MIPLC Studies 35

Shraddha Kulhari

Building-Blocks of a Data Protection Revolution

The Uneasy Case for Blockchain Technology to Secure Privacy and Identity

Nomos

MIPLC Munich Intellectual Property Law Center
Augsburg München Washington DC

MIPLC Studies
Edited by

Volume 35

Shraddha Kulhari

Building-Blocks of a Data Protection Revolution

The Uneasy Case for Blockchain Technology to Secure Privacy and Identity

Nomos

MIPLC Munich Intellectual Property Law Center
Augsburg München Washington DC

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

a.t.: Munich, Master Thesis Munich Intellectual Property Law Center, 2017

ISBN 978-3-8487-5222-5 (Print)
978-3-8452-9402-5 (ePDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-3-8487-5222-5 (Print)
978-3-8452-9402-5 (ePDF)

Library of Congress Cataloging-in-Publication Data
Kulhari, Shraddha
Building-Blocks of a Data Protection Revolution
The Uneasy Case for Blockchain Technology to Secure Privacy and Identity
Shraddha Kulhari
62 p.
Includes bibliographic references.

ISBN 978-3-8487-5222-5 (Print)
978-3-8452-9402-5 (ePDF)

1st Edition 2018

Table of Contents

Abstract

The General Data Protection Regulation (GDPR) replaced the old and battered Data Protection Directive on 25 May 2018 after a long-drawn reform. The rapidly evolving technological landscape will test the ability of the GDPR to effectively achieve the goals of protecting personal data and free movement of data. This thesis proposes a technological supplement to achieve the goal of data protection as enshrined in the GDPR. The proposal comes in the form of digital identity management platforms built on blockchain technology. Such digital identity management platforms enhance the personal autonomy and control of individuals over their identities. This is important in light of heightened profiling activity. However, the very structure of blockchain poses some significant challenges in terms of compatibility with the GDPR. In light of these challenges, the claim of GDPR being a technologically neutral legislation is analysed. Further, the thesis attempts to assess compatibility issues of a blockchain based digital identity management solution on the parameters of data protection principles like accountability, data minimisation, control and data protection by design in conjunction with the right to be forgotten and right to data portability.

Acronyms and Abbreviations

AmI	Ambient Intelligence
Art	Article
CJEU	Court of Justice of the European Union
DIM	Digital Identity Management
DPD	Data Protection Directive 95/46/EC
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ESOs	European Standardisation Organisations
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
GB	Giga Byte
GDPR	General Data Protection Regulation (EU) 2016/679
IP	Internet Protocol
IoT	Internet of Things
MIT	Massachusetts Institute of Technology
TCP	Transmission Control Protocol
WEF	World Economic Forum

I. Introduction

We live in exciting times, where autonomous cars, smart homes and virtual currencies are not merely a creative scriptwriter's plot for an upcoming science fiction movie. These are real life manifestations of human effort, where erstwhile boundaries are being pushed to convert imagination to innovation. Much like any other form of progress, these developments are not happening in a vacuum. This engine of innovation is fuelled by data. According to a white paper by International Data Corporation, the *global datasphere*, i.e., the data created and copied annually, will reach a whopping 163 trillion gigabytes by 2025.[1] To put things into perspective, another study envisages that if the 44 trillion gigabytes were represented by the memory in a stack of iPad Air tablets (each 0.29" thick, having memory of 128 GB), there would be 6.6 such stacks from the Earth to the Moon.[2] While the simple, albeit over-simplified, assumption might be that much of this data would seemingly be impersonal, however in the context of modern data science Princeton University computer scientist Arvind Narayanan claims that the richness of data makes pinpointing people "algorithmically possible". This takes us to the conclusion that the more data there is out there, the less any of it can be said to be private.[3]

In light of the challenges posed by uneven harmonization and the fast pace of technological developments, the twin goals of data protection and free movement of data were falling through the cracks in the erstwhile Data Protection Directive 95/46/EC (DPD) regime. According to the Special Eurobarometer 2015, as many as 89% of surveyed Europeans acknowledged the importance of having the same rights over their personal infor-

1 David Reinsel, John Gantz and John Rydning, 'Data Age 2025: The Evolution of Data to Life-Critical' (April 2017) <www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf> accessed 27 August 2017.

2 Vernon Turner, 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things' (April 2014) <www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm> accessed 27 August 2017.

3 Patrick Tucker, 'Has Big Data made Anonymity Impossible?' MIT Technology Review - Business Report (7 May 2013) <www.technologyreview.com/s/514351/has-big-data-made-anonymity-impossible/?set=514341> accessed 27 August 2017.

mation, irrespective of the EU country in which it is collected and processed.[4] Moreover, the fact that 85% of the same people felt that they did not have complete control over the information they provided online pointed to the failure of DPD in inspiring trust.[5] It is in this context that the data protection ecosystem in Europe went through long-drawn reform eventually leading to the General Data Protection Regulation (GDPR).[6] The GDPR has replaced the DPD as of 25 May 2018, when it became directly applicable in each Member State of the EU amidst expectations of leading to a greater degree of harmonization in the realm of data protection across the EU countries. However, it is still to be seen how well the GDPR juxtaposes itself in the general landscape of data protection, most importantly how it integrates itself in a dynamic technological environment where the manner and rate at which data is processed is phenomenal.

Advances in the technology of storage and processing of personal data pose significant challenges for ensuring informational self-determination to data subjects. In line with Moore's law, sustained improvements in microprocessor technology have made the integration of digital features into everyday objects a reality that we today know as the Internet of Things (IoT).[7] This rapid progress is alarming because the highly connected nature of these 'things' makes profiling individuals a cakewalk.[8] It is a threat to their very identity and right to privacy. Red flags are being raised in data protection circles because data subjects are unable to have control over

4 TNS Opinion & Social, 'Data Protection' Special Eurobarometer 431 (June 2011) 10 <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf> accessed 27 August 2017.

5 ibid 4.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> accessed 27 August 2017.

7 Moore's Law is a computing term which originated around 1970; the simplified version of this law states that processor speeds, or overall processing power for computers will double every two years. < http://www.mooreslaw.org/> accessed 27 August 2017.

8 Gartner Inc. had estimated that 4 billion connected things would be in use in consumer sector in 2016, set to rise to 13.5 billion by 2020.
Gartner Press Release, 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015' (Stamford, 10 November 2015) <www.gartner.com/newsroom/id/3165317> accessed 27 August 2017.

their own personal data. The threat to personal autonomy and identity of an individual has fuelled new approaches to rescue one's identity from drowning in the data deluge. With the reputation blockchain technology has garnered for itself in the short span of a decade, it posits itself as a possible solution to protecting personal data. A solution modelled on blockchain technology holds the promise of returning control to the data subject of her personal data and the ability to maintain the sanctity of her identity in the digital realm.

Thus, the research question that this thesis seeks to address is as under:

> Does the GDPR provide a conducive framework for a blockchain based digital identity management solution?

Answering this question calls for a techno-legal approach and entails a host of sub-questions. Before proposing a structure for the thesis, it is beneficial to list these sub-questions here:

- How is blockchain technology better placed to secure personal data protection?
- What is the relationship between right to privacy and right to data protection?
- Where does the concept of identity find itself in the discussion of privacy and data protection?
- Does the GDPR provide for safeguarding the data subject's identity?
- How is a digital identity management solution based on blockchain better than the existing means of identity management?
- Is the GDPR a technology neutral law?
- Does the GDPR, by itself, have the wherewithal to return control over personal data to the data subjects?
- Are all the principles of data protection in the GDPR to be accorded the same status?
- Is legitimate interest test an all-encompassing test?
- Is there an inherent contradiction between the goal of data protection by design and the other principles of the GDPR, especially in the context of blockchain technology?
- What are the suggested changes/interpretation to the GDPR?

At the outset, since the research question pertains to the compatibility of blockchain technology with the GDPR, it is imperative to introduce blockchain technology. The second chapter of this thesis attempts to put forth a simplified yet comprehensive description of all the essential concepts underlying blockchain technology. The chapter also discusses a

decentralized model for personal data protection built on blockchain. The third chapter deliberates on the nature of the relationship between right to privacy and right to data protection. It has been suggested that the only way to keep up with fast evolving data processing technologies is to ensure that the data subject has control over her personal data.[9] The notion of control emerges from the idea of enhancing autonomy of the data subject, germinating from the German doctrine of informational self-determination.[10] It appears that this right to informational self-determination integrates well with the aim of safeguarding one's identity and forms the basis for control of personal boundaries.[11] The discourse on privacy, data protection and identity leads to another essential concept from the research question –digital identity management. This is crucial in the era of the Web 2.0 and the Internet of Things (IoT), where profiling individuals is the backbone of their functionality and makes encroachments on the right to identity. Last part of the third chapter justifies the need for digital identity management in general and building this on a blockchain in particular. The fourth and most important chapter seeks to round up all the issues that may confront a blockchain-based solution of digital identity management in light of the GDPR. This chapter is crucial as it puts to test the claim that the GDPR is a technologically neutral legislation. It is also the right stage to question the applicability of new principles like right to be forgotten, right to data portability and data protection by design in the face of new technologies. Although this analysis comes in the nascency of GDPR, it presents a good opportunity to have an insight into the future of GDPR and its technological elasticity. The thesis concludes with a review of the obstacles and challenges expected to be faced by the GDPR on its way to realising the purpose of its promulgation, and how far blockchain technology is capable of assisting in this uphill task.

9 Scott R. Peppet, 'Unraveling privacy: The Personal Prospectus and the Threat of a Full-disclosure Future.' (2011) 105 Northwestern University Law Review 1153, 1183.

10 Volkszählungsurteil, BVerfGE Bd. 65, 1.

11 Irwin Altman, 'Privacy: A Conceptual Analysis' (1976) 8 Environment and Behavior 7-29. Altman conceives privacy as a "boundary control process"; the selective control over access to oneself.

II. The Midas touch of Blockchain: Leveraging it for Data Protection

A. Easing into the Blockchain enigma

Before we jump in to the rabbit hole that is the relationship between blockchain and the GDPR, a brief explanation of the technology is imperative. Although hailed as the disruptive technology of this century, Marco Iansiti and Karim Lakhani refer to blockchain technology as a 'foundational' model.[12] They explain that blockchain does not offer a truly 'disruptive' model in the sense that it is not capable of undercutting an existing model with a low-cost solution; rather it resonates better as a 'foundational' model by creating new foundations for social and economic purposes.[13] Drawing parallels with the adoption of TCP/IP - the distributed computer networking technology that established the foundation for the Internet - Iansiti and Lakhani highlight that it took more than 30 years to put the transformative potential of TCP/IP to use.[14] However, studies like the annual Gartner Hype Cycle (which ascertains the promise of emerging technologies) not only includes but showcases blockchain amongst the technologies capable of delivering a high degree of competitive advantage in the coming five to ten years.[15]

The broad range of applications that blockchain is presently being put to is testament to this optimistic projection. From its first application as the underlying technology for Bitcoin, blockchain has stepped out of the shadow of virtual currency and its impact now traverses beyond financial

12 Marco Iansiti and Karim Lakhani, 'The Truth About Blockchain' (Harvard Business Review, January-February 2017) <https://hbr.org/2017/01/the-truth-about-blockchain> accessed 27 August 2017.

13 ibid.

14 ibid.

15 Gartner Press Release, 'Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage' (August 2016) <www.gartner.com/newsroom/id/3412017> accessed 27 August 2017.

services.[16] The new vistas being explored for application of blockchain technology include, amongst others, corporate governance, democratic participation, social institutions and identity management.

The basic principles underlying blockchain technology are its structure as a distributed database, its focus on peer-to-peer transmission for communication, its potential to offer transparency through pseudonymity and irreversibility of records, and last but not the least, computational logic. At the risk of over-simplification, blockchain can be understood as a chronological database of transactions recorded by a network of computers.[17] These computers are called "nodes". When encrypted and smaller datasets known as "blocks" are organized into a linear sequence, they result in a blockchain.[18] Wright and Di Filippi explain that these blocks contain information about 'a certain number of transactions, a reference to the preceding block in a blockchain, as well as an answer to a complex mathematical puzzle, which is used to validate the data associated with that block'.[19]

Validation on a blockchain takes place by way of a digital fingerprint created through a particular hash function. A hash function is a mathematical algorithm that takes an input and transforms it to an output.[20] Therefore, a hash is a result of cryptographically transformed original information. A hash function is critical to the blockchain technology because it is extremely difficult to recreate the input data from its hash value alone.[21] Moreover, a hash function is used to map all transactions in a block,

16 Don Tapscott and Alex Tapscott, 'The Impact of the Blockchain Goes Beyond Financial Services' (10 May 2016) <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services?referral=03759&cm_vc=rr_item_page.bottom> accessed 30 August 2017.

17 Aaron Wright and Primavera Di Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 March 2015) <www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf> accessed 30 August 2017.

18 Wikipedia, 'Blocks' <https://en.bitcoin.it/wiki/Blocks> accessed 30 August 2017.

19 Wright and Di Filippi (n 17) 7.

20 Marc Pilkington, 'Blockchain Technology: Principles and Applications' (September 18, 2015) in F. Xavier Olleros and Majlinda Zhegu. Edward Elgar (ed.), *Research Handbook on Digital Transformations* (2016) <https://ssrn.com/abstract=2662660> accessed 30 August 2017.

21 ibid.

whereby any differences in input data will produce different output data.[22] Every node connected to the blockchain network is able to submit and receive transactions. Furthermore, each node participating in the network has its own copy of the entire blockchain and is periodically synchronized with other nodes to ensure that nodes have the same shared database.[23] This is crucial as it provides for an exceptional degree of resilience on account of distributed storage by multiple computers (nodes) on the network.[24] Since the shared database can be recreated in its entirety, it makes the failure of a few computers on the network irrelevant.

Another key feature of blockchain technology, also described as a kind of distributed ledger technology, is consensus. In a publicly distributed ledger anyone can create a block, however what is required is a unique chain of blocks and a way to decide which blocks can be trusted. This means that in order to ascertain the legitimacy of transactions recorded into a blockchain, the network has to confirm the validity of new transactions. Therefore, a new block of data has to be added to the end of an existing blockchain only after the nodes on the network arrive at a consensus regarding the validity of the new transaction. This consensus is achieved through different voting mechanisms within a network.[25] The most common voting mechanism, also used for Bitcoin blockchains, is the Proof of Work consensus protocol, which depends on the amount of processing power donated to the network. This protocol, also known as mining, involves participating users working to solve difficult mathematical problems and publishing the solutions. Proof of Work consensus protocol uses tangible resources like computers and electricity, making it difficult for participating users/miners to pretend that they have higher mining power on the network than they actually do. The miners are rewarded with digital tokens - for example, in the case of Bitcoin blockchains they are rewarded with Bitcoins. The Proof of Work algorithms use the number and difficulty level of the solutions being found to measure how much of the network

22 Joseph Bonneau et al., 'Research Perspectives and Challenges for Bitcoin and Cryptocurrencies' IEEE Security and Privacy <www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf.> accessed 31 August 2017.

23 Satoshi Nakomoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', BITCOIN.ORG 3 (2009) <https://bitcoin.org/bitcoin.pdf> accessed 31 August 2017.

24 Wright and Di Filippi (n 17) 7.

25 Wright and Di Filippi (n 17) 7.

agrees on the current state of the blockchain.[26] However, this implies that a Proof of Work consensus protocol demands a lot of energy and time for running these computations, making the efficiency of the protocol questionable. Once a block is added to a public blockchain upon achieving the consensus, this block can no longer be altered and the transactions it contains can be accessed and verified by every node on the network.[27] Consequently, this permanent record can be utilized to coordinate an action or verify an event with close to unimpeachable reliability, without having to trust a centralized authority's attestation to the veracity of a transaction. It appears that the confluence of individual and systemic incentives amounts to a pioneering scheme "for eliciting effort and the contribution of resources from people to conduct various record-keeping and verification activities for the public ledger".[28]

Finally, a brief explanation of the security-enhancing feature of blockchain, i.e., the encryption protocol it follows. Blockchain uses a two-step authentication process using public-key encryption. Every participant is issued a public key, which is an algorithmically generated string of numbers/letters representing the participant. This public key can be shared to enable interaction with others. The participants are also issued one/multiple private keys, each of which is also an algorithmically generated string of numbers/letters. However, it is incumbent upon the participant to keep this private key secure. A given pair of public and private keys has a mathematical relationship allowing the private key to decrypt the information encrypted using the public key. It is important to bear in mind that although participants on the network would know the public keys of other participants, the real identity of a participant can still be protected and remains unknown.[29] This ability to remain pseudo-anonymous is the high-

26 Ethereum Stack Exchange, 'What's the difference between proof of stake and proof of work?' <https://ethereum.stackexchange.com/questions/118/whats-the-difference-between-proof-of-stake-and-proof-of-work> accessed 31 August 2017.

27 Wright and Di Filippi (n 17) 8.

28 David S. Evans, 'Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms', Coase-Sandor Institute for Law & Economics, Research Paper No. 685 3 (15 April 2014) <http://dx.doi.org/10.2139/ssrn.2424516> accessed 31 August 2017.

29 Ashurst, 'Blockchain 101: An Introductory Guide to Blockchain', Digital Economy, 20 March 2017 <www.ashurst.com/en/news-and-insights/insights/blockchain-101/> accessed 1 September 2017.

light when we view transactions on a blockchain from a data protection perspective.

It is pertinent to bear in mind that blockchain technology has been around for almost a decade and is not a static phenomenon. Introduced as the underlying technology for the virtual currency Bitcoin, its key feature was a 'public' distributed ledger as explained in the preceding part. However, in order to keep up with the vast spectrum of blockchain technology's potential applications, another variation known as private or permissioned blockchains has emerged. This development comes in light of the fact that anyone can interact with public ledgers by reading from /writing to them, however permissioned or private blockchains are suitable for applications where transaction details are sought to be kept private and not made visible to the general network and the public.[30] This variation comes with the possibility of being able to determine who can participate in the network. The mechanism for inviting new participants to the network may vary from unanimous agreement, core group acceptance, single user invitation to a more general satisfaction of pre-determined requirements.[31]

Vitalik Buterin, from the Ethereum team, writes about two possible variations of permissioned blockchains – consortium blockchains and fully private blockchains.[32] He defines a consortium blockchain as one where the 'consensus process is controlled by a pre-selected set of nodes'. For a block to be validated in a consortium blockchain, for example, a consortium consisting of 15 institutions, each of which operates a node and of these 10 must sign every block.[33] On the other hand, a 'fully private' blockchain reintroduces the very problem sought to be resolved by blockchains –centralized control by one organization. Therefore, during the course of this thesis when private or permissioned blockchains are mentioned, it refers to a hybrid between permissioned and permissionless

30 Hossein Kakavand, Nicolette Kost de Sevres and Bart Chilton, 'The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies' < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251> accessed 1 September 2017.

31 Goldman Sachs Global Investment Research, 'Blockchain: Putting Theory into Practice' (2016) < https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1> accessed 1 September 2017.

32 Vitalik Buterin, 'On Public and Private Blockchains' (7 August 2015) <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> accessed 1 September 2017.

33 ibid.

blockchain –a model that continues to evolve. Further, a permissioned blockchain is preferable given its better speed and lesser requirement of computation power, making it cheaper and faster than the public blockchain alternative. Moreover, as would be clarified in the next section, when read permissions are restricted a permissioned blockchain can provide a greater level of privacy.[34]

Another variation in the technology comes by way of a shift from the Proof of Work consensus protocol to the Proof of Stake. The difference between the two lies in the fact that Proof of Stake is not about mining, rather it is about validating.[35] The participating user who seeks to validate a block must lock up some digital currency in order to be allowed to process a transaction. In this protocol, the owner of the pledged digital currency holds a financial stake in the success of the blockchain it tracks. Therefore, in Proof of Stake consensus protocol you trust the chain with the highest collateral, and the participating users have a financial stake in the correctness and validity of the blockchain at hand. Proof of Stake algorithm decides who gets to validate the block on the basis of the financial stakes involved, and the selection process also involves some randomness to avoid the risk of reverting to a centralized system.

B. Leveraging Blockchain Technology for Personal Data Protection

Keeping in mind the basic concepts about the working of blockchain, we can proceed to the application of blockchain technology for the purpose of protecting personal data. The proposal of using blockchain to protect personal data was made in a pioneering paper written on the topic of decentralizing privacy.[36] It questions the current models where third parties collect and control massive amounts of personal data. Finding issue with centralized organizations amassing significantly large quantities of personal and sensitive information without adequate measures to protect the said data, a proposal for decentralizing privacy is made. In light of falling trust

34 ibid.

35 Ethereum Stack Exchange (n 26).

36 Guy Ziskind, Oz Nathan and Alex Sandy Pentland, 'Decentralizing Privacy: Using Blockchain to Protect Personal Data', 2015 IEEE Computer Society - IEEE CS Security and Privacy Workshops. <www.computer.org/csdl/proceedings/spw/2015/9933/00/9933a180.pdf > accessed 1 September 2017.

levels amongst data subjects, it explores the potential of blockchains to serve functions requiring trusted computing and auditability.[37] Considering that blockchain technology is structured around a network, which is evolutionary in essence, it suggests future improvements to the technology itself and a personal data management platform based on a combination of blockchain and off-blockchain storage. The approach to such a platform is rooted in privacy considerations.

The platform comprises of three entities viz., **users**, interested in using various applications offered online; **services**, providers of these applications who require processing of personal data; and **nodes**, being the entities responsible for maintaining the blockchain. The proposal relies on two assumptions viz., blockchain being tamper-proof and that the user manages her keys in a secure manner. The first assumption calls for a sufficiently large network of nodes making the consensus protocol more reliable, while the latter requires sensitivity on the part of the user to manage her keys. The protection of personal data is sought to be achieved by setting a sort of clearing-house mechanism. By way of illustration, the blockchain accepts two kinds of transactions - one used for access control management and the other for data storage and retrieval. Once the user installs an application using this proposed platform, a shared identity between the user and the service is generated along with the associated permissions and sent to the blockchain as an access control management transaction. The data collected (which could, for example, be sensor data such as location) on the device (i.e., phone or computer) operating the application is encrypted using a shared encryption key and sent to the blockchain in a storage and retrieval transaction. This transaction is further routed to an off-blockchain key-value store, which has an interface with the blockchain, retaining only a pointer (hash of the data) to the data on the public ledger. Once this is done, the service and the user can query the data using a retrieval transaction with the pointer associated to it. The blockchain kicks in to verify if the digital signature (private key) belongs either the user or the service. An additional layer of scrutiny applies for services, whereby their permissions to access the data are checked as well. The user friendly nature of the platform is buttressed by the ease with

37 ibid.

which the user can change the permissions granted to the service including revoking access to previously stored data.[38]

A close perusal of the model articulated by Zyskin, Nathan and Pentland shows that only the user has control over her data. The public nature of the blockchain is overcome by storing only hashed pointers in it. The decentralized nature of the blockchain, along with the digitally signed transactions, ensures that an adversary cannot pose as a user.[39] Further, even if the adversary has control over one or more nodes, it can learn nothing about the raw data because it is encrypted with keys that none of the nodes possess.[40] This model leverages the distributed network feature of blockchain against the possibility of a node tampering with its local copy of data. Risk minimization is proportional to distribution and replication of data across nodes.

Finally, this paper is far-sighted in as much as it recognizes that the model in its present form only caters to storage and retrieval queries making it inefficient for processing data. Moreover, there is always the possibility of a service querying for raw data only to save it for future processing. Therefore, this thesis finds favour with an approach where a service is never allowed to observe the raw data. The technical solution mentioned by Zyskin, Nathan and Pentland, would allow a service to run computations directly on the network and obtain results.[41] It is this variation of their model that fits in with the proposal for a digital identity management platform put forth in the next chapter.

38 ibid 2.
39 ibid 3.
40 ibid.
41 ibid.

III. Data Protection, Privacy and Identity: A Complex Triad

A. The Contours of Right to Privacy and Right to Data Protection

The concept of privacy is a multi-dimensional one, yet scholars across time and space have attempted to confine it to a single definition. Warren and Brandeis in their seminal essay enunciated that the right to privacy was based on a principle of "inviolate personality", thus laying the foundation for a concept of privacy, which we understand as control over one's own information.[42] Similarly, Westin defined privacy as:

> …claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[43]

However, the many facets of privacy are better defined by breaking them down into categories, as done by Roger Clarke in his publications. Clarke identifies four categories of privacy viz., privacy of the person; of behaviour; of data; and of communication. Therefore, instead of equating privacy with data protection, Clarke's taxonomy allows different kinds of privacy to be protected differently. Accordingly, when this thesis discusses protecting personal data in the context of ensuring privacy, it does not in any way insinuate that all categories of privacy can be protected by way of protecting personal data.

The above discussion suggests a natural link between the right to privacy and the right to data protection. However, there is considerable academic discussion regarding the connection, or lack thereof, between the

---

42 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, as cited in Judith DeCew, 'Privacy', The Stanford Encyclopedia of Philosophy, Spring 2015 <https://plato.stanford.edu/archives/spr2015/entries/privacy/> accessed 2 September 2017.

43 Alan F. Westin, 'Privacy and Freedom', Washington and Lee Law Review, Vol. 25 Issue 1 (1967) 7 <http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr> accessed 2 September 2017.

right to privacy and the right to data protection.[44] A strong case about the disconnect between data protection and privacy is made on the basis of the two distinct rights contained in Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.[45] Article 7 of the Charter envisages the right to respect one's private and family life, home and communications, while Article 8 grants the right to the protection of personal data concerning oneself. However, in the absence of a specific right to data protection in Article 8 of the European Convention on Human Rights (ECHR), it materialises in conjunction with the jurisprudence of the European Court of Human Rights on the protection of privacy and private life.[46]

The author believes that although the Charter distinguishes the right to privacy and the right to data protection as two different fundamental rights, this is more in the nature of a formal distinction. It is doubtful whether the content of the two rights can be neatly isolated from each other.[47] This question may perhaps be answered by looking at the genesis of the right to data protection. Scholars in the field opine that the right to data protection has been characterized by strong links to the right to privacy.[48] Others like Van der Sloot are quick to point out the difference between the mandate for earlier Council of Europe instruments and the later engage-

---

44 Gloria Gonzales Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) Chapter 5; Raphael Gallert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 (5) Computer Law and Security Review 522; Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection Jurisprudence of the CJEU and ECtHR' (2013) 3(4) International Data Privacy Law 222; Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

45 European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02. (Hereinafter *Charter*)

46 Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017). See also ECtHR, *Amann v Switzerland* No. 27798/95, ECHR 2000-II, para. 65; *Rotaru v Romania* [GC] App no 28341/95, ECHR 2000-V, para. 43.

47 Raphael Gallert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29(5) Computer Law and Security Review 522, 524.

48 Gloria Gonzales Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) Chapter 5.

ment of the EU in the field of data protection.[49] Van der Sloot opines that while the main focus of the Council of Europe was to protect human rights on the European continent, the mandate to regulate data protection can be traced to market regulation and the facilitation of free flow of information.[50]

However, the line of argument delineating the right to privacy from the right to data protection does not work because today both these rights are enshrined in the Charter. Therefore, to say that the right to privacy is distinct from the right to data protection because the former is rooted in human rights while the latter is treated as an economic matter is a red herring to say the least. The CJEU in *Digital Rights Ireland* categorically highlighted the 'important role played by protection of personal data in light of fundamental right to respect for private life…'.[51] This approach taken by the CJEU is considered a human rights-based review.[52] Moreover, in the *Schrems* case, the CJEU retrospectively interpreted the DPD 1995 as implementing the right to data protection as guaranteed under Article 8 of the Charter.[53] The entire saga ties up neatly in light of Article 52.3 of the Charter – Article 52.3 provides that insofar as the Charter contains rights corresponding to those guaranteed by the ECHR, their meaning and scope shall be the same as that of the ECHR. What follows from this analysis is that the right to privacy as well as right to data protection under the Charter, and the right to privacy under the ECHR, need to be interpreted in a holistic manner.

Another attempt to sever the right to data protection from the right to privacy comes from the manner in which the GDPR is worded. Although unlike its predecessor, the GDPR does not contain any reference to the right to privacy, yet the author believes that this disconnect is merely

49 Van der Sloot, (n 46) 6; See also: Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), which envisages in Article 1 securing for every individual respect for 'right to privacy, with regard to automatic processing of personal data relating to him ("data protection")'.

50 Van der Sloot (n 46), 7.

51 CJEU, joined cases C-293/12 and C-594/12 (*Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*), judgment of 8 April 2014, ECLI:EU:C:2014:238, para. 48.

52 Craig de Burca, 'EU Law: Text Cases and Materials' (6th edn, Oxford 2015) 401.

53 CJEU, case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), judgement of 6 October 2015, ECLI:EU:C:2015:650, para 78.

terminological. Regard being had to the jurisprudence of Europe's two highest courts (i.e., the ECtHR and the CJEU), the position which emerges is that data protection is an expression of the right to privacy.[54] The right to data protection is a nuanced right and builds on the premise that data processing is inadvertent. Accordingly, it follows that the GDPR contains detailed provisions regarding the obligations of the data controller and processor. These provisions on the right to data protection and what constitutes lawful processing are portrayed as a compromise between different legitimate interests. However, in the author's opinion, it does not serve the interests of either the data subject or the controller/processor to showcase their respective interests as being antagonistic to each other. The emphasis on how and when personal data can be legitimately processed is a corollary to the right to protect one's personal data. Regulatory initiatives to safeguard personal data have been grounded on privacy principles that can be used to identify problematic practices in the processing of personal data. Therefore, it is impossible to detach the right to data protection from the right to privacy.

With the relationship between right to privacy and right to data protection clarified, the next part seeks to establish the important connection between privacy and identity and the need for identity management in the framework of data protection. This will also lay the foundation for answering the research question by positing identity management as an effective tool for data protection.

B. Privacy and Identity: In the Shadow of Profiling

The notion of privacy has witnessed considerable shift in the digital age, due to the 'murky conceptual waters' between what is public and what is private.[55] This is especially so in the backdrop of profiling, where smart technologies are increasingly eroding privacy and the autonomy of individuals. Hilderbrandt defines profiling, albeit from a technological perspective, as:

---

54 Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection Jursiprudence of the CJEU and ECtHR' (2013) 3 (4) International Data Privacy Law 222.

55 Gary T Marx, 'Murky Conceptual Waters: The Public and The Private' (2001) 3 Ethics and Information Technology 157.

> …the process of 'discovering' patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify as a member of a group (which can be an existing community or a 'discovered category').[56]

The GDPR contains a jargon-free definition of profiling which is easier to comprehend:

> 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[57]

Profiling has arisen as a new discipline combining data mining and statistics in order to profile the behaviour of users of an online service.[58] The issue of profiling has exacerbated in the context of IoT, where 'seemingly meaningless data generated by IoT sensors can be combined and analysed resulting in meaningful user profiles'.[59] Such indiscriminate profiling results in erosion of privacy and autonomy and is an assault on the very identity of an individual. Autonomic profiling is a precondition for 'smart' environments propelled by IoT.[60] Hilderbrandt explains autonomic profiling by way of comparing it to a futuristic human butler, where the nonhuman environment 'profiles' our needs and provides for their satisfaction.[61] Thus, autonomic profiling entails making decisions without the intervention of human consciousness. Although Hilderbrandt's analysis of profiling is done in the context of Ambient Intelligence (AmI), i.e., a concept developed to tap the idea of a 'smart' adaptive environment that re-

56 Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-disciplinary perspectives* (Springer 2008), 19.

57 GDPR art 4(1).

58 Jean-Marc Dinant, 'The Concepts of Identity and Identifiablity: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009), 112.

59 Sarah Eskens, 'Profiling the European Consumer in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010> accessed 10 September 2017.

60 Mireille Hilderbrandt, 'Profiling and AmI' in Kai Rennenberg, Denis Royer and André Deuker (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer 2009), 287.

61 ibid 288.

quires little deliberate human intervention, her analysis resonates well with the goal being pursued by IoT.[62] Hilderbrandt postulates that autonomic profiling, which is a precondition for AmI, will significantly impact 'autonomous human action and the constitution of human identity'.[63] Furthermore, the means used to gather an individual's personal data, how the data is processed, and the lack of transparency surrounding its further use, stifles the personal autonomy and informational self-determination of the individual.[64] This is also an encroachment on the identity of an individual and involves data protection concerns.

Scholars have associated privacy with the notion of personhood and self-identity.[65] Likewise, the data protection ecosystem has incubated in the context of informational self-determination with guidance from the German Federal Supreme Court decision. The *Population Census* decision established informational self-determination as a constitutional right in Germany.[66] The right to informational self-determination has emerged as an important facet of the right of personality, which guarantees every individual the possibility to develop her own personality.[67] The German Federal Supreme Court found the legal basis for this right in a hybrid view of two separate provisions of the German constitution viz., right to dignity and right to general personal liberty.[68] Moreover, in linking privacy to autonomy, even the ECtHR has acknowledged that individual self-determi-

62 ibid 274.
63 ibid 290.
64 Neil M Richards and Jonathan H King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41 <www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/> accessed 10 September 2017.
65 N. Kanellopoulou, 'Legal Philosophical Dimensions of Privacy', EnCoRe Briefing Paper 2009 2.
66 Judgment of 15 December 1983, 1 BvR 209/83, BVerfGE 65 as cited in Gerrit Hornung and Christoph Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 Computer Law and Security Review 84.
67 Gerrit Hornung and Christoph Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 Computer Law and Security Review 84, 86.
68 Basic Law for the Federal Republic of Germany, art 1 para 1 and art 2 para 1 <www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0021> accessed 10 September 2017.

nation (or autonomy) is an important principle underlying its interpretation of Article 8 ECHR.[69]

There is literature supporting the idea that 'privacy protections are in essence protections of human dignity and personal autonomy'.[70] Given that the GDPR strives towards facilitating the data subject's ability to exercise control over her personal data (thereby embodying consent), it follows that personal autonomy is a key principle deeply entrenched in the fabric of GDPR. Therefore, the right to autonomy jurisprudence has significant importance in understanding the contours of data protection. As previously mentioned, right to data protection is interpreted by the CJEU by referring to the ECHR for guidance, and in light of Article 52.3 of the Charter by giving deference to the EctHR's case law. In *Pretty v UK*, the Strasbourg court expounded that the concept of 'private life' covers the physical and psychological integrity of a person.[71] In *Mikulic v Croatia*, the ECtHR opined that 'private life' embraces aspects of an individual's physical and social identity.[72] Broadening the concept of 'private life' further, the ECtHR in *Evans v UK* relied on previous case law and stated that private life encompasses the 'right to personal autonomy, personal development and the right to establish relationships with other human beings and the outside world'.[73] Personal autonomy emerges as a 'meta-value behind a number of individual fundamental rights'.[74] Another takeaway from the ECtHR's jurisprudence is the importance of safeguarding one's identity, as it is a crucial element of the right to autonomy.

Identity can be defined as a 'person's uniqueness or individuality which defines or individualizes him as a particular person and thus distinguishes him from others'.[75] An individual's identity manifests itself in various attributes, which make a particular person recognizable. These attributes are

69 Gallert and Gutwirth (n 47) 524.

70 Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge 2014), 12.

71 *Pretty v UK* [2002] ECHR 2346/02, para 61.

72 [2002] ECHR 53176/99 para 53.

73 [2006] ECHR 6339/05 para 57.

74 Manon Oostveen and Kristina Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in Mor Bakhoum et al (eds), *Personal Data in Competition, Consumer Protection and IP Law –Towards a Holistic Approach?* (Springer 2017).

75 Johann Neethling, 'Personality Rights: A Comparative Overview' (2005) 38 (2) Comparative and International Law Journal of Southern Africa 210 234.

unique to that particular person, like their life history, name, credit worthiness, voice, appearance, etc to mention a few.[76] A right to identity would thus mirror a person's inalienable 'interest in the uniqueness of his being'.[77] Information associated with an individual's identity is steadily becoming 'an essential enabler of today's digital society, as it is considered a key component in the interactions between end-users, service providers, and intermediaries.'[78]In that backdrop, the author believes that profiling leads to identity mutilation by intensive processing of personal data and de-individualises the individual. Yet, in the grander scheme of data protection outlined by the GDPR, identity is as marginalized as it was in the DPD – merely as a component of defining personal data.[79] Accordingly, in the absence of a distinct right to identity in the GDPR, safeguarding identity requires exercise of the available tools within the concept of lawful processing. The shortcomings of this approach are elaborated upon in the following discussion.

Autonomic profiling is specifically targeted in the GDPR by bringing it under the umbrella of automatic personal data processing.[80] Nevertheless, profiling is chastised in the circumstances where profiling produces 'legal effects' concerning the data subject or 'similarly significantly' affects the data subject.[81] The limitation of the right against being profiled only in so far as it produces 'legal effects', e.g., being rejected for a loan, being rejected for a job after an e-recruitment procedure, etc.) and grouping the myriad possibilities arising from profiling in a loosely worded manner, highlights the shortsightedness of this provision. The effectiveness of this provision is questionable in light of the complexity associated with profiling. For instance the nature of group profiling is that it represents a group and reveals the applicability of attributes to the individuals constituting

76 ibid.

77 Johann Neethling et al, *Neethling's Law of Personality* (Butterworths 1996) as cited in Norberto Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al (eds), *Privacy and Identity Management for Life* (Springer 2010).

78 David Nuñez and Isaac Agudo, 'BlindIdM: A privacy-preserving approach for identity management as a service' (2014) 13 (2) International Journal of Information Security 199.

79 GDPR art 4(1) defines 'personal data' to mean any information relating to an identified or identifiable natural person.

80 GDPR recital 71.

81 GDPR art 22(1).

such a group.[82] This in turn means that the profile is not inferred solely from the personal data of the person so profiled, rather it makes use of large amount of data relating to many other people which may or may not be anonymised. The risk that emerges from this kind of profiling is more vicious than individual profiling because 'the process results in attributing certain characteristics to an individual derived from the probability that he or she belongs to a group and not from data communicated or collected about him or her.'[83] This strikes at the very identity of an individual and takes maintaining the sanctity of her identity beyond the realm of her personal autonomy.

Given that profiling threatens the identity of a data subject, it would serve the interests of the data subject if the GDPR acknowledged the complexity of profiling and addressed it by introducing a right to identity. Thus, automated data processing in the form of profiling could be confined more efficiently by having recourse to the right to identity. The right to identity may be introduced within the GDPR going a step further than the limited scope of an individual's right against automated profiling. Such an inclusion of the right to identity in the GDPR would provide the necessary mandate for putting in place an identity management solution to secure the protection of personal data. The following part buttresses the need for identity management and the role which blockchain technology can play in this regard.

C. *Identity Management: The Blockchain Way Forward*

In the information age, 'privacy paradox' lies at the core of the struggle for data protection. Privacy paradox is the unavoidable trade-off between the value of an individual's personal data and the value attached to their access to online services. The risk to an individual's identity stems from the indispensability of identity to certain transactions, for example, in determining the existence of necessary conditions for the transaction to oc-

82 Norberto Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al (eds), *Privacy and Identity Management for Life* (Springer 2010) 102.

83 Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul de Hart (eds), *Data Protection in a Profiled World* (Springer 2010) 14.

cur, establishing a relationship for repeated transactions or tailoring delivery of products or services.[84] In order to enable such identity-requiring transactions, methods ought to be put in place to facilitate the asking and answering of identity queries.[85] Today digital identity systems have emerged as a reflex to the requirement of transactions in a digital world.[86] Risks to digital identity can come in the form of identity theft resulting from a privacy breach or dilution of identity arising from the inability to exercise control over the collection and processing of attributes. The need to part with personal data in order to establish one's identity, makes it imperative to have efficient tools to exercise control over what data is provided to the online service and how it is being used, i.e., collection and processing.

Ordinarily, control occurs at the start of a disclosure process; in this context privacy control is seen solely as a limitation on what personal data is made available to others.[87] However, in the era of Web 2.0 and IoT, it is seldom possible to exercise control at the initial stage of disclosing personal data because their architecture itself is premised on acquiring the personal data in order to give the user an enriched experience, or any experience for that matter. However, functionality does not warrant indiscriminate collection or processing of all sorts of personal data and there should be limits to the use and reuse of personal data. Therefore, in light of the preceding parts that establish a delicate balance between privacy, identity and data protection, it is imperative to envisage a scenario where identity management is a cornerstone to securing identity and protection of personal data. The previous part established that there are considerable risks involved in service-side storage and processing of personal information. When this is done without transparent and traceable relation to identities, it creates fundamental asymmetries in the relationship between the users and the online service providers. Therefore, user-centric identity management systems, which can restore this balance and confidence, are a

84 World Economic Forum, 'A Blueprint for Digital Identity' (August 2016) 32 <www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf> accessed 7 September 2017.

85 ibid.

86 ibid 36.

87 Edgar A. Whitley, 'Informational privacy, consent and the 'control' of personal data' (2009) 14 Information Security Technical Report 154, 155.

good response.[88]At the same time, it also calls for cautious pragmatism in choosing the tools used for identity management. The second chapter elucidates the basics of blockchain technology and the potential for using it to protect personal data. In this chapter, the author suggests that developing an identity management tool on the blockchain platform could be a more streamlined approach.

Identity Management platforms may be defined as systems that are 'used to support the management of digital identities or digital identity data'.[89] According to International Telecommunication Standardization Sector, identity management is used for:

– Assurance of identity information (e.g., identifiers, credentials, attributes);
– assurance of the identity of an entity (e.g., users, subscribers, groups, user devices, organisations, networks and service providers, network elements and objects, and virtual objects); and
– enabling business and security applications.[90]

For the purposes of this thesis, the focus will be on the utility of identity management to assure the identity of individuals using online services. In this context, identity management systems have tripartite participation from identity providers, relying parties and users.

Identity is a collection of attributes, which determine the transactions in which an individual can participate. The WEF Report categorises attributes as 'inherent, inherited and assigned'.[91] Table 1 illustrates what they mean in the context of an individual.

88 Simone Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, and M. Waidner (eds.), 'Online Privacy: Towards Information Self-Determination on the Internet', Dagstuhl Manifestos, Vol. 1 Issue 1 1–20 11.

89 Kai Rennenberg, Denis Royer and André Deuker (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer 2009).

90 ITU-T, 'NGN Identity Management Framework', (2009) Recommendation Y.2720 1 < https://www.itu.int/rec/T-REC-Y.2720-200901-I> accessed 8 September 2017.

91 World Economic Forum (n 84) 41.

Table 1: Identity attributes in the context of an individual

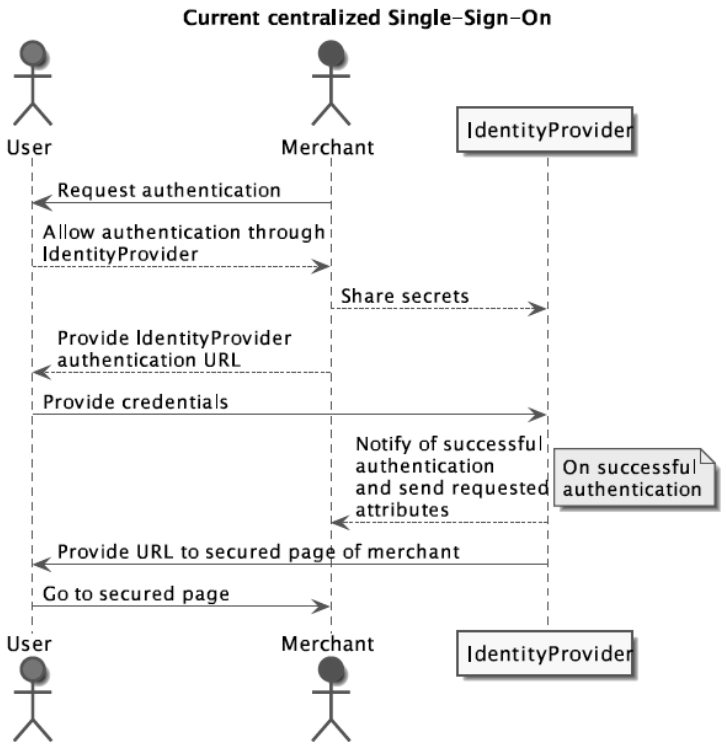
	For Individuals
Inherent Attributes Attributes that are intrinsic to an entity and are not defined by relationships to external entities.	Age Height Date of Birth Fingerprints
Accumulated Attributes Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's life span.	Health records Preferences and behaviours (e.g., telephone metadata)
Assigned Attributes Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.	National identifier number Telephone number Email address

Source: World Economic Forum (2016)

A transaction through digital channels relying on digital identity involves digital storage and exchange of attributes. An ideal digital identity management system would allow the sharing of their information (attributes) by exposing the minimum amount of information required for a given transaction, shielding their information from illicit access all along.[92] Organisations offering centralized identity management systems are able to track transactions enabling them to figure out the details of interactions using their system. Here is a pictorial representation to assist visualizing this problem:

92 World Economic Forum (n 84) 50.

Figure 1: Sequence Diagram of Centralised Single-Sign On



Source: Towards Self-Sovereign Identity Using Blockchain Technology (2016)[93]

Given the pitfalls of a centralised system, there is a strong case for shifting to an identity management system based on distributed identity. In a distributed identity system, multiple identity providers collect, store and transfer user attributes to multiple relying parties. The WEF Report iterates that distributed identity management systems are best suited to 'provide user convenience, control and privacy in an online environment'. This kind of identity management system can protect user privacy and enhance control by allowing users to choose which entities can hold their in-

93 Djuri Baars, 'Towards Self-Sovereign Identity Using Blockchain Technology', Master Thesis, University of Twente 2016 2 <http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf> accessed 7 September 2017.

formation, removing a single point of failure from the system. [94] A distributed identity management system provides an entry point to blockchain technology, as the identity information is to be stored in a decentralized manner. [95]

The aim of this thesis is to propose a mechanism for minimizing the vulnerabilities faced by an individual in maintaining his digital identity within the ambit of the new personal data protection framework. The data protection framework shows some promise because it protects the attributes of identity in the form of 'personal data'. Using blockchain technology to build such a digital identity management platform would give it the required technological push.

Through a digital identity management platform, the data subject should be able to decide which attributes she is willing to disclose within the scope of permissions granted to a service provider. These permissions should govern the processing of data and can be revoked by the user of the digital identity management platform. Relying on the model proposed by Zyskin, Nathan and Pentland for personal data protection using blockchain may help in achieving this.[96] The fact that the access, storage and retrieval transactions are undertaken on the blockchain, it leaves an immutable trail of the manner in which access is provided conditional to permissions, which attributes are requested by a service provider and even how the personal data underlying these attributes is processed. This makes it easy for the data subject to exercise control over her attributes in the form of personal data. The blockchain approach is favoured over traditional identity management systems because the latter follows a centralized system characterized by single point of failure. Moreover, use of zero knowledge proof cryptography allows an identity owner to choose which identity information to reveal about herself and to prove claims about herself without revealing the underlying personal data.[97]

Currently, a few start-ups are leveraging the blockchain model to provide digital identity management platforms. Notable amongst these platforms are Sovrin and uPort.

Sovrin offers a permissioned blockchain that allows public access to identity owners but allows only trusted institutions to work as nodes on

94 World Economic Forum (n 84) 62.
95 World Economic Forum (n 84) 59.
96 Text to n 36.
97 Zyskin, Nathan and Pentland (n 36).

the network. It envisages an extra layer of verification of identity attribute asserted by an individual resulting in a decentralized identifier. Thereafter, claims made regarding one's identity are verified by accessing the relevant personal data, however, the blockchain can be tapped only for the decentralized identifier and the hashes/digital signatures of a claim, and not the personal data as such.[98]

uPort is a digital identity management service provided on the Ethereum blockchain network. uPort provides heightened levels of control to its users who can be fully in control of the identities created on this platform.[99] The MIT Human Dynamics lab as a part of their Core Identity Blockchain Project is also assessing the potential of uPort.[100]

Given that blockchain based digital identity management solutions are already offering their services, it becomes all the more important to analyse the compatibility of such a solution with the GDPR framework. Table 2 gives a brief overview of the possible interplay between the features of the proposed solution and the GDPR provisions.

Table 2: Mapping the GDPR provisions to blockchain powered DIM

Features of Blockchain powered DIM	**GDPR Provisions**
Decentralised transaction storage	Accountability
Replication of data over nodes	Data minimisation
Querying on a DIM platform	Control by Data Subject, Purpose and use limitation
Immutability	Right to be forgotten
Locking up of Data	Right to Data portability
Core features of blockchain	Data protection by design

98 Sovrin, 'Identity for all' <www.sovrin.org/> accessed 8 September 2017.

99 Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton and Michael Sena, 'Uport: A Platform for Self-Sovereign Identity' (21 February 2017) <https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf> accessed 8 September 2017.

100 Massachusetts Institute of Technology, 'Core Identity Blockchain Project' (2017) <https://law.mit.edu/blog/core-identity-blockchain-project> accessed 8 September 2017.

IV. Fitting the Blockchain Solution into the GDPR Puzzle

This chapter assesses the proposal of leveraging blockchain technology for personal data protection by establishing a digital identity management platform on the touchstone of the GDPR. It is done by systematically mapping the compatibility of the proposal to the established principles of data protection as codified in the GDPR. However, this chapter begins with a general analysis of the GDPR's claim to technological neutrality.

A. GDPR: A Technolog(ically)y Neutral Law?

This part endeavours to evaluate the claim that the GDPR is a technologically neutral law.[101] Hilderbrandt and Tielmans give a lucid distinction between 'technology neutral law' and 'technologically neutral law'.[102] While 'technology neutral law' pertains to the understanding that legal effect should not depend on a particular technology used by those addressed by the law, use of the term 'technologically neutral law' is reserved to the notion that law does not depend on the articulation of a technology.[103] Hilderbrandt and Tielmans challenge this second approach by calling it a misconception. According to them, law can never be technologically neutral because it is always enabled by a particular technological ICT infrastructure.[104]Therefore, the assessment with regard to GDPR ought to be whether it is a 'technology neutral law'.

At the outset it is essential to understand the raison d'être of the GDPR. It is an established principle of law and economics that regulation is a response to externalities that impose a social cost.[105] Traditionally in the context of data protection, the externality appeared in form of imbalance of power between state and individual where the state wielded the upper

101 Recital 15 GDPR.
102 Mireille Hilderbrandt and Laura Tielmans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law and Security Review 509, 516.
103 ibid.
104 ibid.
105 Ronald H Coase, 'The Problem of Social Cost' (1960) 3 Journal of Law and Economics 1.

hand in terms of collection, use and retention of data. However, over the years the rising economic potential of data has called for a re-evaluation of this approach to regulation and it makes a case for recognizing the private commercial interests in accumulating and processing data with the increasing technological ease. Therefore, the reform can be seen as a response to the technological externalities of advances in high-speed networking and data storage. The social cost imposed by these technological externalities was recognised by the Article 29 Data Protection Working Party Report, where it stresses the risk of lack of control and information asymmetry.[106]Information asymmetry is characterized by the significant gap between the data controller's and data subject's knowledge about the fate of the latter's personal data.[107]

Given that the GDPR is a response to technological externalities that threaten privacy and data protection, it is desirable to analyse the GDPR according to the three interpretations of technology neutral legislation propounded by Hilderbrandt and Tielmans. The three interpretations are as under:

1) In order to be neutral, law may have to provide for technology specific provisions to retain the substance of the legal right they support. The aim is to achieve equivalent effect in online and offline environments.
2) Legislation should not discriminate between different kinds of technologies with the same functionality because this could stifle innovation and result in unfair competition.
3) There is an underlying need for legislation to be future proof because legislative acts take a long time to reach fruition and the focus on a particular technology may render the legislation outdated and ineffective sooner than expected.[108] (emphasis added)

The GDPR, in all its technology neutral glory, still states data protection by design and default as one of its fundamental features.[109] Article 25 warrants for technical and organizational measures, in particular suggesting pseudonymisation, designed to implement data protection principles. In

106 Article 29 Data Protection Working Party (2014) 'Opinion 8/2014 on the on Recent Developments on the Internet of Things', WP 223, 6.

107 Janice Y Tsai et al, 'The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study' (2011) 22(2) Information Systems Research 254, 1.

108 Hilderbradnt and Tielmans (n 102) 510.

109 Article 25 GDPR.

this regard the technology specific nature of the provision, where technology itself is visualized as creating equivalent protection. Therefore, technological specificity embodied in Article 25 is needed to achieve technology neutral legislation. Secondly, parallel to data protection by design, the GDPR confers upon the data subjects a right to data portability, which has strong links to interoperability as a pre-requisite for dynamic efficiency.[110] This facilitates different technologies to thrive because it empowers the data subject to demand portability from one data controller to another, perhaps using different technology to ensure a more privacy friendly default. This achieves non-discrimination against technologies by the GDPR. Lastly, given the long and uncomfortable journey of the data protection law reform, the GDPR provisions are formulated in a manner so as to allow sufficient sustainability if not eternity of their relevance in a fast changing technological landscape.[111]

It flows from the above discussion that the GDPR has all the requisite features for being considered a technology neutral law. However, the mettle of this claim can be truly assessed only in light of a real confrontation. The blockchain model for digital identity management confronts the GDPR to prove its technology neutral credentials in practice.

It is the author's understanding that eventually the receptiveness of GDPR to revolutionary technologies like Blockchain would depend upon the kind of regulatory instrument the GDPR is categorised as.[112] Categorising it as a command and control regulatory instrument would mean that it is a 'classical' regulation operating through rule-based coercion. But if it were seen as falling within the class known as 'consensus', then it would be more likely to accommodate a digital identity management solution based on blockchain. The latter class of the regulatory instrument entails an exceptionally broad range of regulatory arrangements.[113] This ranges from 'self-regulation' to various forms of co-operative partnerships

110 Article 20 GDPR.

111 An example could be the phrasing of 'right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her' in Article 22 GDPR.

112 For an understanding of different regulatory instruments. Brownen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007) Ch 3, 79.

113 ibid 92.

between state and non-state actors in an attempt to regulate.[114] It has been claimed that industry self-regulation is more efficacious where the regulated activity (in this case being collection, storage and processing of personal data on a blockchain) is thought to require a high level of technical or expert knowledge, owing to superior informational capacities as compared to the state. Flexibility and adaptability to new technological needs are advantages of self-regulation over command and control regulation.

However, self-regulation has its limitations like absence of formal government approval and inadequacy of leniency to achieve public goals to mention a few. Hirsch highlights that in the absence of guarantees to legal compliance, a puritan form of self-regulation will 'neither attract sufficient industry involvement nor address the need for international privacy standards'.[115] Therefore, what is desirable is something on the other side of the spectrum of possibilities offered by consensus kind of regulatory instruments –co-regulation. Standardisation can be one way of achieving co-regulation. The European Commission recently published its decision on a standardisation request towards the European Standardisation Organisations (ESOs).[116] This request is a Commission Implementing Decision based on the Regulation 182/2011.[117] This request entails a mandate, if accepted by the ESOs, for developing privacy management standards. In as much as it involves oversight by the Commission, this standard setting activity by the ESOs falls within the domain of co-regulation. Although the mandate pertains to the DPD, but since the GDPR itself recognises standardization and certification, it can be said that such standard setting activity would have a mandate under GDPR to co-regulate.[118] This creates a window for a blockchain based digital identity management platform to

114 ibid.

115 Dennis D Hirsch, 'In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct' (2013) 74 Ohio State Law Journal 1029, 1043.

116 European Commission (2015) M/530 Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy

117 OJ L 55, 28/2/2011

118 Articles 42,43 GDPR.

find compatibility with the GDPR if it can prove its credentials during the standard setting process at the ESOs. However, the standard setting process has to keep in mind that the participating technology is compliant with mandatory legal requirements.[119] This implies that if a blockchain based digital identity management solution can assert that it is compliant with the legal requirements of the GDPR and if it is able to prove its technological credentials, it may be incorporated as a technical standard for data protection by design. According to Falke et al, 'compliance with standards may create 'legitimate expectations' and people may assume them to have official legal standing'.[120] This will root the legal status of a blockchain-based solution by way of co-regulation.

The GDPR cannot weather the storm of emerging technologies solely by relying on the sufficiency of the new legal provisions. In so far as the mandate is seen as a response to technology specific challenges and the need to elaborate technology design obligations, the abovementioned Commission Implementing Decision would not produce results, which fall foul of the technology neutral aspect of the GDPR. Therefore, if there is room for interpreting the GDPR as a regulatory instrument allowing co-regulation, it actually helps the GDPR realise its ambition of being called a technology neutral law.

However, it remains to be seen if the model of digital identity management built on blockchain is able to assert legal compliance with the GDPR – a hurdle that returns to be overcome. The next part takes stock of this challenge.

B. GDPR and Blockchain Technology: Possibilities and impossibilities

1. Accountability

Given that both permissioned and permissionless blockchains rely on the multiplicity of nodes to ensure trust, pinpointing accountability seems to

119 Irene Kamara, 'Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate'' (2017) 8(1) European Journal of Law and Technology <http://ejlt.org/article/view/545/723>.

120 Josef Falke and Harm Schepel (eds.), *Legal Aspects of Standardisation in the Member States of the EC and of EFTA*, vol 1 (H. S. A. Luxembourg: Office for Official Publications of the European Communities 2000), 181.

be a daunting task. In a short time-span, blockchain as a distributed ledger has posed a serious challenge for regulatory approaches that hinge on central intermediaries.[121] The simplistic definitions of data controller and data processor retained in the GDPR, although supplemented by way of onerous obligations to ensure data protection, are still not adequate to cover all entities involved in data processing in an interconnected technological environment.[122] The inability to pin-point a controller could have serious implications for the entire data protection framework in the GDPR and many of the data subjects rights would be rendered useless, e.g., right to data deletion, access and portability, security breach notifications and most importantly it would be difficult to coerce compliance with the stick of heavy fines.[123]

However, the situation is not that grim, given that currently the entities providing digital identity management on a blockchain are using permissioned blockchains. In this scenario, regulators can focus on either a technical system operator or consider the group of participating entities as joint controllers. The GDPR clarifies that in case of joint controllers they should have a transparent arrangement regarding the respective responsibilities for compliance and empowers the data subject to exercise her rights in the GDPR against one or all of the controllers irrespective of such an arrangement.[124] But if it were a case of public blockchain, the open and permissionless nature would mean that there could be an ever-growing army of nodes. Moreover the personal data is processed at every node each time a block is added in furtherance of a transaction, in such a situation the concept of joint controller responsibilities would fail to meet the requirement in Article 26(1) of having a transparent arrangement of responsibilities for compliance. The other option of choosing one or all the nodes as per Article 26(3) seems to be procedurally untenable.

Another variation of this challenge may manifest itself in the form of the data subject herself being the data controller because that is the aim of

121 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, 424.

122 Neil Robinson et al, *Review of the European Data Protection Directive* (Cambridge 2009) <https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf> accessed 5 September 2017.

123 Berberich and Steiner (n 121) 424.

124 Article 26 GDPR.

the digital identity management platform –to return complete control to the data subject. However, it is probable that establishment offering these digital identity management services could be considered as 'gatekeepers' to the blockchain and find themselves bearing the brunt of compliance to GDPR. An entity like Sovrin or uPort could showcase willingness to comply with data protection principles by way of appointing a Data Protection Officer to carry out tasks specified under Article 39 of GDPR. Furthermore, as per the DIM model described previously, it is also possible to track the requests for access to personal data and the grant of the same by the data subject on the blockchain. This provides enhanced accountability and data provenance of personal data of data subjects utilising a DIM on a blockchain platform. The entities providing the DIM platform play a role in determining how the personal data of its users is processed, imparting to them characteristics of processors. Once clarified that the DIM platform provider is to be considered the controller and processor, veracity of permissions given by the data subject vis-à-vis the data usage can be authentically tracked on the blockchain and the platform provider be held accountable. This, in the author's opinion, strengthens the accountability principle.

2. Data Minimisation

This principle is a stalwart in the realm of data protection. Data minimization manifests itself in Article 5(1)(c) GDPR whereby the amount of personal data collected should be 'limited to what is necessary' to achieve purposes for which the data processed. Strangely enough it deviates from Article 6(1)(c) DPD, which provided that personal data must be 'relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. In the DPD the provision was directed at ensuring minimality at the stage of data collection. However, the principle of data minimisation is also reflected in the purpose limitation provision whereby personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed'.[125] Bygrave opines that rules encouraging transactional anonymity are also direct manifestations of the

125 Article 5(1)(b) GDPR.

minimality principle.[126] The GDPR goes a step further in encouraging pseudonymisation of data. Digital identity management platforms built on blockchain would fall foul of the traditional understanding of the data minismisation principle whereby it focuses on minimization at the collecting and processing stage. This contradiction would arise from the very structure of blockchain technology where data is replicated on each node. At the same time, however, merely storing hashed pointers to the personal data and not the personal data itself on the blockchain would perhaps find favour with data minimisation. The requirement of transactional anonymity would be fulfilled by way of zero knowledge proof, whereby the data subject avails this feature on the digital identity management platform to return queries by the online service provider. In this manner, the online service provider would have access to bare minimum personal data, e.g, if YouTube wants to know that you are above 18 years to watch a particular video, it does not need to know your birthdate, a simple yes or no answer would suffice.

The relevance of using blockchain technology for a digital identity management platform manifests itself in reducing availability of personal data to online service providers. This squarely addresses the problem of profiling in the digital realm as well.

3. Control

As rapid technological developments mount new challenges for protection of personal data, the GDPR acknowledges the importance of trust in the digital economy. Recital 7 of the GDPR states the need for natural persons to have control over their personal data. In order to ensure this, the new framework goes out on a limb to broaden the scope of control and makes it more comprehensive.

The notion that consent could empower a data subject to have control over her personal data is based on a narrow view that control is limited to controlling the disclosure of data, in the author's opinion control is rather based on a broader right to personal autonomy. Throughout the GDPR, various provisions are intended to enhance control of the data subject over

126 Lee A Bygrave, *Data Privacy Law: An Interntional Perspective* (Oxford 2014), 152.

her personal data. This is achieved by empowering the data subject with a strong portfolio of rights like right of access, right to be forgotten and right to data portability being the most important ones.[127] The author sees these rights as reinforcing individual control supported by the GDPR envisioning a heterogeneous set of normative and technological tools, for example, ways to ensure accountability and privacy by design mechanisms. Control also fosters autonomy by giving the data subject the ability to manage information about herself. Although the GDPR does not mention a 'right to identity', its provisions implicitly enable the data subject to control how she is perceived. This also fits well with the understanding that privacy is determined by the ability to control personal information.[128]

The digital identity management solution built on blockchain achieves the said goal of returning control over their personal data back to the data subjects in line with the reformed provisions of GDPR. It does so by providing the data subjects full control regarding who gets access to how much of their personal data and for what purposes it may be used. Therefore, the proposed model supports the data subjects to undertake privacy management in an effective manner. The technology aids them and eases the burden of maintaining their personal autonomy. It is a step in the direction of inculcating a culture of data protection rather than merely regulating data protection. The rights of data subjects are to be construed as a means to achieving higher degree of control rather than as ends.

4. Right to be Forgotten

Article 17 codifies one of the most important provisions enabling the data subjects to exercise personal autonomy with respect to their identities. The inclusion comes in the backdrop of the seminal *Google Spain* decision.[129] In this judgment, CJEU also highlights the perils of profiling. The provision attempts to regulate the privacy risks online in the age of 'perfect re-

127 Articles 13, 17, 20 GDPR.

128 H T Tavani, 'Privacy and the Internet' (2000) Boston College Intellectual Property & Technology <www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html> accessed 8 September 2017.

129 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317

membering'.[130] Mitrou and Karyda opine that 'perfect and precise remembering affects the claim of individuals to live and act without leaving permanent traces or shadows'. This interferes with a crucial aspect of information privacy, in particular the right to informational self-determination and control of one's own personal data.

Article 17 encompasses the right of the data subject to erasure of her personal data and injunct the data controller from engaging in further dissemination of her data. This right comes into effect if:

a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
b) the processing of personal data does not comply with the data protection framework; or
c) the data subject withdraws her consent or objects to the processing.[131]

It is pertinent to mention that this right to be forgotten does not apply retrospectively to the data already processed. Furthermore, this right imposes limited obligation on the controllers to 'what is technically feasible and does not require a disproportionate effort.[132] Therefore, it is important to bear in mind that right to be forgotten is not an absolute right that can always be requested by the data subject.

Right to be forgotten poses a big challenge for blockchain-based digital identity management solutions, given the immutable nature of the data stored on the blockchain. Although, immutability is the bedrock of blockchain technology, yet there are some technological suggestions to make the blockchain editable.[133]However, the author opines that it would be better to keep the feature of immutability intact if it comes at the cost of functionality that supports data protection. Regulators should not adopt a very restrictive interpretation and rather strike a balance between protecting privacy and the understanding of how technology shapes up. Article 35(1) of Germany's Federal Data Protection Act lends credibility to such

130 Lilian Mitrou and Maria Karyda, 'EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245&rec=1&srcabs=2032325&alg=1&pos=10> accessed 8 September 2017.

131 Mitrou and Karyda (n 130) 11.

132 Article 19 GDPR.

133 Accenture, 'Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World' <www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf> accessed 7 September 2017.

an approach. According to Article 35(1), the controller can circumvent the obligation to erase personal data where erasure would be impossible or would involve a disproportionate effect due to the specific mode of storage. In such circumstances, the German Federal Data Protection Act proposes restriction of processing said personal data as per Article 18 of the GDPR. The German Act also relieves the controller oft he obligation to erase in the instance of erasure adversely affecting the legitimate interests of data subject. The utility of 'legitimate interest' provision in this regard is discussed at the end of this part.

Therefore, it is suggested that indefinite locking of data on an immutable blockchain should actually be considered compliance with other data protection principles in the GDPR rather than seeking to admonish it under the right to be forgotten. The insufficiency of legal instruments alone to deal with technological challenges has been buttressed already. It follows that the utility of the right to be forgotten will depend on its interpretation in the technological landscape and a forward looking approach similar to the one taken by Germany is advisable. It should not be the case that an isolated island of this right is created detached from the mainland that is the GDPR.

5. Right to Data Portability

This right is an internet-specific new right allowing the data subjects to exercise the freedom of changing who controls their data. In the current framework, for example, of data storage on the cloud, service providers spend considerable time and resources to push their registered users to further deepen their profiles. Once this is done, it is extremely difficult to extract their information from one platform and move it in entirety to another platform, making it extremely difficult to change service providers.[134] So far there has been neither the carrot nor the stick for ensuring system interoperability when it comes to personal data storage. However, the GDPR seeks to remedy this by specifically entitling the data subject to demand data portability in a commonly used and machine-readable format

134 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, 189.

directly to the new controller of her choice.[135] However, what is peculiar is to hinge this right to portability to cases where the processing is done in furtherance of consent. This releases the controller from obligations to port data where the collection has happened on grounds other than consent, e.g., the good old legitimate interest ground for lawful processing contained in Article 6(1)(f) of the GDPR.

Further, there are arguments to tap the regulatory toolbox for governing data portability under competition law. [136] Koops also ponders over not employing competition as a regulatory tool, but laments that it may be due to the market structures of the data economy. However, he suggest that in light of dominance of certain multinational internet companies, a focus on providing market incentives for alternative providers with more privacy-friendly policies and default settings might be more helpful than command-based rules for data processing.[137]

However, when it comes to the digital identity management platform on a blockchain, it has inherent features of ensuring seamless interoperability because the data subject is in control of her personal attributes and can share them with whomever she chooses. In the rigid sense of the term data portability, whereby the data has to be on the servers of a new controller seems to be undesirable because one of the features of the digital identity management platform on blockchain is that nobody has access to the off-chain storage of the personal data and only pointers to the data are stored on the blockchain. Regarding portability to another DIM platform, it can be easily achieved in case of public blockchains by sharing the public key and pointing the new DIM service provider to the data, after which the said new DIM service provider would handle the access and use permissions.[138] In case of permissioned blockchains, portability may be achieved by way of the users downloading the data (using their private key) from one DIM service provider's platform and moving it to a new one. This

135 Article 20(1) GDPR.

136 De Hert and Papakonstantinou (n 134) 190.

137 Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (TILT Law and Technology Preprint Publications 2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692> accessed 8 Spetember 2017.

138 Blockchain Bundesverbrand, 'Blockchain, data protection, and the GDPR' (2018) <https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v 1.0.pdf> accessed 30 October 2018.

would have to be supplemented by a request to restrict processing of their personal data made to the previous DIM service provider.

6. Data Protection by Design

In furtherance of its technology neutrality, the GDPR mandates data protection by design.[139] The Article 29 Working Party had argued for the induction of data protection by design as a legal obligation in order to take technological data protection into account at the planning stage of platforms dealing with personal data.[140] The objective of data protection by design is that 'the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'.[141] This provision provides the stimulus for innovation in the field of technical data protection by design principles. At the same time, the technologies do not have a free pass and ought to provide data protection as envisaged in the GDPR framework. Data protection by design seeks to encourage the integration of technical and organizational measures into the business models of data controllers. The role that technical standards can play in achieving data protection by design has been covered in the part discussing technology neutrality of the GDPR.

It follows from the above discussion that although the digital identity management platforms claim to provide heightened level of protection for personal data, these claims have to be tested regarding their compliance with the obligations set forth in the GDPR. The previous points in this part of the thesis explain how provisions like data minimisation and right to be forgotten interact with a blockchain-based solution for personal data protection.

One way of reconciling all the abovementioned issues is to take into consideration the 'legitimate interest' as a legal basis for processing personal data. This strikes a cord with the other aim of the GDPR, i.e., ensure free movement of data and is the saving grace for data controllers.[142] The EU jurisprudence is replete with cases emphasizing that interferences with

---

139 Article 25 GDPR.
140 Hilderbrandt and Tielmans (n 102) 516.
141 ibid 517.
142 Lee A Bygrave, *Data Privacy Law: An Interntional Perspective* (Oxford 2014), 121.

the rights to privacy and data protection must be strictly proportionate to the aims pursued.[143]Moreover, the *Google Spain* decision requires that the balancing activity for establishing 'legitimate interest' must take note of the data subjects' rights arising from Articles 7 and 8 of the Charter.[144] In the GDPR Article 6(1)(f) codifies the 'legitimate interest' route to lawful processing. It considers processing done for legitimate interests pursued by the data controller to be lawful. The *Breyer* decision offers some insight regarding the interpretation of 'legitimate interests'.[145] According, to this decision a service provider's activity of collecting and processing personal data without the data subject's consent can be considered to be lawful if such collection and processing is necessary to facilitate the use of those services by the data subject.

In furtherance of the interpretation of 'legitimate interest' in the *Google Spain* and *Breyer* decisions, it is possible to reconcile a blockchain-based solution for protecting personal data with the GDPR. The underlying technology for the digital identity management platforms suggested in this thesis entails significant difficulties for compliance with the prevailing understanding of the right to be forgotten and the accountability principle. Yet it is possible to take recourse to the very structure of the blockchain technology, which imparts the high level of data protection to the said platforms. Therefore, in as much as the collecting and processing of personal data done by these platforms is necessary for the functionality of these platforms in protecting personal data of the users, such activities can be considered lawful irrespective of the challenges posed by other provisions in the GDPR. It is important to note that legal rules pertain to normativity rather than regularity and should 'work as standards for interaction that create legitimate expectations', leaving scope for interpretation.[146]

---

143 CJEU, joined cases C-465/00, C-138/01 and C-139/01 (*Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk*), judgment of 20 May 2003, ECLI:EU:C:2003:294, para. 86; case C-275/06 (*Productores de Música de España (Promusicae) v Telefónica de España SAU*), judgment of 29 January 2008, ECLI:EU:C:2008:54, para. 54; joined cases C-92/09 and C- 93/09 (*Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*), judgement of 9 November 2010, ECLI:EU:C:2010:662, para. 72.

144 *Google Spain* (n 129).

145 Case C –582/14 *Commission v. Breyer* ECLI:EU:C:2017:563.

146 Hilderbrandt and Tielmans (n 102) 518.

Here is a table illustrating the extent to which reconciliation of digital identity management platforms built on blockchain with GDPR is possible.

Table 3: Reconciliation Chart

Features of Blockchain powered DIM	**GDPR Provisions**	**Possibility of Reconciliation**
Decentralised transaction storage	Accountability	Possible
Replication of data over nodes	Data minimisation	Possible
Querying on a DIM platform	Control by Data Subject	Achieved by the technology
Immutability	Right to be forgotten	Requires flexible interpretation
Locking up of Data	Right to Data portability	Possible
Core features of blockchain	Data protection by design	Achieved by the technology itself

V. Conclusion

The thesis builds on basic concepts in order to answer the research question -does the GDPR provide a conducive framework for a blockchain based digital identity management tool. The discussion on privacy, identity and data protection leads to a point of convergence where although right to data protection is distinct from right to privacy, yet it is understood as adding value to it. Right to data protection achieves this value-addition by promoting informational self-determination and individual personality rights. In light of the increasing prowess of collection and processing of data, profiling is identified as a real threat to personal autonomy of an individual. Identity takes centre-stage in this discussion on automated processing of personal data and the limitations of the GDPR are highlighted in this context. Accordingly, the author finds favour with the incorporation of a right to identity within the GDPR would provide the requisite mandate for arresting the threat posed by the proliferation of profiling in the age of IoT. Relying on this right to identity could provide the adequate legal mandate for developing a digital identity management solution based on the blockchain model.

The thesis also seeks to evaluate the assertion that the GDPR is a technologically neutral legislation or a technology neutral one. It remains to be seen how far the GDPR in its current form is able to assimilate/resolve the contradictions posed by applications of blockchain technology. Particularly, the digital identity management solution built on a blockchain model faces many hurdles before even getting close to achieving its dream goal of establishing a self-sovereign identity –a scenario where the data subject is in full control of her personal data to the exclusion of others.

In law and technology literature the term 'law lag' is used to depict the inadequacy of existing legal provisions to deal with a social, cultural or commercial context created by rapid advances in information and communication technology.[147] To avoid being characterized by 'law lag', it is pertinent that the provisions of GDPR are interpreted to allow new technolo-

147 John H. Clippinger and David Bollier (eds), *From Bitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society* (Institute for Institutional Innovation by Data-Driven Design 2014), 138.

gies to come forward and help with the mammoth task that is data protection. In that context, a co-regulation approach is proposed, where standard setting organisations can assist the GDPR in meeting the challenge posed by emerging technologies. Going through a standard-setting procedure is particularly favourable for blockchain based digital identity management solution because it gets to prove its credibility and upon being incorporated as a standard, would attain a *de facto* legal status.

The EU holds the distinction for being the vanguard of data protection movement. It is then naturally incumbent upon it to be alive to the promises and possibilities that blockchain technology has to offer for revolutionizing this movement. Therefore, the provisions of the GDPR should not be interpreted narrowly and be mindful of the pace at which the technology is developing. The provision on 'legitimate interests' provides significant leeway to interpret the GDPR in a manner conducive to a blockchain-based solution for data protection. Moreover, instead of nipping it in the bud, a blockchain approach for a digital identity management solution could also be encouraged to make requisite changes to the existing models. The potential of adaptability of the blockchain is evident in the manner in which off-chain storage is being suggested in addition to the possibility for an editable blockchain. This requires keeping channels of communication open between the regulators and the industry.

In case the proposed approach is able to reconcile the promise of blockchain technology with the challenges posed by GDPR, another question that arises is if returning control over personal data to the data subject in this manner would find favour with the discussion regarding creating ownership in data. It would be interesting to see how the business models relying on collection and processing of data would respond.

A daunting task, during the course of writing this thesis, was to find good references for the blockchain applications beyond Bitcoin. Most of the research at the time was published in blogs, conferences, symposiums and workshops. The need for high quality journals where the focus is on blockchain was deeply felt.[148] However, it is a humble attempt to bring to the table a host of questions that face the viability of a digital identity

148 Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 11(10): e0163477. <https://doi.org/10.1371/journal.pone.0163477> accessed 12 September 2017.

management solution built on a blockchain, if not adequately answer them.

List of Works Cited

Primary Sources

Cases

Amann v Switzerland [2000] ECHR 27798/95.

Commission v. Breyer ECLI:EU:C:2017:563.

Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others ECLI:EU:C:2014:238.

Evans v UK [2006] ECHR 6339/05.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ECLI:EU:C:2014:317.

Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650.

Mikulic v Croatia [2002] ECHR 53176/99.

Pretty v UK [2002] ECHR 2346/02.

Productores de Música de España (Promusicae) v Telefónica de España SAU ECLI:EU:C:2008:54.

Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk ECLI:EU:C:2003:294.

Rotaru v Romania [GC] App no 28341/95, ECHR 2000-V.

Volkszählungsurteil, BVerfGE Bd. 65, 1

Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen ECLI:EU:C:2010:662

European Union Legislation and Preparatory Acts

Basic Law for the Federal Republic of Germany

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

Data Protection Working Party (2014) 'Opinion 8/2014 on the on Recent Developments on the Internet of Things', WP 223, 6.

Directive 95/46/EC of the European Parliament and of the Council.

European Commission, M/530 Commission Implementing Decision C (2015) 102.

European Commission, OJ L 55 Commission Implementing Decision 28/2/2011.

European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02

Regulation No. 182/2011 (EU) of the European Parliament and of the Council.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council.

Regulation (EU) No. 2016/679 of the European Parliament and of the Council.

Secondary Sources

Books

Bakhoum, M., et al (eds), *Personal Data in Competition, Consumer Protection and IP Law –Towards a Holistic Approach?* (Springer 2017).

Bernal, P., *Internet Privacy Rights: Rights to Protect Autonomy* (Cambridge 2014).

Bygrave, L.A., *Data Privacy Law: An Interntional Perspective* (Oxford 2014).

Clippinger, J.H. and Bollier, D. (eds), *From Bitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society* (Institute for Institutional Innovation by Data-Driven Design 2014),

de Burca, C., *EU Law: Text Cases and Materials* (6th edn, Oxford 2015).

DeCew, J., *Privacy* (The Stanford Encyclopedia of Philosophy, Spring 2015)

Falke, J. and Schepel, H. (eds.), *Legal Aspects of Standardisation in the Member States of the EC and of EFTA*, vol 1 (H. S. A. Luxembourg: Office for Official Publications of the European Communities 2000).

Fischer-Hübner, S., et al (eds), *Privacy and Identity Management for Life* (Springer 2010).

Fuster, G.G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

Gutwirth, S., et al (eds), *Reinventing Data Protection?* (Springer 2009).

Gutwirth, S., Poullet, Y. and Paul de Hart (eds), *Data Protection in a Profiled World* (Springer 2010).

Hildebrandt, M. and Gutwirth, S., (eds), *Profiling the European Citizen: Cross-disciplinary perspectives* (Springer 2008).

Leenes, R. et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

Morgan, B. and Yeung, K., *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007)

Neethling, J. et al, *Neethling's Law of Personality* (Butterworths 1996)

Olleros, F.X., and Elgar, M.Z.E. (ed.), *Research Handbook on Digital Transformations* (2016).

Rennenberg, K., Royer, D. and Deuker, A. (eds), *The Future of Identity in the Information Society: Challenges and Opportunities* (Springer 2009).

Contribution to edited books

Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer 2017).

Jean-Marc Dinant, 'The Concepts of Identity and Identifiablity: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?' as cited in Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009).

Manon Oostveen and Kristina Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' as cited in Bakhoum, M., et al (eds), *Personal Data in Competition, Consumer Protection and IP Law –Towards a Holistic Approach?* (Springer 2017).

Marc Pilkington, 'Blockchain Technology: Principles and Applications' (September 18, 2015) in F. Xavier Olleros and Majlinda Zhegu. Edward Elgar (ed.), *Research Handbook on Digital Transformations* (2016).

Norberto Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al (eds), *Privacy and Identity Management for Life* (Springer 2010).

Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, as cited in Judith DeCew, 'Privacy', The Stanford Encyclopedia of Philosophy (Spring 2015).

Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul de Hart (eds), *Data Protection in a Profiled World* (Springer 2010) 14.

Journal articles

Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 (1) SCRIPTed 3.

David Nuñez and Isaac Agudo, 'BlindIdM: A privacy-preserving approach for identity management as a service' (2014) 13 (2) International Journal of Information Security 199.

Dennis D Hirsch, 'In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct' (2013) 74 Ohio State Law Journal 1029.

Edgar A. Whitley, 'Informational privacy, consent and the 'control' of personal data' (2009) 14 Information Security Technical Report 154.

Gary T Marx, 'Murky Conceptual Waters: The Public and The Private' (2001) 3 Ethics and Information Technology 157.

Gerrit Hornung and Christoph Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 25 Computer Law and Security Review 84

Irwin Altman, 'Privacy: A Conceptual Analysis' (1976) 8 Environment and Behavior 7.

Janice Y Tsai et al, 'The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study' (2011) 22(2) Information Systems Research 254.

Johann Neethling, 'Personality Rights: A Comparative Overview' (2005) 38 (2) Comparative and International Law Journal of Southern Africa 210.

Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection Jurisprudence of the CJEU and ECtHR' (2013) 3 (4) International Data Privacy Law 222.

Marco Iansiti and Karim Lakhani, 'The Truth About Blockchain' (Harvard Business Review, January-February 2017).

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.

Mireille Hilderbrandt and Laura Tielmans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law and Security Review 509.

Nadja Kanellopoulou, 'Legal Philosophical Dimensions of Privacy', EnCoRe Briefing Paper 2009.

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.

Raphael Gallert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 (5) Computer Law and Security Review 522.

Ronald H Coase, 'The Problem of Social Cost' (1960) 3 Journal of Law and Economics 1.

Scott R. Peppet, 'Unraveling privacy: The personal prospectus and the threat of a full-disclosure future.' (2011) 105 Northwestern University Law Review 1153 1183.

Simone Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, and M. Waidner (eds.), 'Online Privacy: Towards Information Self-Determination on the Internet', Dagstuhl Manifestos, Vol. 1 Issue 1 1–20.

Online articles

Aaron Wright and Primavera Di Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (10 March 2015) <www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf>.

Alan F. Westin, 'Privacy and Freedom', Washington and Lee Law Review, Vol. 25 Issue 1 (1967) 7. <http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>.

Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (TILT Law and Technology Preprint Publications 2014). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692>

Blockchain Bundesverbrand, 'Blockchain, data protection, and the GDPR' (May 2018). < https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v 1.0.pdf >

Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton and Michael Sena, 'Uport: A Platform for Self-Sovereign Identity' (21 February 2017). <https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf>.

David S. Evans, 'Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms', Coase-Sandor Institute for Law & Economics, Research Paper No. 685 3 (15 April 2014). <http://dx.doi.org/10.2139/ssrn.2424516>.

David Reinsel, John Gantz and John Rydning, 'Data Age 2025: The Evolution of Data to Life-Critical' (April 2017). <www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>.

Don Tapscott and Alex Tapscott, 'The Impact of the Blockchain Goes Beyond Financial Services' (10 May 2016) <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services?referral=03759&cm_vc=rr_item_page.bottom>.

Guy Ziskind, Oz Nathan and Alex Sandy Pentland, 'Decentralizing Privacy: Using Blockchain to Protect Personal Data', 2015 IEEE Computer Society - IEEE CS Security and Privacy Workshops. <www.computer.org/csdl/proceedings/spw/2015/9933/00/9933a180.pdf>.

H T Tavani, 'Privacy and the Internet' (2000) Boston College Intellectual Property & Technology. <www.bc.edu/bc_org/avp/law/st_org/iptf/commentary/content/2000041901.html>

Irene Kamara, 'Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate'' (2017) 8(1) European Journal of Law and Technology. <http://ejlt.org/article/view/545/723>.

Joseph Bonneau et al., 'Research Perspectives and Challenges for Bitcoin and

Cryptocurrencies' IEEE Security and Privacy. <www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf.>.

Lilian Mitrou and Maria Karyda, 'EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge'. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245&rec=1&srcabs=2032325&alg=1&pos=10>.

Massachusetts Institute of Technology, 'Core Identity Blockchain Project' (2017). <https://law.mit.edu/blog/core-identity-blockchain-project>.

Moritz Walther, 'The EU GDPR and Distributed Ledgers (Blockchain): Solutions to a Worst Case Scenario' (2018). <https://www.researchgate.net/publication/325069696_The_EU_GDPR_and_Distributed_Ledgers_Blockchain_Solutions_to_a_Worst_Case_Scenario>

Neil M Richards and Jonathan H King, 'Three Paradoxes of Big Data' (2013) 66 Stanford Law Review Online 41. <www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/>.

Neil Robinson et al, *Review of the European Data Protection Directive* (Cambridge 2009). <https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf>.

Patrick Tucker, 'Has Big Data made Anonymity Impossible?' MIT Technology Review - Business Report (7 May 2013). <www.technologyreview.com/s/514351/has-big-data-made-anonymity-impossible/?set=514341>.

Sarah Eskens, 'Profiling the European Consumer in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?'. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010>.

Satoshi Nakomoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' BITCOIN.ORG 3 (2009). <https://bitcoin.org/bitcoin.pdf>.

Vernon Turner, 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things' (April 2014). <www.emc.com/leadership/digital-universe/2014iview/digital-universe-of-opportunities-vernon-turner.htm>.

World Economic Forum, 'A Blueprint for Digital Identity' (August 2016). <www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf>.

Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 11(10): e0163477. <https://doi.org/10.1371/journal.pone.0163477>.

Website and blogs

Ashurst, 'Blockchain 101: An Introductory Guide to Blockchain', Digital Economy, 20 March 2017. <www.ashurst.com/en/news-and-insights/insights/blockchain-101/>.

Accenture, 'Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World'. <www.accenture.com/t00010101T000000__w__/es-es/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf>.

Djuri Baars, 'Towards Self-Sovereign Identity Using Blockchain Technology', Master Thesis, University of Twente 2016. <http://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf>

Ethereum Stack Exchange, 'What's the difference between proof of stake and proof of work?'. <https://ethereum.stackexchange.com/questions/118/whats-the-difference-between-proof-of-stake-and-proof-of-work>.

Gartner Press Release, 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015' (Stamford, 10 November 2015). <www.gartner.com/newsroom/id/3165317>.

Gartner Press Release, 'Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage' (August 2016). <www.gartner.com/newsroom/id/3412017>.

Goldman Sachs Global Investment Research, 'Blockchain: Putting Theory into Practice' (2016). <https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1>.

ITU-T, 'NGN Identity Management Framework', (2009) Recommendation Y.2720. <https://www.itu.int/rec/T-REC-Y.2720-200901-I>.

Sovrin, 'Identity for all'. <www.sovrin.org/>.

TNS Opinion & Social, 'Data Protection' Special Eurobarometer 431 (June 2011). <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pd>.

Vitalik Buterin, 'On Public and Private Blockchains' (7 August 2015). <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>.

Wikipedia, 'Blocks' <https://en.bitcoin.it/wiki/Blocks>.