information to link their public keys to their real-world identities, there may be means reasonably likely to be used to identify a natural person from the public key.

In addition to the above-described possibility to identify a natural person from the public keys, the public availability of metadata and transaction history may cause another risk of re-identification. It is possible that public keys could single out a natural person if they are combined with other information, such as e-mail addresses, credit card data or IP addresses. This other information could be accessed from service providers that enable customers to pay with cryptocurrencies.[229] While there is not necessarily legal means for anyone who access the public key from the publicly available transaction history to acquire additional information from

[224] Alex Biryukov, Dmitry Khovratovich and Ivan Pustogarov, 'Deanonymisation of Clients in Bitcoin P2P Network' (Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery 2014) 15 <http://arxiv.org/abs/1405.7418> accessed 19 August 2018.
[225] Finck (n 13) 13.
[226] Ibáñez, O'Hara and Simperl (n 8) 6.
[227] Finck (n 13) 13-14.
[228] Ibáñez, O'Hara and Simperl (n 8) 6.
[229] Salmensuu (n 172) 109.

the service providers, the public key could be personal data for the service providers because they have access to both the public key and the other information necessary to identify a natural person. Data analysis techniques could help these service providers to associate users' public keys and to single out individuals by combining public keys with other available information.[230] Even if there would be legal means to identify, it should be further assessed whether using these techniques to single out a natural person would be regarded as means reasonably likely to be used to identify a natural person, considering the necessary effort in time and cost.

4.3.3 Technological solutions for better protection of individuals privacy and data protection

Many traditional blockchain applications process personal data and must comply with the provisions of the GDPR as discussed above. Several technological solutions have been proposed to provide more privacy for individuals transacting on blockchain networks. So far, most of the solutions have focused on improving users' privacy, whereas the issues concerning data protection have received attention only recently.[231] Nevertheless, these solutions are not only interesting from the privacy perspective but also from the perspective of data protection. Some of the solutions could help to comply with the obligations of the GDPR and some possibly render data anonymous.

The transparency of transactions and metadata is a problem on the most basic level of blockchain, *i.e.*, on the protocol or the consensus layer, which does not prevent technologists from developing more advanced encryption and obfuscation methods on top of that layer.[232] Many blockchain applications already rely on hashing and encryption techniques to mitigate issues arising from the transparency. In that regard, the interesting question is whether advanced encryption methods could qualify as anonymisation techniques in the future. At the moment, there is legal uncertainty of the actual threshold of anonymisation. However, the requirement that identification should be irreversibly prevented sets a considerably high standard for anonymisation. There is clearly a need for legal certainty as what could be considered as an acceptable risk of re-identification.[233]

[230] Salmensuu (n 172) 110.
[231] Ibáñez, O'Hara and Simperl (n 8) 7.
[232] De Filippi (n 61) 13.
[233] Ibáñez, O'Hara and Simperl (n 8) 13.

Some of the most discussed and exciting solutions are presented briefly below to give a glimpse of the proposed technological solutions; some of them can help to comply with the GDPR, others provide more privacy for users by obscuring the receiver or the sender of the transaction or the amount sent. Cryptocurrencies are the most advanced use case of blockchain technology, and so many of the leading solutions providing more anonymity in blockchain transactions have been proposed regarding cryptocurrencies.

Name of the solution	Description
Hashing-out	Storing transactional data on encrypted external off-chain storage controlled by a third party while only hashes of that data are stored on the actual blockchain. It has been described as one of the most prominent solutions because it is rather easy to deploy and greatly help to meet with obligations of the GDPR. However, it has been criticised for 'betraying the principle of decentralization' as it requires a centralised third party for controlling the off-chain storage.[234]
Stealth address	Monero has presented a solution for hiding the destination of the transactions in a way that only the sender and receiver may know in which address the payment was sent to. Stealth addresses could be used for example by a website that wants to receive donations without making these donations publicly available on the blockchain.[235]
Mixing technologies	Mixing technologies make it more difficult to use deanonymisation techniques to link different addresses users' use to send and receive transactions. Decentralised peer-to-peer mixing projects, such as CoinJoin or CoinShuffle, gather together several users to make a single transaction and so hide the direction of transaction movement.[236]
Merge avoidance	Merge avoidance can solve a problem that mixing services cannot, *i.e.*, the problem of linking user's accounts together whenever a user spends from the accounts at the same time. While it is an interesting solution for that purpose, the privacy it can provide has been criticised 'highly porous and heuristic, with nothing even close to approaching high guarantees'.[237]
Ring signatures	The main idea behind ring signatures is to protect the identity of the sender by gathering together a group or 'ring' of individuals which each own a private key that can produce a digital signature for the transaction. This makes it much more difficult to determine which of the group member's private key initiated the transaction but still enables validators to validate the transaction.[238]
Zero-knowledge proofs	A zero-knowledge proof is a cryptographic technique implementing a form of homomorphic encryption. A zero-knowledge proof is a method by which an individual may prove to another individual that she knows a value x without disclosing any other information except the fact that she knows the value x. In the context of blockchain, it enables users to transact with each other without disclosing the sender, the receiver or the transaction value to the validators. A zero-

[234] Finck (n 13) 11-12; Ibáñez, O'Hara and Simperl (n 8) 8.
[235] Monero, 'Stealth Address' (*Monero*) <https://getmonero.org/resources/moneropedia/stealthaddress.html> accessed 14 August 2018.
[236] Narayanan (n 221) 182.
[237] Vitalik Buterin, 'Privacy on the Blockchain - Ethereum Blog' (*Ethereum blog*, 15 January 2016) <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/> accessed 14 August 2018.
[238] Monero,'Ring Signature' (*Monero*) <https://getmonero.org/resources/moneropedia/ringsignatures.html> accessed 14 August 2018.

	knowledge proof is a promising technique for different blockchain use cases, and it has been already deployed successfully, *e.g.,* in Z-Cash cryptocurrency.[239]
Secure Multi-Party Computation	Secure Multi-Party Computation (SMPC) allows to compute over encrypted data and to hide the content of the transactions from both the public and the validators while maintaining the possibility to validate the computations. In SMPC two or more users can collaborate to process even sensitive personal data. Each user's input is divided into shares, which are distributed randomly to other participants. The users can see only their own result of the computation and receive only meaningless shares of other participants inputs. [240]
Confidential transactions	Elements Project has developed a solution for keeping the actual amounts transacted visible only to the individuals of the transaction while allowing validators to validate the transactions.[241]

Table of different technological solutions providing more privacy for individuals making transactions in blockchain network.

The table briefly describes some of the most discussed technological solutions picked up by legal scholars researching the issues of blockchain technology in relation to data protection. More detailed analysis of the technological solutions goes far beyond the scope of this research. Both legal and technological community seem to agree that different combinations of the above-mentioned techniques could improve users' privacy in traditional blockchains remarkably. While many encouraging solutions have been presented, in most cases they are computationally too impractical for widespread use at the moment. Buterin has well described the situation by noting that there is no 'magic bullet' for privacy in blockchains, but instead developers should focus on 'partial solutions for specific use cases'.[242] In order to help developers to build privacy-enhancing solutions for different blockchain use cases, legal certainty in respect to the acceptable level of anonymisation is required. As long as the legal uncertainty prevails, it is hard to assess whether any of the current or proposed solutions suffice for anonymising transactional data or metadata (public keys). In any case, the high standard for anonymisation set out by Article 29 Working Party is likely to result in many cases for blockchain-based applications to trigger the application of the GDPR.

[239] Ibáñez, O'Hara and Simperl (n 8) 7.
[240] Spindler and Schmechel (n 162) 175-76.
[241] The Elements Project, 'Confidential Transactions' (*Elements Project*) <www.elementsproject.org/elements/confidential-transactions/> accessed 14 August 2018.
[242] Buterin, 'Privacy on the Blockchain - Ethereum Blog' (n 237).

4.4 Allocation of responsibilities on blockchain networks

4.4.1 Main users of personal data under the GDPR

Primarily the GDPR only codified already existing roles and practices of different participants in data processing activities. In general, a data controller is still the most important role because a data controller has the main responsibility for complying with different obligations of the regulation and for ensuring that data subjects' rights are protected. However, the GDPR assigned more responsibilities also to data processors, who must comply with many of the requirements that apply to data controllers.[243] A data controller is defined in the regulation as the one who *determines the purposes and the means* of the processing of personal data.[244] Article 29 Working Party has provided some guidance on how to interpret the notion of 'purposes and means of processing'. In its opinion it concluded that while determining the purposes (why data is processed) is solely reserved for data controllers, the determination of certain technical and organisational elements related to the means of processing could be delegated to data processors. However, most substantial questions such as 'which data shall be processed' and 'who shall have access to them' are still reserved for controllers.[245] The legal form is not decisive in determining a responsible data controller because a data controller may be a natural or a legal person or any other entity.[246] In situations where the determination should be made between an individual, such as an employee, and a company or government agency, Article 29 Working Party has emphasised that the company or agency should be considered as a data controller rather than an individual employee because entities are in better place to exercise data subjects' rights.[247] In any case, determining who should be a data controller requires careful attention to the factual circumstances of the case.[248]

Determination between a data controller and a data processor can be difficult especially when there are several participants in the data processing activities. The main difference between the

[243] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 101.
[244] GDPR Article 4(7).
[245] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010) WP169 15.
[246] GDPR Article 4(7).
[247] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (n 245) 15.
[248] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 102.

roles is that data controllers define the means and purposes of processing whereas data processors process data on behalf of data controllers.[249] Thus, there is a relationship between data controllers and processors in which data processors are acting under the control of a data controller. The GDPR requires that data controller and data processors enter into a binding contract, which defines 'the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller'.[250]

The GDPR also recognises situations where two or more controllers process personal data for a shared purpose and jointly determine the purposes and means of processing. Joint controllers shall allocate their responsibilities for compliance with the GDPR in a transparent manner, preferably in written form.[251] Article 29 Working Party has emphasised a flexible interpretation which could cover increasingly complex data processing scenarios. According to the opinion, joint controllership does not necessarily require an equal participation and different controllers may have different roles in the processing.[252] Further, in complex data processing scenarios, special attention should be paid to allocate responsibilities in a clear and transparent manner.[253]

4.4.2 Accountability gap and enforcement issues on traditional blockchains

The core nature of traditional blockchain technologies relies on distributed ledgers and peer-to-peer networks, which is in a total contradiction with the underlying assumption of the GDPR that personal data are stored on centralised data silos under the control of a specific central intermediary. Due to this fundamental problem, it is difficult to allocate data protection responsibilities to different participants on blockchain networks. Here, it is worth remembering that even among traditional blockchains there are different ways to use the blockchain technology for transacting. When the blockchain technology is used for direct transactions between individuals, such as in the case of Bitcoin, the participants are not the same as to when

[249] Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 101.
[250] GDPR Article 28(3).
[251] GDPR Article 26(1).
[252] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (n 245) 19.
[253] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (n 245) 22.

blockchain technology is used as a backend for decentralised applications.[254] Therefore, determination of the respective data protection responsibilities on blockchain networks should be done on a case-by-case basis considering the actual roles and functions of each participant.[255] On blockchain networks, there are several participants including nodes, miners, developers, application providers, and other service providers. Legal scholars have presented different ideas for allocating responsibilities on blockchain networks. Much attention has been paid to whether nodes, which are computers through which users connect to a blockchain network, qualify as data controllers or processors. Berberich and Steiner have considered that there are two options; either no node qualifies as a data controller or every node qualifies as a data controller.[256] Another way to look at the issue is to consider all nodes together as joint data controllers. The third and more extreme option would be to consider data subjects also as data controllers. Some have also presented an idea that nodes and miners should rather be considered as infrastructure than responsible participants in data processing activities.[257] All of the options are discussed in more detail below.

The difficulty to determine who is a responsible data controller undermines the principle of accountability, one of the main principles of the GDRP. Berberich and Steiner have described this issue as an 'accountability gap', where the exercise of data subjects' rights, compliance with data protection principles and obligations, and enforced sanctions could lose their effectiveness.[258] In addition to the difficulties in determining a responsible data controller, perhaps even more difficult issue may arise in relation to enforcement. It is hard to define the exact number, identity, and location of nodes considering the pseudonymous and supranational nature of blockchain networks.[259] What is more, due to the supranational nature of blockchain networks and the extraterritorial scope of the GDPR, the regulation is likely to catch even data controllers that are established outside of Europe but have some connection to data subjects in the Union.[260] If nodes were to qualify as data controllers or joint controllers, data subjects could

[254] Ibáñez, O'Hara and Simperl (n 8) 9-10.
[255] Valeria Ferrari, 'EU Blockchain Observatory and Forum Workshop on GDPR , Data Policy and Compliance' (Report on EU Blockchain Observatory and Forum Workshop, Brussels, 8 June 2018) ch 4.2 < https://blockchain-society.science/wp-content/uploads/2018/07/blockchain_society_research_nodes_1_GDPR_workshop_03072018.pdf> accessed 17 August 2018.
[256] Berberich and Steiner (n 48) 424.
[257] Eichler and others (n 190) 6.
[258] Berberich and Steiner (n 48) 242.
[259] Finck (n 13) 17.
[260] The extraterritorial scope of application is defined in Article 3(2), according to which the regulation applies also to data controllers and processors which are established outside of the Union, if their processing activities relate either to targeting their goods or services to data subjects in the Union or monitoring their behaviour in the

claim their rights against each node independently, which is not technically feasible. Individual nodes are unable to respond to the tasks the GDPR sets out for data controllers because in many cases the data stored in blockchains is either encrypted or hashed and the immutable ledger makes it practically impossible for an individual node to modify data on blocks. In a such case, nodes would most likely violate the provisions of the GDPR and would have to face hefty fines. It could be contested whether that would be proportionate considering the passive role of the nodes in data processing.[261] In case nodes qualify as data processors instead of controllers, there would still be difficulties considering that data controllers (data subjects or application providers) would need to conclude data processing contracts with each node, and in case the nodes violate their obligations, same type of enforcement difficulties may arise even if data controllers carry the overall responsibilities.[262] In light of the aforementioned, it is clear that enforcing compliance with the GDPR would be extremely difficult in such circumstances.

4.4.3 Allocation of responsibilities on traditional blockchains

Legal scholars have presented various ideas for allocation of responsibilities on blockchain networks. Berberich and Steiner have presented the idea that either no node qualifies as a data controller because there is no individual control over the distributed ledger or every node qualifies as a data controller because technically each node process copies of the ledger. Without giving preference to either option, they simply state that 'both outcomes hardly bring meaningful results'.[263] Finck has considered that more likely outcome is that every node qualifies as a data controller because they independently pursue their objectives, decide whether to join the blockchain network or not, and decide the means and purposes of the processing. Determining that each node qualify as a data controller will lead to serious enforcement difficulties as explained above. Further, it seems to lead to a disproportionate situation where each node could face heavy sanctions for not complying with the obligations of the GDPR while

Union. Extraterritoriality has been criticised by legal scholars because it risks of being a 'paper tiger' as the EU has no power to execute provisions of the GDPR outside the Union. In the context of blockchain, the situation is even more complex and problematic if nodes are considered as data controllers or joint controllers because nodes may be located all around the globe. Salmon and Maxwell (n 154) 11. On the extraterritorial scope of application see n 98.

[261] Finck (n 13) 17-18.

[262] In case a data processor would not respect the conditions of the data processing contract, the data processor would most likely be regarded as a data controller acting unlawfully or as a joint controller together with the data controller. Union Agency for Fundamental Rights - Council of Europe-European Court of Human Rights - European Data Protection Supervisor (n 66) 108.

[263] Berberich and Steiner (n 48) 424.

those nodes do not have real possibilities to comply with the obligations.[264] Salmensuu has proposed an interpretation according to which nodes could be excluded from the liability due to their 'mere technical, automatic and passive nature of data processing'.[265]

Another way to look at the data controller issue is to consider all nodes on blockchain network as joint controllers. There has been a debate among legal scholars whether nodes could qualify as joint controllers. The debate has concerned whether nodes are jointly determining the means and purposes of processing. Finck, Berberich and Steiner have argued that nodes do not meet with the standards set out for joint controllers because there is no transparent and clear allocation of responsibilities, but instead the system is 'shaped by the nodes' individual behaviour'.[266] On the other hand, Ibáñez, O'Hara and Samperl have considered in their research that public and permissionless blockchains are 'closer to a scheme where all participants are potential joint-controllers'.[267] Similarly, Wirth and Kolain have questioned the necessity of 'intention to agree' and argued that there is strong case for considering that joint controllership applies to blockchain networks because nodes in the network are equal participants of the network, free to choose whether to join or not, and capable of changing the rules if majority of the nodes agree. However, Wirth and Kolain continue that if nodes are to be considered as joint controllers, blockchain developers would have to design a layer of liability on top of blockchain applications to allocate responsibilities between nodes in a clear and transparent agreement, which could severely diminish the attractiveness of the blockchain applications.[268]

Legal scholars have presented also the idea that data subjects could qualify as data controllers under certain circumstances. Salmon and Maxwell have compared blockchain networks to cloud computing systems, where the cloud systems are considered as data processors while the users downloading the files on the cloud are data controllers. On blockchain networks, in the absence of centralised intermediary, the users could be considered as data controllers for

[264] Finck (n 13) 17.
[265] Salmensuu has noted that similar precedent can be found on the EU law in the context of e-Commerce Directive, where ISPs are exempted from liabilities, if the 'activity is of a mere technical, automatic and passive nature. Salmensuu (n 172) 103-04.
[266] Berberich and Steiner (n 48) 424; Finck (n 13) 17.
[267] Ibáñez, O'Hara and Simperl (n 8) 5.
[268] Michael Kolain and Christian Wirth, 'Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data' in Wolfgang Prinz & Philipp Hoschka (eds), *Proceedings of the 1st ERCIM Blockchain Workshop 2018* (European Society for Socially Embedded Technologies 2018) <https://hdl.handle.net/20.500.12015/3159> accessed 19 August 2018.

themselves and data processors for others.[269] Moreover, it is possible to build on top of traditional blockchain applications sophisticated access authentication systems, which could give individuals true control over their personal data. Users can decide to whom they give access to their personal data and disable the access to the data anytime.[270] In such scenarios, the means of processing could be determined by the blockchain-based application while it is up to the end-user to determine the purposes of processing.[271] De Filippi has considered that in decentralised data systems the 'responsibility of keeping data private' shifts from centralised intermediaries to individuals.[272] Such approach seems prima facie to be in line with the objective of giving individuals more control over their personal data. However, Salmensuu has criticised the approach because it presumes that data subjects are well-informed not only of their rights as data subjects but also of the different technologies used to process personal data.[273] Accepting data subjects as data controllers in the context of traditional blockchains would likely require educating data subjects of the risks related to the processing of personal data on 'immutable' blockchains. Further, it would require a flexible approach, which approves alternative means to achieve objectives of the GDPR, to the allocation of responsibilities.[274]

Ibáñez, O'Hara and Samperl have presented in their research two practical scenarios for traditional blockchains. Firstly, traditional blockchains can be used by individuals to interact directly with blockchain, for instance, when individuals exchange cryptocurrencies without a centralised intermediary. In such a situation, the authors consider that it is impossible to find an accountable data controller. Thus, the responsibility for compliance should be shifted to the end-users by requiring them to sign terms of use.[275] In the second scenario, traditional blockchains are used as a backend for applications or platforms (smart contract platforms). The most obvious interpretation would be to consider the application providers as data controllers because they determine what personal data is collected and how the data is processed on a blockchain.[276] Other participants such as nodes, miners, online wallet operators, and other

[269] Salmon and Maxwell (n 7) 10.
[270] Salmensuu (n 172) 114.
[271] Finck (n 13) 18.
[272] De Filippi (n 61) 15.
[273] Salmensuu (n 172) 102.
[274] Finck (n 13) 29.
[275] The terms of use would prohibit users from uploading certain personal information on the blockchain. Secondly, users would be required to consent to the processing or some other legal basis for the processing would be expressed. The consent and the legitimate interest as lawful bases for the processing are analysed in more detail in relation to data subject's right to erasure in Chapter 5.2.2. Ibáñez, O'Hara and Simperl (n 8) 9-10.
[276] Ibáñez, O'Hara and Simperl (n 8) 10.

service providers would qualify as data processors.[277] While this scenario seems prima facie much easier to carry out, it also comes with some impracticalities. The GDPR requires a data controller to enter into data processing contract with every data processor it is using.[278] This would mean that data processing contracts would have to be concluded with every node or miner of the blockchain network, which could be extremely challenging. Eichler and others have argued that these issues illustrate why nodes and miners should rather be considered as infrastructure than actual users of personal data in all circumstances.[279]

Above described different scenarios give a brief illustration of how problematic the allocation of responsibilities and enforcement of data protection obligations can be on traditional blockchains. Considering that accountability and enforcement of the obligations are crucial for a proper functioning of the GDPR, these issues deserve more attention and research. The EDPS has recognised the importance of the difficulties and recommended experts to look at the issue.[280] Without considering what would be the most likely regulatory approach for allocating responsibilities on traditional blockchains, this research settles at this point for stating that such determination is not an easy task. As legal scholars have acknowledged, the determination should be done on a case-by-case basis considering the actual roles and functions of different participants in every individual case.[281]

5 The conflict between the right to erasure under the GDPR and the immutability of traditional blockchains

5.1 History and scope of the right to erasure

5.1.1 History of the right to erasure

[277] Ferrari (n 255) ch 4.2.
[278] GDPR Article 28.
[279] Eichler and others (n 190) 6.
[280] European Data Protection Supervisor, 'Annual Report 2016' (Publications Office of the European Union, 2017) 4.
[281] Ferrari (n 255) ch 4.2.

The need for the right to be forgotten or the right to erasure arises from the rapid development of data analysis techniques and reduced data storage costs. In the past, information was forgotten by default because there were no efficient ways to search and process data and storing data was more expensive. Today, in the digital age a data is remembered by default and individuals cannot be truly forgotten in online. Due to this development, individuals have neither control over their data nor their identities online. In such a world, there seems to be a need for the right to be forgotten in order to give individuals more control over their data and identities.[282] In spite of that, the right received a lot of criticism during the legislative process of the GDPR. Understanding the actual scope of the right helps to exercise the right properly and to avoid some common misconceptions relating to its extent.

Instead of a being entirely new right, the right to erasure, more commonly known as the right to be forgotten, has developed progressively over the years. Some instances of the right were already present in different national data protection laws drafted before the DPD, which entered into force in 1995.[283] The DPD does not contain a separate right to erasure or a right to be forgotten, but certain provisions of the DPD can be regarded as a seed for the right to erasure as it appears under Article 17 of the GDPR. Article 12(b) of the DPD gave data subjects the right to obtain rectification, erasure or blocking of data particularly if the data was incomplete or inaccurate. Article 12(c) in turn provided obligation for a data controller to inform third parties of the request to erase data, when the request was carried out in compliance with Article 12(b). Furthermore, Article 14 of the DPD provided data subjects with a right to object to the processing of personal data under certain conditions.[284] These rights have been considered as 'diluted right to be forgotten provisions'.[285]

The European Commission published its Communication in 2010 in which it acknowledged that the right to be forgotten should be clarified to strengthen individuals' control over their personal data.[286] The Communication was a starting point for a legal debate of the right to be

[282] Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, 'Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions' [2018] Journal of Cybersecurity 1, 9 <https://doi.org/10.1093/cybsec/tyy001> accessed 2 September 2018.
[283] Gabriela Zanfir, 'Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Reforming European Data Protection Law* (Springer 2015) 227, 239.
[284] Cesare Bartolini and Lawrence Siry, 'The Right to Be Forgotten in the Light of the Consent of the Data Subject' (2016) 32 Computer Law and Security Review 218, 224.
[285] Markou (n 11) 207.
[286] European Commission (n 88) 8.

forgotten. In 2012, the Commission published the draft version of the GDPR, which contained an ambitious wording of the right to erasure. The extraterritorial scope of application of the GDPR also attracted the attention of the United States (US) legal scholars, who harshly criticised the right to be forgotten.[287] The criticism focused especially on the potential conflicts between the right to be forgotten and the freedom of speech, on the difficulties in enforcing the right, and on the ambiguity of the terms erasure and forgetting.[288] In the US, the freedom of speech is typically interpreted widely and often at the expense of the privacy and data protection. Against that background, it is unsurprising that the right to be forgotten was seen as an excessive threat to the freedom of speech. In the Union, the right to data protection, by contrast, is recognised as a fundamental right that should be equally balanced with other fundamental rights, such as the freedom of speech. This and other underlying differences on the approach to data protection between the US and the EU explains the strong reaction to the right to be forgotten.[289]

The right to be forgotten was also criticised for the burden it places on data subjects. According to the critics, the right to be forgotten presumes that individuals know what personal data of them are processed and who is the responsible data controller. However, this is rarely the case in the era of big data. These difficulties of exercising the right could reduce the efficiency of the right.[290] Further, the right to be forgotten was criticised for the ambiguity of the term 'forgotten'. The term forget implies that data subjects have an actual right to have any information on them permanently erased from the web. However, such a right would be in a collision with the freedom of speech and not practically feasible considering that it is extremely difficult to be sure whether information that has once been published online exist somewhere even if the controller has erased the data.[291] Search engines further challenge the concept of web's forgetfulness by providing tools for anyone to find information that could be otherwise buried on the web and forgotten.[292] Nevertheless, Article 17 of the GDPR does not provide a right to be genuinely forgotten on the web, even though it is a significant step towards such a right. It has been argued that Article 17 should not contain the label right to be forgotten at all

[287] Zanfir (n 283) 230.
[288] Kieron O'Hara and Nigel Shadbolt, 'The Right to Be Forgotten: Its Potential Role in a Coherent Privacy Regime' (2015) 1 European Data Protection Law Review 178, 178.
[289] O'Hara and Shadbolt (n 288) 181.
[290] Muge Fazlioglu, 'Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet' (2013) 3 International Data Privacy Law 149, 151.
[291] Politou, Alepis and Patsakis (n 282) 13.
[292] Markou (n 11) 219.

because the term may be misleading.[293] On the one hand, the label might undermine the actual content of the right by implying that the right is available only if data is outdated. On the other hand, it might mislead data subjects to believe that they have a right to get rid of their online history and to be de facto forgotten.[294]

The next significant landmark on the development of the right to be forgotten was the *Google Spain* decision given in 2014.[295] In the case, a Spanish citizen lodged a complaint against a Spanish newspaper and the Google Spain. The claimant demanded that information concerning real-estate auction notice of his repossessed home would not appear on the Google's search results because the proceedings were resolved years ago and the reference to them was no longer relevant. The claimant requested the newspaper to delete certain web pages and the Google Spain to remove his personal data so that the search results would no longer display such personal information.[296] The Court ruled that search engines can be data controllers under the DPD and data subjects have a right to request search engines to remove links to web pages containing personal data of them if the data is no longer necessary for the initial purposes, especially when the data has become inaccurate, inadequate, irrelevant or excessive.[297] Furthermore, the Court found that the right is not absolute because it must always be balanced against other fundamental rights including the right to free expression.[298]

The case raised another legal debate regarding the right to be forgotten. The Commission argued that even though the ruling did not explicitly mention the right to be forgotten, the Court applied implicitly existing right to be forgotten.[299] This argument has been questioned by several legal scholars, who have argued that the Court did not apply the right to be forgotten at all, but that instead, the Court applied Articles 12(b) and 14 under the DPD.[300] This was also expressed by the Advocate General Niilo Jääskinen in his Opinion in the Google Spain in which he stated that the DPD 'does not provide a general right to be forgotten'.[301] Regardless whether the Court

[293] The right to be forgotten is mentioned in the label of the Article 17, although it is in brackets; Article 17 Right to erasure ('right to be forgotten').
[294] Markou (n 11) 215-16.
[295] Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* EU:C:2014:317.
[296] European Commission, 'Factsheet on the " Right to Be Forgotten" ruling (C-131-12)' (Commission factsheet, 2014).
[297] Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* EU:C:2014:317, paras 83, 93.
[298] Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* EU:C:2014:317, para 85.
[299] European Commission, 'Factsheet on the " Right to Be Forgotten" ruling (C-131-12)' (n 296).
[300] On the legal debate see eg Bartolini and Siry (n 284) 233-34.
[301] Case C-131/12 *Google Spain v. AEPD and Mario Costeja González* [2013] EU:C:2013:424, Opinion of AG Jääskinen, para 111.

applied an implicit right to be forgotten or not, it is obvious the ruling did not cover the right to erasure to the extent it is under Article 17 of the GDPR.[302]

5.1.2 The right to erasure under Article 17 of the GDPR

Although the right to erasure is not an entirely new right *per se*, Article 17 provides more detailed and precise right for data subjects to exercise. Article 17 is divided into three paragraphs. According to the Article 17(1):

> *1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*

The first paragraph, on the one hand, gives data subjects a right to obtain erasure, and on the other hand, sets an obligation for data controllers to erase data without undue delay. The right to erasure is not, however, an absolute right as it requires that at least one of the following six grounds applies.

The first ground applies when personal data is no longer necessary for the purposes it was initially or otherwise processed.[303] This ground is in line with the principle of purpose limitation. The second ground applies when data processing is based on the data subject's consent, and the data subject has decided to withdraw the consent. However, this ground does not apply in case the data controller has other legal ground for the processing.[304] Under the DPD, there was no explicit right to withdraw consent, which was problematic considering that a consent is the most common lawful basis for processing.[305] The right to withdraw consent under Article 7(3) of the GDPR combined with the right to request erasure when the consent is withdrawn pursue to restore data subjects the control over their personal data even after they have given their consent for the processing. As long as the scope of 'other legal ground' exception remains uncertain, the exception forms a risk for an effective exercise of the right to erasure when withdrawing consent.[306] The third ground is applicable when a data subject

[302] Bartolini and Siry (n 284) 229.
[303] GPDR Article 17(1)(a).
[304] GPDR Article 17(1)(b).
[305] Bartolini and Siry (n 284) 223.
[306] Bartolini and Siry (n 284) 230.

exercises the right to object pursuant to Article 21(1) unless a data controller has an overriding legitimate ground for the processing. The exception of overriding legitimate ground does not apply if the data subject objects processing for direct marketing purposes.[307] Successful objection to processing does not result in the erasure of the data, so it seems that data subject should request the erasure separately alongside with the objection.[308] The fourth ground applies when data is processed unlawfully, for instance, when there is no legal ground for the processing or the processing infringes data processing principles.[309] The fifth ground applies when data must be erased to comply with a legal obligation. The last ground applies when data is collected and processed in the context of offering information society services to a child younger than 16 years.[310]

The second paragraph contains another obligation for data controllers, which have made personal data public and are obliged to erase the data pursuant to the first paragraph. According to the Article 17(2):

> *2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.*

While the first paragraph sets an obligation for a data controller to delete data under certain circumstances, the second paragraph goes further by embracing the right to be 'forgotten'.[311] In theory, a data subject could request each controller or third party individually to erase any replications of the personal data. However, in cases where the initial controller has made the personal data public, it is practically difficult to know who those other controllers are because once information is published online, it is easy to replicate it.[312] As a response to this practical problem, Article 17(2) strengthens data subjects' right to obtain erasure by obliging initial data controllers to take reasonable steps to inform other controllers processing the data of the request.[313] In essence, data controllers are obliged to implement technical means for tracking

[307] GDPR Article 17(1)(c).
[308] Zanfir (n 283) 233.
[309] De Hert and Papakonstantinou (n 89) 185.
[310] GDPR Article 17(1)(e) and 17(1)(f).
[311] Politou, Alepis and Patsakis (n 282) 11.
[312] Politou, Alepis and Patsakis (n 282) 13.
[313] Bartolini and Siry (n 284) 230.

personal data.[314] The second paragraph thus represents an attempt to provide data subjects with a possibility to obtain complete erasure of their personal data – to be actually forgotten.

The right to be forgotten has been criticised for the fact that it sets an unreasonable burden on data controllers because it is practically impossible to delete information permanently in an online environment.[315] Politou, Alepis and Patsakis have reviewed in their research several state-of-art methods and architectures that seek to enable permanent erasure of widely distributed data. They point out that there are interesting solutions for tracking data and helping data controllers to comply with the obligation to inform other controllers.[316] In the same vein, Bartolini and Siry have noted that many actors have already implemented such solutions, and that there is a growing trend to adopt such means.[317]

Moreover, in contrast to the obligation to erase personal data without undue delay, the obligation to inform other controllers of the request is not a duty to achieve a specific result but instead a duty of best effort. In other words, the data controller is not required to ensure that other controllers remove links, copies or any replication of the personal data, but it is enough that the data controller takes reasonable steps to inform them. Thus, the data controller is not held liable even if it fails to inform other controllers, provided that it has taken reasonable steps to inform.[318] Regulators drafted deliberately quite a general obligation to inform and avoided binding the provision to any specific technical means in order to prevent the provision becoming outdated as a consequence of technological advances.[319] It has been argued that the lack of technical guidance on the right to be 'forgotten' might compromise the future enforcement of the right.[320]

As already noted, the right to erasure is not an absolute right considering that it requires a specific legal ground to apply. Secondly, the right to erasure under Article 17 contains a specific list of limitations on the right. The third paragraph contains limitations which cover both the obligation to erase data and the obligation to inform other controllers. The freedom of

[314] Bartolini and Siry (n 284) 231.
[315] Politou, Alepis and Patsakis (n 282) 12-13.
[316] Politou, Alepis and Patsakis (n 282) 16.
[317] Bartolini and Siry (n 284) 231.
[318] Zanfir (n 283) 217.
[319] Politou, Alepis and Patsakis (n 282) 12.
[320] Politou, Alepis and Patsakis (n 282) 11.

expression and information is the most discussed limitation for the right to erasure. That is only natural considering that when personal data is made public, the right to have one's personal data erased is often in conflict with the right of the general public to have access to that information. The limitation aims to strike a balance between the data protection and the freedom of expression. The Court recognised the exception already in the *Google Spain* case, where it ruled the right to delisting not to be an absolute right because it must be balanced against other fundamental rights, especially the freedom of expression and the freedom of the media.[321] Other limitations concern the compliance with legal obligations or performance of a public task, the processing for public interest in the area of public health, the processing for historical, statistical, and scientific purposes, and the processing for exercising legal claims. These limitations provide necessary guidance of the actual scope of the right to erasure.[322]

5.1.3 The right to erasure and other provisions of the GDPR

Article 17 states under which conditions the right to erasure applies and what is the scope of the right. However, a proper understanding of the right also requires attention to some other important aspects of the right. Significant novelty concerning the exercise of the right is a reversed burden of proof, which is in line with the new principle of accountability. Instead of requiring a data subject to prove that the data is inaccurate or outdated and should be erased, the GDPR provides data controllers to be able to prove that the data cannot be erased as it is necessary for the processing. Moreover, the extraterritorial scope of application and significant sanctions avoid circumventing the obligations and encourage companies to comply with the right.[323]

In general, the right to erasure is an essential tool for improving individuals' control over their personal data and enhancing their right to data protection. Besides providing a separate right to erasure, Article 17 can help to exercise other rights under the GDPR, such as the right to object processing of personal data or the right to withdraw consent.[324] The right to erasure has also a connection to the right to the restriction of processing, which could be applied when processing is unlawful but the data subject requests a restriction of the processing instead of an erasure of

[321] European Commission, 'Factsheet on the " Right to Be Forgotten" ruling (C-131-12)' (n 296).
[322] GDPR Article 17(3)(b), (c), (d), and (e).
[323] European Commission, 'Factsheet on the " Right to Be Forgotten" ruling (C-131-12)' (n 296).
[324] Markou (n 11) 210.

the data.[325] Moreover, Article 19 requires data controllers to notify any erasure carried out pursuant to Article 17(1) to each recipient to whom the personal data have been disclosed. However, the data controller may derogate from this obligation if the obligations proves impossible or requires a disproportionate effort.[326]

As discussed above, it has been contested whether the right to be forgotten existed implicitly already in the DPD or not. Without delving deeper into that debate, it is evident that Article 17 provides much more detailed and specified right to erasure than ever seen before. The provision specifies circumstances for exercising the right by introducing both legal grounds for its application and limitations on the scope of it.[327] This detailed definition of the right helps both the data controllers and the data subjects to assess when the right can be exercised. The legal grounds for the right extend the scope of the previously existed 'diluted right to be forgotten provisions' under the DPD. The right to erasure is thus a very welcome right for enhancing individuals' data protection in the digital age. Despite both the right to erasure and the GDPR itself were adopted as a response to the challenges stemming from advanced data analysis techniques, it seems, that the regulation is already one step behind technology.

5.2 Reconciling the conflict between the immutability and the right to erasure

5.2.1 What is the conflict about?

The previous chapter presented the actual scope of the right to erasure under the GDPR. With that presentation in mind, it is time to move forward to delve into the issues stemming from the immutability of traditional blockchains. The immutability is a core feature of blockchain technologies that allows affirming the integrity of the ledger without having to trust on third parties.[328] In traditional blockchains, data is stored on blocks. Only new blocks can be added to the chain, and each new block is connected to the previous block through a hash function. The blocks form a distributed chronological ledger.[329] Each node holds only copy of the ledger. Technically, a local copy of the ledger could be modified, but the modified ledger would not be

[325] GDPR Article 18(1)(b).
[326] GDPR Article 19.
[327] Markou (n 11) 210.
[328] Finck (n 13) 4.
[329] Salmon and Maxwell (n 7) 6.

approved by other nodes. Modifying data on old blocks invalidates the blockchain as even a slight modification of the block's data creates a different hash for the block, and the hash would no longer correspond with the hash stored on the next block.[330] In traditional blockchains, modifying or erasing data on old blocks would require to unbuild the blockchain, modify or erase the data on the block, and then rebuild the unbuild part of the blockchain again. [331] Another way would be to build a new chain containing the modifications. The modifications would require a majority of the nodes to agree (consensus), which can be extremely difficult to accomplish in a decentralised peer-to-peer network.[332]

Traditional blockchains are decentralised peer-to-peer networks in which achieving consensus to modify data on old blocks is extremely challenging due to the large number of unrelated and pseudonymous participants. Nevertheless, true immutability does not exist on Bitcoin or Ethereum currently because old data could be modified, and the modifications could be validated if the majority of the nodes agreed. Essentially, Bitcoin and Ethereum trust on the majority of the network instead of centralised intermediaries.[333] Bitcoin and Ethereum are currently based on PoW consensus algorithm in which miners create blocks.[334] It would be very expensive but not impossible for a centralised mining pool or a government to install more mining power than the rest of the network and to achieve control over the blockchain.[335] The DAO hack was an illustrating real-life example how blockchains are not truly immutable.[336] While traditional blockchains are not genuinely immutable because the ledger could be modified and validated by the majority, traditional blockchains are still incredibly tamper-resistant and nearly immutable ledgers.

[330] Neisse, Steri and Nai-Fovino (n 133) 2.
[331] Berberich and Steiner (n 48) 426.
[332] Greenspan, 'The Blockchain Immutability Myth' (n 49).
[333] Giuseppe Ateniese and others, 'Redactable Blockchain - Or - Rewriting History in Bitcoin and Friends' [2017] IEEE European Symposium on Security and Privacy 111, 120 < https://ieeexplore.ieee.org/document/7961975/> accessed 2 September 2018.
[334] Ethereum is about to release a Casper protocol which implements the PoS consensus algorithm instead of the PoW. In the PoS, new blocks are not created by miners, but instead so that 'a set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its deposit (i.e. stake).' The main benefits of PoS compared to the PoW are improved security, reduced risk of centralisation, and energy efficiency. 'Proof of Stake FAQs' (Github ethereum wiki) <http://cryptorials.io/glossary/proof-of-stake/%5Cnhttps://en.bitcoin.it/wiki/Proof_of_Stake> accessed 20 September 2018.
[335] Greenspan, 'The Blockchain Immutability Myth' (n 49).
[336] More on DAO hack see n 137.

It should be noticed that the conflict between the right to erasure and the immutability is tightly connected to the question about personal data and anonymisation and the question about allocation of responsibilities on traditional blockchains, which were discussed in Chapter 4.3 and 4.4 in more detail. Firstly, anonymisation techniques are the most obvious and effective solution for the conflict. If transactional data and public keys could be anonymised, the GDPR would not apply, and there would be no need to consider how to comply with the right to erasure at all. Secondly, the question about allocation of responsibilities on traditional blockchains is crucial in determining who should comply with the obligation to erase and from whom the data subjects could obtain the erasure. The allocation of responsibilities with regard to the right to erasure is considered in Chapter 5.3.2.

The conflict between the immutability and the right to erasure has been recognised by some legal scholars, who have reviewed possible solutions to the conflict. From a legal perspective, the solutions are based on that the right to erasure is not an absolute right and the term erasure is not defined in the GDPR. The right to erasure is not an absolute right considering that Article 17(3) lists five different limitations on the right to erasure. These exceptions are not, however, of particular interest in relation to the immutability but could be relied on if a blockchain application is used for such purposes.[337] Moreover, data controllers are obliged to erase data only if at least one of the six legal grounds for the erasure applies. The exact meaning of the term erasure is also uncertain. Therefore, it is possible to argue that erasure does not necessarily refer to an outright deletion of the data, but instead, some alternative solutions could be used to disable access to the data.[338] In addition to the legal solutions, blockchain developers have developed means to make it easier to erase data on old blocks. All these solutions are analysed in detail in Chapter 5.2.3.

The right to erasure covers two obligations for data controllers. The obligation to erase personal data without undue delay if certain conditions are met seems to be prima facie in total conflict with the immutability of traditional blockchains because erasing data on blocks is extremely difficult. The second obligation requires a data controller to inform other controllers of the request to erase any links, copies, or replications of the personal data if the personal data is made public and if there is an obligation to erase pursuant to Article 17(1). While the conflict

[337] Finck (n 13) 23.
[338] Finck (n 13) 25.

between the immutability and the obligation to erase is the primary focus of this research, it is worth also analysing the second obligation with respect to traditional blockchains.

5.2.2 Obligation to inform other controllers of the request to erase in traditional blockchains

The second obligation requires data controllers if they have made the personal data public to take reasonable steps to inform other controllers that data subject has requested erasure. This second obligation attempts to guarantee data subjects the right to be 'forgotten' by requiring the initial controller to implement technical means to track the movement of personal data in order keep up with who has replicated the data. While the obligation to erase has attracted a lot of attention in the blockchain community, the obligation to inform other controllers has been overlooked. The GDPR allows taking account of available technology and the cost of implementation when assessing the reasonable steps to inform, which could provide room for a flexible interpretation that considers the technical difficulties of complying with the obligation in a blockchain environment. Due to the abstract wording of Article 17(2), it is uncertain how the obligation will be enforced in practice.[339] On traditional blockchain networks, transactions are not only distributed to all nodes on the network but are also available for anyone to review online. Thus, it seems that the data in the transactions and the public keys are made public on blockchains.

Neisse, Steri and Nai-Fovino have presented in their research two data accountability and provenance tracking solutions build on Ethereum platform, which could enable data subjects (users) to track data controllers and processors to whom the data subjects have given access to their personal data.[340] These solutions could be interesting in relation to the obligation to inform other controllers because they enable means for tracking bounces of data on traditional blockchains. Access authorisation solutions implemented on blockchain applications could provide users with technical means to keep track of data controllers and processors to whom the user has directly or indirectly given access to the data.[341] As discussed in Chapter 4.4.3, it is possible to argue that on traditional blockchain networks users are both data subjects and data controllers at the same time. The user (data controller) could keep track of the data that he or

[339] Politou, Alepis and Patsakis (n 282) 11.
[340] Neisse, Steri and Nai-Fovino (n 133).
[341] Neisse, Steri and Nai-Fovino (n 133) 1.

she is willing to share with other data controllers and processors. However, it seems that the problem exists in relation to the public keys. The user would not be able to keep track of the data controllers accessing the public keys from publicly available transaction history.

Regarding the obligation to inform data controllers of the request to erase any links, copies or replications of the personal data, it could be argued that the technical means to track bounces of the data could not be implemented by reasonable means on traditional blockchain applications. Another way to comply with Article 17(2) would be the anonymisation of public keys. As discussed in Chapter 4.4.3, it is uncertain whether public keys could be anonymised with state-of-art anonymisation techniques or with advanced anonymisation techniques in the future. A flexible interpretation that would reconsider the high threshold for anonymisation set out by Article 29 Working Party could enable the anonymisation of public keys on traditional blockchains.

5.2.3 Solutions proposed for reconciling the conflict between the right to erasure and the immutability of traditional blockchains

Interpretations of the legal grounds under Article 17(1)

Some legal scholars have noted that solution for the conflict between the right to erasure and the immutability of traditional blockchains could be found on the legal grounds upon which the right to erasure applies. Berberich and Steiner have claimed that it is not unthinkable that the 'core functioning principle of technology' could serve as a basis to refuse to accommodate a request to erase data from a blockchain.[342] Article 17(1)(a) provides a data subject with the right to obtain erasure if the personal data are no longer necessary for the purposes they were collected or otherwise processed. Berberich and Steiner have argued that it is conceivable that in the context of blockchain personal data are considered as necessary for the processing purposes because a perpetual and immutable storage is a necessity for the proper functioning of the blockchain.[343] Ibáñez, O'Hara and Simperl have similarly pointed out that it is possible to consider that the perpetual processing is always necessary for processing the data for the purposes they have been collected or otherwise processed. They use a land registry as an example to illustrate that the perpetual processing may be the precise reason for relying on

[342] Berberich and Steiner (n 48) 426.
[343] Berberich and Steiner (n 48) 426.

blockchain technology.[344] While this might provide a counter-argument for refusing to comply with a data subject's request in a particular case, it does not exclude traditional blockchain technologies in general from the obligation to erase data because the data subject may still rely on other applicable legal grounds under Article 17.

Another interesting legal ground that entitles data subjects to request erasure applies when the processing has been based on a data subject's consent, and the data subject has later withdrawn the consent. However, this ground is not unconditional because it does not apply if there is some other legal ground for the processing. The scope of the 'other legal ground' exception is uncertain and will depend on future interpretations of the Court. The exception seems to refer to the lawful bases for processing listed in Article 6 of the GDPR.[345] Berberich and Steiner have pondered whether the core functioning principle of technology could serve as other legal ground under Article 17(1)(b).[346] Considering the lawful bases set out in Article 6, the performance of a contract and the legitimate interest of a controller or third party appear to be the most suitable ones for the core functioning principle of technology.[347] The perpetual processing of personal data could be regarded as necessary for the performance of the contract when a data subject has entered into a contract that is performed by using a blockchain technology or stored in a blockchain. The problem with this option is that the data subject may terminate the contract, and after the termination, the data should be erased by a request.[348]

Another option would be to consider the core functioning principle of technology under the legitimate interest of a controller or third party. That would require carrying out a balancing exercise between the interests of the data controller or third parties and the interest and fundamental rights of the data subject as detailed below. Recital 47 of the GDPR states that when assessing the legitimate interest of the controller, attention should be paid to the relationship between the data subject and the controller and to the reasonable expectations of the data subject concerning whether further processing takes place on such circumstances. Thus, it is recommendable to inform the data subject in a transparent manner that he or she can neither exercise the right to withdraw consent nor the right to obtain erasure on the basis of withdrawing

[344] Ibáñez, O'Hara and Simperl (n 8) 4.
[345] Bartolini and Siry (n 284) 229-230.
[346] Berberich and Steiner (n 48) 426.
[347] Berberich and Steiner (n 48) 426.
[348] Salmensuu (n 172) 117.

consent. This informing could be done by using terms of service by which the user gives consent for the processing and knowingly waive the right to obtain erasure on the basis of Article 17(1)(b).[349] In practice, data subjects would have to give their consent in perpetuity acknowledging that the consent can no longer be efficiently withdrawn.[350] Such practise defeats the new possibility to efficiently exercise the right to withdraw consent introduced by the GDPR. It remains to be seen how data protection authorities or courts would respond to that.

The third legal ground for the erasure applies if data subject objects to the processing and there are no overriding legitimate grounds for the processing. A contrario, data controller could refuse to comply with the request to erase if it can demonstrate an overriding legitimate ground for the processing.[351] Besides relying on the consent as a legal basis for the processing, traditional blockchain applications could also rely on the legitimate interest of controllers or third parties as a lawful basis for the processing.[352] Traditional blockchains may be used for various use cases, such as cryptocurrencies, decentralised identity management, decentralised job markets, and so forth. Article 29 Working Party has noted that the concept of interest is rather broad covering not only benefits of the controller but also benefits for society in general.[353] Considering that traditional blockchains could enable new types of peer-to-peer applications which are specially developed to benefit individual users, it is conceivable that traditional blockchain applications could rely on the legitimate interest of third parties as a lawful basis for the processing. Processing personal data on a transparent and immutable ledger could be argued to pursue the legitimate interest of users because the processing is necessary to allow users to verify the validity of the ledger without trusting on a centralised intermediary.[354]

[349] Ferrari (n 255).
[350] Ibáñez, O'Hara and Simperl (n 8) 4.
[351] Bartolini and Siry (n 284) 229.
[352] Hungarian data protection authority has considered in its opinion (given before the GDPR came into force) that under the Hungarian data protection law a consent of the data subject or a legitimate interest of the users are the possible lawful bases for processing personal data stored on blockchains. Hungarian National Authority for Data Protection and Freedom of Information, 'The Opinion of the Hungarian National Authority for Data Protection and Freedom of Information on Blockchain Technology in the Context of Data Protection' [2017].
[353] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014) WP217 9.
[354] Article 29 Working Party has used 'publication of data for purposes of transparency and accountability' as an example of legitimate interest of third parties. In that example, public disclosure of data is considered necessary in certain situations for the interest of other stakeholders than controller including, for instance, employees or journalists, or the general public. While this does not perfectly fit into the context of blockchain, it shows that legitimate interest of third parties could be used as lawful basis when data is made public. Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 353) 27.

However, the availability of legitimate interest is not enough for the processing to be considered lawful, but instead, Article 6(1)(f) provides that such interest must override the interests and fundamental rights of the data subject. Legitimate interest is the only lawful basis that requires further balancing between the interest of the controller and the interests and fundamental rights and freedoms of the data subject to determine whether the basis applies. In general, the more important and compelling the interests of the controller or third party are, the more far-reaching impact the interest may have on the interests and fundamental rights of the data subject.[355] Berberich and Steiner have pointed out regarding the balancing test between policy interests and fundamental rights that the German Constitutional Court has recognised a 'right in the confidentiality and integrity of information technology systems' as a constitutional right. While it is not recognised as a fundamental right in the EU level, this shows that acknowledging the core functioning principle of technology under the legitimate interest of third parties is not a purely hypothetical scenario.[356]

In the balancing test, different additional safeguards which could 'prevent undue impact on data subjects' have a special role as one of the three key factors that should be considered when carrying out the balancing exercise.[357] Such additional safeguards include, *inter alia*, the use of anonymisation techniques such as encryption and pseudonymisation.[358] According to the opinion, important legitimate interests of the controller combined with additional safeguards could justify even a significant infringement or impact on data subjects' interests and fundamental rights.[359] On the one hand, blockchain applications often rely on pseudonymisation and encryption which could, if combined with the interest of the users, justify even a significant impact on the data subjects. On the other hand, the processing of personal data on blockchains would have a substantial impact on the data subjects' fundamental rights considering that the data subjects could not necessarily exercise their right to erasure. In any case, if blockchain technology is to be used for the processing of personal data by relying on the legitimate interest

[355] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 353) 30.
[356] Berberich and Steiner (n 48) 425.
[357] According to the Opinion 06/2014, other key factors that should be considered are 'the nature and source of the legitimate interest' and 'the impact on the data subjects'. Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 353) 50.
[358] Article 29 Working Party has noted that encryption and pseudonymisation do not automatically tip the balance in favour of controller, but implementing such measures affect the evaluation of the impact on the data subjects and could turn it to the advantage of the controller. Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 353) 42.
[359] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 353) 30.

of third parties as a lawful basis, the balancing test should be carried out to determine whether the legitimate interests of third parties override the interests and fundamental rights of the data subject in a particular case.

The GDPR provides data subjects with the right to contest the legitimate interest of a data controller under Article 21. According to Article 21, a data subject has the right to object to the processing of his or her personal data on grounds relating to his or her particular situation. Contrary to the DPD, Article 21 of the GDPR contains a reversed burden of proof. A data controller must be able to demonstrate that it has a compelling legitimate ground for the processing which overrides the interests and rights of the data subject.[360] The exercise of the right to object to the processing requires a similar balancing test than with Article 6(1)(f). However, Article 21(1) sets out an additional requirement, *i.e.,* the legitimate ground must be *compelling*. The GDPR does not entail any definition of the compelling legitimate ground. Article 29 Working Party has considered regarding profiling that the legitimate ground might be compelling when the processing (profiling in that case) is beneficial for society at large (or a broader community) and not just for the business interest of the controller.[361] Again, considering the potential of blockchain technology to boost new types of peer-to-peer applications, it could be argued that the processing of personal data in a particular blockchain application may be beneficial to such 'broader community'.

If a data controller cannot demonstrate a compelling legitimate ground for the processing, the processing must be interrupted.[362] According to Article 17(1)(c), a data subject has the right to request erasure of the data if he or she objects pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing. Article 17(1)(c) does not explicitly require compelling legitimate grounds, but it seems that exercising the right to erasure on the basis of the objection requires a successful objection under Article 21.[363] In order to lawfully refuse to accommodate with a data subject's request to erase data, a data controller should be able to demonstrate compelling legitimate grounds. Therefore, it could be argued that to process

[360] GDPR Article 21(1).
[361] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2016) WP251 25.
[362] GDPR Article 21(1).
[363] Jef Ausloos, 'The Interaction between the Rights to Object and to Erasure in the GDPR' (*KU Leuven Data Protection and Privacy Blog*, 25 August 2016) <www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/> accessed 3 September 2018.

personal data on blockchain data controller should be able to demonstrate *compelling* legitimate grounds, which override the interests and fundamental rights of the data subject if no other solution for the conflict between immutability and the right to erasure is available.

Nonetheless, even if the controller could demonstrate compelling legitimate grounds for the processing, that does not exempt the data controller from complying with data protection principles listed in Article 5.[364] Lawful processing of personal data requires not only lawful basis for the processing but also the data protection principles to be respected.[365] Article 17(1)(d) gives to a data subject a legal ground to obtain erasure if personal data have been processed unlawfully. It is for the data controller to prove that the processing of personal data has been lawful.[366] Blockchain technologies, however, are not necessarily in line with some of the data protection principles. The immutability of blockchains, the perpetual storage of data, and the difficulties in determining a responsible data controller might collide with the principles of data minimisation, storage limitation, and accountability.[367] Unfortunately, the scope of this research does not allow a more detailed examination of these issues. In any case, if the processing of personal data by particular blockchain application is considered unlawful because it is incompatible with some of the data protection principles, the data subject has a right to obtain erasure even if the data controller could demonstrate a compelling and overriding legitimate interest for the processing.

Above described interpretations of the legal grounds for erasure could provide room for refusing to accommodate data subject's request. However, it may well be contested whether these practices would be acceptable from the data subject's perspective. Data subjects should, at least, be educated about the risks related to the processing of personal on traditional blockchains. Even though traditional blockchains rely on encryption and pseudonymisation, an immutable and permanent database is a dangerous combination considering that even a high level of state-of-art encryption could be broken in the future, for instance, by quantum computers.[368] To sum up, the analysis of the legal grounds for erasure proved that it is important

[364] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (n 353) 11.
[365] De Hert and Papakonstantinou (n 89) 185.
[366] GDPR Article 5(2).
[367] More on the issues between blockchain technology and the data protection principles see eg Filippone (n 2) 31-34.
[368] Eichler and others (n 190) 4.

to consider the conflict between the right to erasure and immutability already when determining the lawful basis for the processing because the choice of a lawful basis could also affect to the obligation to erase in the future.

The technological solution proposed for the conflict

In addition to the above-mentioned legal solutions for reconciling the conflict between the right to erasure and the immutability of traditional blockchains, legal scholars have recognised the possibility to use a specific technological solution to help complying with the obligation to erase in the context of blockchain.[369] The promising technological solution is known as **chameleon-hashes**. The chameleon-hashes enable to give either to trusted third parties or several distrustful parties the capability to modify or erase data on old blocks without having to unbuild the whole blockchain before the modification. Ateniese and others have presented in their research the concept of redactable blockchain based on special chameleon-hashes which could be rather easily implemented to any traditional blockchains without a considerable computational overhead.[370] The chameleon-hashes differ from standard hashes used on blockchains as they include a 'digital trapdoor' that allows those who know the secret trapdoor key to modify or erase transactional data on an old block without invalidating the chain.[371] Once data on the old block is modified or erased, the new special blockchain is distributed to all other nodes on the network, who should then replace other versions of the blockchain with it.[372]

The redactable blockchains could offer particularly interesting solutions for the right to erasure because they allow giving the possibility to redact data on blocks for trusted third parties without compromising the operation of the blockchain. The blockchain itself would still run on the chosen consensus algorithm and transactions would be verified as usual. In such situations, the power to redact data on blockchains could be given to trusted third parties, such as arbitrators or data protection authorities. The ability to edit data on blocks could be reserved to trusted third parties, and for the 'bad actors', the blockchain would remain immutable.[373] If application providers would be considered as data controllers on traditional blockchains, the

[369] See eg Finck (n 13) 24; Ibáñez, O'Hara and Simperl (n 8) 8.
[370] Ateniese and others (n 333).
[371] Ateniese and others provide a proof-of-concept implementation of their redactable blockchain by implementing it on top of Bitcoin core. They represent how the integrity of the ledger could be maintained by using hash collision algorithm so that the hash of the new message is the same as the original (erased or modified) message. Ateniese and others (n 33) 124.
[372] Ateniese and others (n 333) 118.
[373] Ateniese and others (n 333) 113.

possibility of redacting blockchain could be given to them. This way the data controller could comply with the right to erasure in respect to transactional data. While this is a potential solution for compliance with the right to erasure, it reintroduces the need for trusted third parties and 'betrays the decentralisation principle' of traditional blockchains.

Ateniese and others, however, have presented also a decentralised application of their redactable blockchain in which the trapdoor key is either distributed to all full miners of the network (for blockchains with small number of participants) or secretly shared to a fixed set of chosen users, which could together modify or erase data on blocks by engaging in a multi-party computation.[374] As such, the possibility to edit data on old blocks could also be achieved in a truly decentralised way.

Some legal scholars have reviewed the possibilities to use chameleon-hashes for complying with the right to erasure on blockchains. Ibáñez, O'Hara and Simperl have taken quite an optimistic view of the chameleon-hashes by considering that state-of-art blockchain technologies must adopt chameleon-hashes.[375] On the other hand, Finck has taken a more critical approach to chameleon-hashes by pointing out that the chameleon-hashes come with many drawbacks.[376] Firstly, there is a risk that if the trapdoor key is lost, the blockchain will turn immutable again.[377] Further, this solution would still require other nodes to accept the modified 'special ledger', which is a question that should be addressed in an application-specific manner.[378] Thirdly, the use of chameleon-hashes to erase data on old blocks does not change the fact that old copies of the ledger, which contain the erased data, may still exist.[379] It should be reminded that the right to erasure does not contain de facto right to be forgotten on the internet. Instead, data controllers are obliged to take reasonable steps to inform other controllers that data subject has requested erasure of any links, copy or replication of the data.

The chameleon-hashes could provide an interesting solution for complying with the right to erasure on traditional blockchains. Thus, it should be further examined and explored how the

[374] Ateniese and others (n 333) 120.
[375] Ibáñez, O'Hara and Simperl (n 8) 8.
[376] Finck (n 13) 24.
[377] Ateniese and others (n 333) 112.
[378] Ateniese and others (n 333) 118.
[379] Ateniese and others (n 333) 114.

chameleon-hashes could be applied in practice to comply with the right to erasure. For instance, how the secret set of users, who can by collaborating modify old blocks, could together assess whether there is a legal ground for the right to erasure or whether the limitations of Article 17(3) would apply in a particular case? The redactable blockchains further presume that the redactions would not be carried out often, but instead only under exceptional circumstances, for instance, when inappropriate content containing child pornography or equivalent material is stored in the blockchain.[380] Many blockchain applications, however, process personal data on a constant basis (even though data might be hashed or encrypted). Data subjects have the right to request erasure of their personal data whenever their personal data is processed on a blockchain as long as there is a legal ground for the request. In such situations, the erasure might not be as exceptional measure as envisioned. In any case, the chameleon-hashes are an interesting technological solution that is worth examining in more detail with regard to compliance with the right to erasure.

Alternative interpretations of the erasure

Article 17 does not provide any explanation of the term 'erasure'. Legal scholars have argued that it is conceivable that erasure could be interpreted to mean something else than an outright deletion of data.[381] The ruling on the *Google Spain* case, although not concerning the right to erasure under the GDPR, seems to support a flexible interpretation. Instead of requiring deletion of the original data, the Court only required erasure of the links to the data from search results (delisting). Thus, the Court considered that reducing accessibility to the data by delisting could achieve the desired result.[382] On the other hand, the ruling on the *Nowak* case could imply a direction to a stricter interpretation of the erasure. In the *Nowak* case, the Court ruled on the right to obtain erasure under Article 12(b) of the DPD. The Court considered that the data subject had a right to have his school examination script 'erased, that is to say, destroyed'.[383] Despite the rulings, the exact meaning of the erasure remains uncertain, and there is still room for alternative interpretations under the GDPR. Moreover, while the GDPR is directly applicable in all Member States, the Member States may have some margin of discretion.[384]

[380] Ateniese and others (n 333) 112.
[381] Finck (n 13) 24.
[382] Ludo Gorzeman and Paulan Korenhof, 'Escaping the Panopticon Over Time: Balancing the Right To Be Forgotten and Freedom of Expression in a Technological Architecture' (2017) 30 Philosophy and Technology 73, 79.
[383] Case C-434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:994, para 55.
[384] According to Article 23 of the GDPR, Member States may impose further restrictions on the rights of data subjects as long as there is legal ground for the measure and the measure is proportionate and respects the essence of the fundamental rights and freedoms.

The German national data protection law contains a 'softer version' of the right to erasure, however, in relation to non-automated data processing.[385] While it remains to be seen whether it is considered to be in accordance with Article 17, it shows that alternative interpretations, which take into account the technical infeasibilities arising from the mode of storage, could be introduced.[386]

As an alternative solution to the outright deletion, some legal scholars have considered the possibility to use **sufficiently strong encryption** to obscure the data stored in blockchains, **and** then **destroy the decryption key**. In such a situation, the encrypted data would still exist on the blockchain, but the data could no longer be decrypted with the private key.[387] As in the *Google Spain* ruling, the data on the storage (here blockchain) would not be deleted, but access to the data is made infeasible.

The adequacy of the solution depends on what constitutes a sufficient level of encryption under the GDPR.[388] As discussed in Chapter 4.3, this question remains uncertain. For the time being, only guidance on the matter is the Article 29 Working Party Opinion on the anonymisation techniques from 2014. According to the opinion, an encryption cannot prevent identification of a data subject because the encrypted data could be restored to the original form, for instance, 'by applying the algorithm in the opposite way, or by brute force attacks, depending on the nature of the schemes, or as a result of a data breach'.[389] As Ibáñez, O'Hara and Simperl have noted, the opinion emphasises the existence of the decryption key and original data, '(f)or as long as the key or the original data are available (even in the case of a trusted third party, contractually bound to provide secure key escrow service), the possibility to identify a data subject is not eliminated'. Regarding the proposed solution, it would no longer be possible to decrypt the encrypted data with a private key, but the risk of brute force attacks still exists.[390]

The important question here is whether a data subject could be directly or indirectly identified from his or her public key by using a brute force attack. As discussed in Chapter 4.3, the GDPR

[385] Article 35 of the Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680.
[386] Finck (n 13) 25.
[387] Ibáñez, O'Hara and Simperl (n 8) 8.
[388] Ibáñez, O'Hara and Simperl (n 8) 8.
[389] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 146) 29.
[390] Ibáñez, O'Hara and Simperl (n 8) 9.

requires to take account of 'all the means reasonably likely to be used' to identify a natural person considering all objective factors, *inter alia*, 'the costs and amount of time required for identification and technological developments'.[391] State-of-art brute force attacks could not derive user's private key from the public key, but in a long-term, for instance, quantum computers could break the SHA 256-bit keys used in Bitcoin or Ethereum.[392] Considering the implementation costs, amount of time required, and available technology it seems that a brute force attack is beyond the means reasonably likely to be used to identify a natural person from the public key at the moment. However, taking account of potential technological developments, it is possible that quantum computers could break the public-key encryption in a long-term.

Legal scholars have not been unanimous of the sufficient level of encryption. Eichler and others have considered that due to the risk of future breaches, data should never be stored in encrypted form to the blockchain.[393] Article 29 Working Party has considered that the development of technology should be considered for 'the period for which the data will be processed', which seems to support the opinion of the Eichler and others because in traditional blockchains data is often processed for an unlimited period of time. Limiting the time for how long data are processed should be considered when developing traditional blockchain applications. Ibáñez, O'Hara and Simperl, on the other hand, have taken a more optimistic view by considering that state-of-art encryption provides a sufficient level of encryption. However, blockchain developers should follow technological advances, especially the development of quantum computers, in light of the risk of re-identification.[394] They consider that the destruction of the private key and original data could be interpreted to constitute erasure since the encrypted data is made unintelligible for anyone.[395] In other words, the encrypted data is rendered anonymous because it cannot identify a natural person by means reasonably likely to be used, and therefore the right to erase does no longer apply to such data.

[391] Recital 26 of the GDPR.
[392] As a good illustration of state-of-art brute force attacks against public keys it has been noted that, 'brute-force attacks against 256-bit keys will be infeasible until computers are built from something other than matter and occupy something other than space'. 'Couldn't Everybody Put in Random Private Keys, Look for a Balance, and Send to Their Own Address ?' (*MyEtherWallet FAQ*) < https://kb.myetherwallet.com/faq/couldnt-everybody-put-in-a-random-key-and-send-to-own-address.html> accessed 3 September 2018.
[393] Eichler and others (n 190) 4.
[394] Ibáñez, O'Hara and Simperl (n 8) 9.
[395] Ibáñez, O'Hara and Simperl (n 8) 12.

Here, an important question is who could enforce the right to erasure by destroying the private key. In an ideal situation, the users would create their own private keys and enforce the right to erasure by themselves. However, a common practice is that users rely on centralised or decentralised wallets for their key management. Centralised wallets do not provide users with full access to their private keys. Thus, these users should request the centralised wallets to erase their private keys. Decentralised wallets instead allow users to have full control over their private keys, and thus the users could enforce the right to erasure by themselves by destroying the private key.[396] This solution seems to put the onus on data subjects who could independently enforce the right to erasure by destroying the private key or possibly just by retaining the control over the private key.

Another alternative interpretation of the erasure relies on **hashing-out and deleting the off-chain data**. As mentioned in Chapter 4.3, blockchains could be used as 'decentralised verification machines', which store only hashes of the personal data.[397] The main idea of hashing-out is that instead of storing data directly on the blockchain, data could be stored on external off-chain storage while only hashes of the data would be stored on-chain. Hashing-out simplifies matters with regard to data protection significantly because data could be stored on a modifiable off-chain database under the control of a responsible data controller. Many legal scholars recognise the potential of hashing-out as a possible solution for traditional blockchains.[398] Finck has regarded it even as 'the most important step developers must take to ensure GDPR compliance'.[399]

Hashing-out enables that data could be modified and even erased from the off-chain storage without compromising the validity of blockchain because the hashes would still exist on-chain. Hashing-out would greatly help to exercise the right to erasure since the transactional data stored off-chain could be erased by data subject's request.[400] Nevertheless, a hash of the transactional data, which may constitute personal data, remains on-chain and the problem regarding the right to erasure may exist. Eichler and others have considered that when off-chain

[396] Tasos Kakouris, 'Decentralized Wallets : A Need & a Hurdle' (*Medium*, 11 June 2018) <https://medium.com/@tasoskakouris/decentralized-wallets-a-need-a-hurdle-486d3c57b1a9> accessed 17 September 2018.
[397] Ibáñez, O'Hara and Simperl (n 8) 12.
[398] See eg Ibáñez, O'Hara and Simperl (n 8) 8; Eichler and others (n 190) 8; Salmon and Maxwell (n 7) 16.
[399] Finck (n 13) 12.
[400] Ibáñez, O'Hara and Simperl (n 8) 8.

data is erased, and the original off-chain data cannot be easily retrieved from the hash, there would not necessarily be a conflict with the right to erasure. The original data would be erased, and the on-chain hash could be considered anonymous because identification on the basis of the hash could be considered as means which are beyond what is reasonably likely to be used to identify an individual.[401]

However, hashing-out often requires re-introduction of a trusted third party, which is in a total contradiction with the purpose of traditional blockchains to eliminate the need for trusted middle-men.[402] Betrayal of the decentralisation principle is not necessarily an unavoidable problem. Eberhardt and Tai have presented on their research different patterns for moving computation and data off-chain while preserving one of the main features of traditional blockchains – the trustlessness.[403] Although the purpose of their research was primarily to examine the current state of the off-chain solutions in order to resolve functionality and storage cost issues relating to on-chain operations, these patterns are also potential from the data protection perspective.[404] The most potential pattern for reconciling the conflict between the right to erasure and immutability seems to be the content addressable storage. It could allow storing only hashes of the data on-chain without relying on a centralised intermediary for storing the off-chain data.[405] However, instead of relying on centralised intermediaries, the pattern relies on distributed peer-to-peer off-chain storages, such as InterPlanetary File System (IPFS) or Swarm, which are permanent or immutable in the sense that a user cannot force other nodes hosting the off-chain data to erase it.[406] Therefore, the conflict between immutability and the right to erasure seems to remain in a truly decentralised version of the hashing-out.

Another interesting alternative interpretation of the term erasure, which could provide a solution for the conflict between immutability and the right to erasure, concerns **access authorisation systems**. As mentioned in Chapter 4.2, it has been widely recognised that blockchain

---

[401] Eichler and others (n 190) 8.
[402] Ibáñez, O'Hara and Simperl (n 8) 8.
[403] These off-chaining patterns include challenge response, off-chain signatures, content-addressable storage, delegated computation, and low contract footprint patterns. Jacob Eberhardt and Stefan Tai, 'On or off the Blockchain? Insights on off-Chaining Computation and Data' in Flavio De Paoli, Stefan Schulte and Einar Broch Johnsen (eds), *Service-Oriented and Cloud Computing - 2017* (Springer, 2017) 3.
[404] Finck (n 13) 12.
[405] Eberhardt and Tai (n 403) 9.
[406] Eberhardt and Tai (n 403) 9; 'Can I Delete My Content from the Network? # 9' (*IPFS FAQ)* <https://github.com/ipfs/faq/issues/9|> accessed 18 September 2018; '1 Introduction' (*Swarm Guide*) <https://swarm-guide.readthedocs.io/en/latest/introduction.html> accessed 18 September 2018.

technology could be used to develop advanced access authorisation systems that allow individuals to have true control over their personal data. These solutions could be built on top of blockchain applications so that only the users manage and control their data.[407] The users could decide who can access the data and keep track of data controllers or processors accessing and using the data. Moreover, these solutions could provide data controllers with a convenient way to prove that their processing is based on the data subject's consent.[408]

The data subject could exercise the right to erasure by **disabling access** to the data from any party the data subject has previously given access to the data. The data is not erased from the storage but rather the access to the data is disabled from other parties. Salmensuu has argued that it is conceivable that regulators would accept disabling access to the data as an alternative solution for outright deletion considering the potential of these solutions to provide individuals with the true control over their personal data.[409] However, withdrawing consent would only make the data inaccessible from that moment on while all old data would stay recorded, which speaks against disabling access as an alternative solution for an outright deletion.[410]

Regarding transactional data stored and processed on traditional blockchains, above described alternative interpretations of the erasure could provide solutions for reconciling the conflict between immutability of traditional blockchains and the right to erasure. Nevertheless, these solutions cannot provide a solution for erasing public keys, which are an essential feature of any traditional blockchain application. The public key and the transaction history would still be available on the ledger. As discussed in Chapter 4.3, public keys constitute personal data under the GDPR in many cases. Thus, the conflict between the right to erasure and immutability of traditional blockchains persists. The public keys are much more problematic regarding the right to erasure because they cannot be erased or stored off-chain as the public keys are crucial for validating transactions on blockchains.[411] Here, the question of anonymisation arises again. Anonymisation of public keys would be the most effective solution for complying with the right to erasure in traditional blockchains. Data subjects should not rely on third parties for their key management in order to avoid situations similar to the *Breyer* case. Further, developers have

[407] Salmensuu (n 172) 23.
[408] Neisse, Steri and Nai-Fovino (n 133) 1.
[409] Salmensuu (n 172) 115.
[410] Neisse, Steri and Nai-Fovino (n 133) 7.
[411] Finck (n 13) 14.

already found ways to validate transactions on blockchains without concealing the public keys or the content of the transactions to the validators.[412] While these solutions may not be ready for widespread implementation, the rapid development of technology could provide solutions in the future.

5.3 Taking a review of the current state of play and a look into the future

5.3.1 Assessing the current situation of the conflict

Previous Chapters 5.1 and 5.2 examined the content of the right to erasure, established that there is a conflict between Article 17 and immutable blockchains, and analysed different solutions proposed for reconciling the conflict. In light of the above, it is time to assess the current state of play. The conflict between the right to erasure and the immutability of traditional blockchains has been well recognised in both legal and blockchain communities. However, very few commentators have gone further to research how to resolve the various issues between blockchain technology and data protection.[413] At the moment many blockchain projects, which are specifically designed to process personal data or allow processing of any type of data risk violating Article 17 of the GDPR because there is no clear and convenient way to erase personal data by a request. A closer look into the different solutions proposed to reconcile the conflict between the immutability of traditional blockchains and the right to erasure, however, reveals that the conflict may not be as insurmountable as it prima facie seems.

Firstly, the right to erasure is not an absolute right, but instead, the data subject must have a legal ground for his or her request. Some legal scholars have proposed flexible interpretations of the legal grounds. The flexible interpretations could allow taking account of the specific features of blockchain technology and turning down the data subject's request in certain circumstances.[414] For instance, the core functioning principle of technology could be regarded

[412] For example, zero-knowledge proofs have been considered as potential for concealing the public keys and transaction amounts. More on the technological solutions discussed for anonymising data on blockchains see Chapter 4.3.3 Table of different technological solutions providing more privacy for individuals making transactions in blockchain network.
[413] Christopher Kuner and others, 'Blockchain versus Data Protection' (2018) 8 International Data Privacy Law 103, 104.
[414] Berberich and Steiner (n 48) 426; Ibáñez, O'Hara and Simperl (n 8) 4.

as an 'other legal ground' under the Article 17(1)(b), or personal data could be considered necessary for the processing due to the immutability of blockchains.[415] The legal grounds for the right to erasure are closely connected to the lawful bases for the processing under Article 6 of the GDPR. Blockchain developers should carefully assess the lawful basis for the processing already in the design phase. Choosing consent or legitimate interest of third parties as the lawful basis for the processing could provide a way to refuse accommodating data subject's request of erasure. It remains to be seen whether any of these arguments could hold in courts.

In addition to purely legal solutions, the technological community has presented an interesting solution that could help to comply with the right to erasure on traditional blockchains. Blockchain developers have presented a concept of redactable blockchains, which enable to modify or erase data on old blocks in a convenient way without invalidating the blockchain and causing a considerable computational overhead.[416] While implementing chameleon-hashes to traditional blockchains seems an attractive option from a data protection perspective, further research on how chameleon-hashes could be used in practice to comply with the right to erasure seems necessary.

The third possible solution for the conflict relies on the interpretation of the term 'erasure'. Legal scholars have noted that the erasure is not defined in the GDPR, which could provide room for alternative interpretations to outright deletion.[417] There are different interpretations of the erasure for different use case scenarios of traditional blockchains. When traditional blockchains are used as decentralised verification machines (only hashes of the personal data are stored on-chain), it is conceivable that making data unintelligible for anyone by destroying the off-chain data and possible salt could constitute erasure under Article 17. Similarly, when processing of personal data is carried out by smart contracts, destroying the encryption key and original data could be regarded as an alternative implementation of the erasure.[418] Third alternative implementation could be available when access authentication systems are built on top of traditional blockchain applications. The data subject could exercise control over his or her personal data and independently enforce the right to erasure by disabling access to the

[415] Berberich and Steiner (n 48) 426.
[416] Ateniese and others (n 333).
[417] Finck (n 13) 25.
[418] Ibáñez, O'Hara and Simperl (n 8) 12.

data.[419] These alternative interpretations of the erasure are particularly interesting because they enable to respond to data subjects' requests in traditional blockchains without compromising immutability. Therefore, if flexible interpretations of the erasure would be accepted, both data protection and blockchain communities could be satisfied.

While the above-described solutions could help to comply with the right to erasure with respect to transactional data, in many cases, the problem exists in relation to the public keys. The transactional data stored on blockchains is often linked to a particular public key, which must be publicly available to enable validators to verify transactions. When relying on alternative interpretations of the erasure, only a transactional data stored inside the block is made unintelligible. Public keys would still be visible on the blockchain.[420] The most obvious solution for the issue of erasing public keys would be the anonymisation of public keys.[421] The question remains open whether public keys could be anonymised data with advanced anonymisation techniques.[422] The question of public keys and anonymisation should be carefully considered when developing new blockchain applications because compliance with the right to erasure could be even more problematic with public keys than transactional data.

Blockchain applications that allow processing any type of data or which are specifically designed to process personal data currently run the risk of infringing Article 17, although the different solutions analysed above could help to comply with the right to erasure. Traditional blockchains applications could face heavy sanctions set out in Article 83 of the GDPR. Infringement of Article 17 is one of the infringements that could trigger the most aggravated administrative fines of the regulation, 'administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher'.[423] Even though the question concerning allocation of responsibilities on blockchains, and thus who could face the administrative fines remains open, these heavy sanctions combined with the legal uncertainty in relation to the conflict between the right to erasure and traditional blockchains may deter investors and blockchain developers from designing new blockchain applications and possibly individuals from using those

[419] Salmensuu (n 172) 114.
[420] Finck (n 13) 14.
[421] Finck (n 13) 16.
[422] Finck (n 13) 16.
[423] GDPR Article 83(5)(b).

applications. Therefore, there is a need for guidance that could provide answers to these questions and legal certainty for all the stakeholders.

5.3.2 Building a bridge between the GDPR and blockchain technology

There are many uncertainties and open questions that require further research. In order to reconcile the conflict between the immutability of traditional blockchains and the right to erasure under Article 17 of the GDPR, it is important to identify the relevant questions that should be addressed. From a legal perspective, the first and most essential question concerns the anonymisation. What would be a sufficient level of encryption or hashing that could render data anonymous under the GDPR? Anonymisation could provide a solution especially to issues arising from the transparency of metadata (public keys). Many legal scholars have argued that the high threshold for anonymisation set out by Article 29 Working Party should be revised.[424] Anonymisation would the most obvious and efficient solution for the issues between the regulation and blockchain technology. While advanced anonymisation techniques may offer extremely high level of privacy for individuals, the development of quantum computers could threaten these solutions in the future.[425] Considering that often data is stored on blockchains for an unlimited period, any possibility to break the encryption in the future should be taken seriously, especially when personal data is concerned. Therefore, attention should be paid also to how long the data is to be processed on blockchains.

Another essential question concerns the allocation of responsibilities in traditional blockchains. Who should be responsible for the processing of personal data on blockchains? Considering nodes and miners as data controllers or joint controllers would lead to enforcement difficulties because they could not respond to the tasks of data controllers under the GDPR.[426] However, the chameleon-hashes could provide a way to comply with the right to erasure in such decentralised peer-to-peer networks by relying on secret sharing schemes, where certain chosen parties are responsible for redacting blockchain.[427] Some have argued that when blockchain is used for direct interaction between individuals, it is not possible to find a responsible data controller at all. Nodes and miners should instead be considered as infrastructure, and the

[424] El Emam and Álvarez (n 173) 76; Stalla-Bourdillon and Knight (n 175) 307.
[425] Eichler and others (n 190) 8.
[426] Finck (n 13) 17.
[427] Ateniese and others (n 333) 118.

responsibility over the personal data should be shifted to the data subjects.[428] Shifting responsibility over the personal data to data subjects would require educating the data subjects of the risks related to processing of personal data on blockchain applications. When personal data are processed in smart contract platforms, responsibility could be allocated to the owners of the blockchain application, which relies on traditional blockchain as a backend. In such a scenario, nodes and miners could be considered as data processors, which would, in turn, result in the obligation to conclude data processing agreements with all the nodes and miners of the blockchain network. This obligation would be difficult to enforce in practice, which has been regarded by some scholars as a sign that nodes and miners should be considered as infrastructure in all scenarios.[429]

As regards to allocation of responsibilities in light of enforcing the right to erasure, it seems that considering nodes and miners as separate data controllers or joint controllers would not be recommendable because they cannot independently erase data by a request. Achieving a majority of the nodes to agree with the erasure would not be a practical solution due to a large number of participants. The chameleon-hashes could enable a decentralised way to enforce the right by giving the power to redact blockchain to a secret set of users. Further, if the owners of blockchain application are considered as data controllers, the chameleon-hashes could be used to empower them to erase data from the blockchain. The third option would be to consider users as both data controllers and data subjects at the same time. The users could enforce the right to erasure independently by relying on alternative means of erasure, for instance, by destroying the private key and original data or by disabling access to the data. Allocation of responsibilities is not an easy task on traditional blockchain networks but all the more important in respect to compliance with the right to erasure.

The solutions proposed to reconcile the conflict between the right to erasure and the immutability of traditional blockchains are based on flexible interpretations. It remains to be seen whether courts and authorities could approve the flexible interpretations of the legal grounds for erasure. Similarly, the legitimacy of the alternative means of erasure depends on how the term erasure will be interpreted by courts and authorities. The third uncertain element of Article 17 concerns the obligation to inform other controllers, the actual right to be

[428] Eichler and others (n 190) 6; Ibáñez, O'Hara and Simperl (n 8) 10.
[429] Eichler and others (n 190) 6.

'forgotten' provision, and how courts will enforce it. Even though Article 17 provides rather detailed and precise right to erasure, the actual scope of the right will be shaped by future interpretations.

Some of the questions identified above require blockchain-specific responses. Guidance on the matters could be delivered by data protection authorities, such as national DPAs, the EDPB, and the EDPS. In addition, the Commission has established the EU Blockchain Observatory and Forum, which is currently researching the issues between blockchain and the GDPR. Some questions might require even more detailed and specific answers for which the GDPR offers certain soft law instruments. Approved certification mechanisms under Article 42 could prove to be a practical way of providing legal certainty for more specific questions.[430] Approved codes of conducts under Article 40 could, in turn, provide case-specific guidance on the industry level.[431]

While guidance may be provided either by hard law or soft law instruments, it is likely that some of the questions will be answered by courts of the Member States and the Court. Not all questions require blockchain-specific answers, but instead, for instance, the questions about the threshold of anonymisation or the interpretation of the 'erasure' may be answered within another context than blockchain. The blockchain technology is not alone with the problems regarding the GDPR. For instance, similar issues have arisen in relation to big data and machine learning.[432] In addition to keeping an eye on the different interpretations of the concepts and terms of the GDPR, other conflicts between blockchain technology and the GDPR, especially with respect to data protection principles, should be carefully followed. If processing of personal data on a specific traditional blockchain application is in infringement with some of the data protection principles, and therefore the processing is considered unlawful, data subject will have a legal ground to request erasure regardless of the possible consent or legitimate interest of third parties for the processing.

[430] Wirth and Kolain (n 268).
[431] De Hert and Papakonstantinou (n 89) 192.
[432] Tal Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47(4) Seton Hall Law Review 995; Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 Computer Law and Security Review 304.

Identifying relevant legal questions and addressing them is essential for reconciling the conflict between the right to erasure and the immutability of traditional blockchains. In addition to the legal approach, the technology itself could provide solutions for the conflict in the future. Further advances in the anonymisation techniques, the chameleon-hashes, or the blockchain-based access authorisation systems could help to comply with the right to erasure and other data subjects' rights. The best way to achieve compliance with the GDPR is to consider data protection issues already in the design phase of blockchain projects. The EDPS has emphasised this view by recommending developers to build privacy-friendly blockchains which are in line with the principle of data protection by design.[433] So far, most of the technological attempts have focused on providing more privacy to individuals using blockchain applications. While improving privacy is certainly beneficial also for users' data protection, more attention should be explicitly paid to data protection compliance on traditional blockchains.[434] On the other hand, the rapid development of technology might bring new data protection issues, for instance, quantum computers could break even high-level encryption. Blockchain developers should follow these advancements in technology and prepare solutions also for the emerging issues.[435]

Considering that blockchain technology is widely recognised as an innovative and extremely potential technology, the fact that blockchain technology could provide individuals with the 'true control' over their personal data and enable new alternative means to achieve the objects of the GDPR[436], and the fact that the GDPR was not drafted taking into account blockchain technologies, there seems to be room for an flexible approach for the problems between the regulation and blockchain technology. A simple solution for the problems would be to change or reform the GDPR, which, however, is not likely to happen because changing the regulation would be very lengthy and laborious process, and even after such reform, the regulation would likely be outdated again.[437] A general exception for blockchain technology seems just as unlikely scenario as the reform because the GDPR expressly states that the data protection of individuals should be technologically neutral.[438] Most likely the GDPR will apply to blockchain applications that process personal data, and hopefully, the GDPR will be interpreted in a flexible manner taking into consideration specific properties of the technology. It is important to notice that the flexible interpretations require that blockchain projects are by design developed

[433] European Data Protection Supervisor (n 280) 43.
[434] Ibáñez, O'Hara and Simperl (n 8) 7.
[435] Ibáñez, O'Hara and Simperl (n 8) 12.
[436] Finck (n 13) 29.
[437] Villaronga, Kieseberg and Li (n 433) 312.
[438] Recital 15 of the GDPR.

considering compliance with data protection obligations. This research has focused on building a bridge between the GDPR and traditional blockchains by identifying legal questions, especially in relation to the conflict between the right to erasure and the immutability of traditional blockchain technology, which could be addressed with flexible interpretations that enable compliance with the right to erasure. In order to enable peaceful coexistence of the regulation and the blockchain technology in the future, it is recommendable that data protection and technological experts cooperate to find solutions for designing privacy-friendly blockchain applications that allow further development of traditional blockchains without causing an undue impact on data subjects.[439]

6. Conclusions

It is a common phenomenon that regulation is one step behind innovations and advancing technologies. The blockchain technology is a prime example of this phenomenon. Trying to apply different data protection rights and obligations of the GDPR to the traditional blockchain technology is not an easy task. Essentially, reconciling tensions between the regulation and the technology is about finding a balance between the data protection of individuals and the promotion of innovation. Even though the right to data protection is a fundamental right and must be respected accordingly, it should not ride roughshod over the promotion of innovation. Promotion of innovation is a normative objective of the EU. [440] Creation of the Innovation Union as part of the Europe 2020 strategy for smart, sustainable and inclusive growth reflects the importance of fostering research and innovation in the Union. Establishment of the EU Blockchain Observatory and Forum is, in turn, a clear sign that the Commission has recognised the potential of blockchain technology. Both interests are worth protecting. Therefore, it is necessary to examine how to find a balance between law and technology – between the GDPR and the traditional blockchain technology.

The focus of this research has been especially on the conflict between 'immutable' traditional blockchains and the right to erasure under Article 17 of the GDPR. Before going deeper into the main issue, this research addressed two essential preliminary questions to give a proper

[439] Finck (n 13) 29.
[440] Finck (n 13) 29.

understanding of the main issue. The question about anonymisation and personal data on blockchains, on the one hand, determines whether the GDPR and its obligations apply to a specific blockchain application at all. On the other hand, anonymisation of personal data could be the most effective solution also for the conflict between the immutability and the right to erasure. This research notes that not all blockchain applications process personal data, but many traditional blockchain applications revolve around transactions between individuals. Blockchain applications which allow storing any type of data to the blockchain and applications which are specially developed to process personal data trigger in many cases the application of the GDPR even though the applications rely on pseudonymisation and encryption to provide more privacy for the individuals transacting. The threshold for anonymisation is currently very high, but hopefully, the near zero-risk requirement is reconsidered soon.

The question about allocation of responsibilities on traditional blockchain networks is another relevant question because it addresses who should be responsible for enforcing data subjects' right to erasure and from whom the data subjects should request the erasure. Allocation of responsibilities is an illustrative example of the difficulties applying the GDPR to the blockchain technology. This research reviewed different possibilities to allocate responsibility on traditional blockchains. In respect to enforcing the right to erasure on traditional blockchains, two most suitable approaches are to develop further and implement chameleon-hashes or to shift the responsibility for enforcing the right to data subjects, who could enforce the right independently by relying on alternative means of erasure.

The first conclusion of this research concerns the current situation of the conflict between the immutability and the right to erasure. Processing personal data on traditional blockchain applications is currently likely to infringe the right to erasure under Article 17, even though there are different solutions proposed for compliance. Alternative interpretations of the right to erasure could provide a solution for erasing transactional data. However, in many cases the problem exists in relation to public keys. If traditional blockchain application infringes Article 17, it could face heavy administrative fines. The legal uncertainty is a significant impediment to the development and implementation of traditional blockchains at the moment.

The second conclusion is about how to address the conflict in the future. This research balances between the data protection of individuals and the promotion of innovation and argues that the GDPR should not prevent the development of blockchain technology considering the widely recognised potential of blockchain technology, the fact that the GDPR was not drafted taking into account blockchain technology, and the fact that blockchains may also provide new ways to give individuals more control over their data and to achieve objectives of the GDPR. As discussed in the Introduction, this research relies on law and economics approach, and, in particular, on normative economic analysis of law. According to so-called Kaldor-Hicks efficiency, there is a need for change if it is possible to increase 'the total welfare of a society' by creating enough benefits for some individuals while compensating the loss caused to other individuals.[441] This research argues that there is a need for change because, if traditional blockchains are designed taking account of data protection obligations and principles, the loss caused to individuals' data protection could be so insignificant that the benefits of the technology to individuals could compensate that loss. The change is not about anything drastic, such as reforming the GDPR or enacting a new blockchain-specific law, but instead, when blockchain applications are designed to be data protection and privacy-friendly, traditional blockchains could comply with the GDPR if the provisions are interpreted in a flexible manner. This research has identified relevant legal questions regarding the main conflict. These questions should be addressed to provide legal certainty for all the stakeholders in the blockchain ecosystem. This thesis ha alsos proposed how to reconcile the main conflict by providing flexible interpretations that could enable traditional blockchain applications to comply with the right to erasure.

It is worth emphasising that traditional blockchain applications are still immature and far from being widely implemented, even though Bitcoin and other cryptocurrencies have reached a large group of users. Most of the traditional blockchain projects are still in a trial or pilot phase.[442] The issues about data protection and privacy are not the only bottlenecks, but the issues concerning, for instance, scalability and security are also hindering widespread implementation of the technology. That does not mean that it is too early to research and discuss the data protection issues concerning traditional blockchains. On the contrary, this is a perfect time for this discussion because it is still possible to affect the development of the technology.

[441] Pacces and Visscher (n 15) 89.
[442] Michel Rauchs and others, 'Distributed Ledger Systems: A Conceptual Framework' (Cambridge Centre for Alternative Finance 2018) <https://ssrn.com/abstract=3230013> accessed 19 September 2018.

The discussion should focus on both identifying and addressing the issues. At the heart of the issues is the fact that the GDPR was not written considering the decentralised approach of traditional blockchains. Thus, reconciling the issues requires a new and more flexible way of thinking. To quote one of the most influential physicists of the 20th century, Albert Einstein, '(t)he significant problems we face cannot be solved at the same level of thinking we were at when we created them.'