THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/JBBA-1-1-(4)2018

Blockchain and Privacy Protection in Case of The European General Data Protection Regulation (GDPR): A Delphi Study

Simon Schwerin
Berlin School of Economics and Law, Germany

Correspondence:
simon@schwerins.de

Received: 28 March 2018 **Accepted**: 30 March 2018 **Published**: 18 April 2018

Abstract
The present work deals with the interrelationships of blockchain technology and the new European General Data Protection Regulation, that will be intact after May 28th, 2018. The regulation harmonizes personal data protection across the European Union and aims to return the ownership of personal data to the individual. This thesis, therefore, addresses the question how this new technology that is characterized by decentralization, immutability and truly digitized values will be affected by the strict privacy regulation and vice versa. The aim of this work is to clarify whether blockchains can comply with the new regulation on the one hand and to identify how blockchain could support its compliance, on the other hand. The questions are validated through an extensive literature review and are further investigated by using a Delphi study that asks a panel of 25 renowned experts to find opportunities, limitations and general suggestions about both topics. In addition, a framework is proposed to support the assessment of privacy and related risks of blockchains.

As a result, it becomes apparent that blockchains can become more privacy friendly and comply with the regulation if an active dialogue between blockchain developers and regulatory authorities helps to strengthen their mutual understanding and work. With the support of this work and the blockchain Privacy Impact Assessment canvas a foundation for the necessary next steps is laid to overcome the challenges of defining a data controller or deleting personal data within a blockchain.

Keywords: blockchain, privacy, data protection regulation, General Data Protection Regulation (GDPR), Delphi study, Data Protection Impact Assessment (DPIA), blockchain Privacy Impact Assessment

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
Simon Schwerin[1] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
Simon Schwerin[1] acknowledges Bruce Pon, Roland Müller and Ing. Katarina Adam for their feedback and suggestions on this paper.

Table of Contents

Chapter Page

Table of Contents 3
List of Tables 5
List of Figures 6
List of Abbreviations 7
1. Chapter: Introduction 8
1.1. Motivation 8
1.2. Research Goal 9
1.3. Theoretical Relevance 9
1.4. Practical Relevance 10
1.5. Research Process 10
1.6. Outline 11
2. Chapter: Background and Literature Review 12
2.1. Data Protection Regulation in the EU 12
2.1.1. Before the GDPR 13
2.1.2. Introduction to the GDPR 15
2.1.2.1. Purpose 15
2.1.2.2. Structure 15
2.1.2.3. Impact on the EU 16
2.1.2.4. Key definition and concepts 16
2.1.3. Implications of the GDPR for blockchain 18
2.2. Blockchain 20
2.2.1. Background and definition 20
2.2.2. How blockchains work 22
2.2.2.1. Exchange of digital values 22
2.2.2.2. Hashes and blocks 23
2.2.2.3. Mining 24
2.2.2.4. Smart contracts 24
2.2.2.5. Public, private, permissioned and permissionless 25
2.2.3. Existing privacy solutions 25
2.3. Hypotheses 28
3. Chapter: Research Methodology 30
3.1. The Delphi Method 30
3.1.1. Background 30

3.1.2. Suitability 32
3.1.3. Participant Selection and Background 34
3.1.4. Questionnaire Design 36
3.1.4.1. Delphi round one 37
3.1.4.2. Delphi round two 39
3.1.4.3. Delphi round three 39
3.1.5. Data Collection 40
4. Chapter: Results 42
4.1. Analysis 42
4.1.1. H1: Blockchains have an impact on personal data. 43
4.1.2. H2: Data protection regulations will have an impact on blockchains related to personal data 46
4.1.3. H3: Personal data cannot be stored on the blockchain directly, but indirectly. 49
4.1.4. H4: Blockchains can be designed in a privacy-friendly manner by using the approach of privacy by design. 52
4.1.5. H5: Blockchains can help to solve (privacy) challenges accompanying the implementation of the new GDPR. 53
4.1.6. Interim Summary 58
4.1.7. Statistical analysis 59
4.2. Blockchain privacy impact assessment (bPIA) canvas 59
4.3. Practical Recommendations 64
5. Chapter: Conclusion 66
5.1. Résumé 66
5.2. Limitations and need for further research 68
References 69

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

List of Tables

Table Page
Table 1: Literature Review - Keywords and Sources 12
Table 2: Mentions of the GDPR and blockchain in existing literature 19
Table 3: Well-known cryptographic techniques [87], [88], [84] 26
Table 4: Cutting edge cryptographic solutions [87], [88], [84] 27
Table 5: Comparison of Research Methods and Tools, created and adapted by the EU JRC from the Futures Research Methodology [30], [104] 34
Table 6: Experts' backgrounds, response rates and time durations 40
Table 7: Participants' study specific experience 41
Table 8: Distribution of answers over categories (questions and hypotheses) 43
Table 9: Results for Hypothesis 1 (part 1) 45
Table 10: Results for Hypothesis 1 (part 2) 46
Table 11: Results for Hypothesis 2 48
Table 12: Results for Hypothesis 3 (part 1) 50
Table 13: Results for Hypothesis 3 (part 2) 51
Table 14: Results for Hypothesis 4 53
Table 15: Results for Hypothesis 5 (part 1) 55
Table 16: Results for Hypothesis 5 (part 2) 56
Table 17: Results for Hypothesis 5 (part 3) 57
Table 18: Summary of highest rated Delphi results 58
Table 19: Results of Duncan's MRT 59
Table 20: Practical recommendations for privacy-friendly blockchain development 65

List of Figures

Figure Page

Figure 1: Research process (own presentation) partly adapted from Linstone and Turloff (2002) [31] 11
Figure 2: A brief history of the General Data Protection Regulation by Wilhelm (2016) [39] 13
Figure 3: Eleven chapters of the GDPR (own presentation) [51] 16
Figure 4: Ontology layers of blockchain transactions based on de Kruijff and Weigand (2016) [67]21
Figure 5: Transactions written to a block chain (own presentation) based on Tschorsch (2015)..... 23
Figure 6: The mining process (own presentation) partly based on Tschorsch (2015) 24
Figure 7: Zoomed in Delphi study in Research Process cut out from 1. Chapter: Introduction..... 30
Figure 8: Typical Delphi steps - (own presentation) based on Pfeiffer (1968) [101]..... 31
Figure 9: Combined experience in years of the expert panel in 4 categories (own presentation) 35
Figure 10: Country of residence of the expert panel (own presentation) 36
Figure 11: Structure of Delphi round one (own presentation)..... 37
Figure 12: Categories for Delphi round two (from actual questionnaire, own presentation) 39
Figure 13: Boxplot (own presentation)..... 42
Figure 14: Specific steps of the PIA process (own presentation) adapted from ICO's guidance [129]61
Figure 15: Strategies by tactics from *Colesky and Hoepman (2016) [134]*..... 63
Figure 16: Privacy design strategy definition framework from *Colesky and Hoepman (2016) [134]*63

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

List of Abbreviations

ACM	Association for Computing Machinery
AI	Artificial Intelligence
BC	Blockchain
BE	Belgium
c't	Magazin für Computertechnik (magazine for computer technology)
CH	Switzerland
DApp	decentralised application
DE	Germany
EDPS	European Data Protection Supervisor
EP	European Parliament
EU	European Union
GDPR	General Data Protection Regulation
IE	Ireland
IEEE	Institute of Electrical and Electronics Engineers
IMF	International Monetary Fund
ISO TC	International Standards Organization - Technical Committee
JRC	Joint Research Centre (of the European Commission)
KR	South Korea
MT	Malta
PD	Personal Data
PII	Personally Identifiable Information
UK	United Kingdom
US	United States of America
WEF	World Economic Forum

1. Chapter: Introduction

1.1. Motivation

Personal data protection (the US term "privacy" is used interchangeably within the context of this thesis) is becoming more important than ever before. There is an increasing demand of identity and a right to privacy in developing countries, which are implementing compulsory biometric data services [1]. Under the current speed of development for Artificial Intelligence (AI) in combination with centralized service providers like Google and Facebook (it is assumed that well-known companies with such high market and news presence do not need a reference) that currently own the personal data (PD) of their users, the question becomes inevitable to what will happen with that data in the future [2], [3], [4], [5], [6]. Will these individuals be willing to keep trusting their governments and these companies to use the services and algorithms they developed fairly? To bring back trust to a digital world, one proposed solution is blockchain technology (used interchangeably with blockchain and the abbreviation BC) [7], [8]. In short blockchain technology can be described by comparing it to a spreadsheet in the sky, where each person has the latest version of the document, and everyone can inspect it. Users need to reach a mutual consensus to define its content, and instead of one company like Google storing it centrally, every user keeps a copy of the blockchain on their machine [9].

In the blockchain ecosystem, people talk about an evolution and paradigm shift that will influence each fragment of the world currently known [10]. The distributed version of trust will affect existing business models and industries, legal systems and governments and ultimately to society as a whole [7]. Blockchains most prominent use case is the digital money Bitcoin, which is proposed for audit functions, exchanges and to host other applications where the often monopolistic central organizations have become inefficient or untrustworthy [10]–[12].

To take a step back, blockchain itself is not the only factor that led to the realization of the necessity to seriously rethink our current systems and structures of powers and wealth attribution [3]. None of today's technological trends (e.g., blockchain, AI, Big Data, Internet of Things (IoT)) would occur without the rise of innovations that enabled immensely efficient data collection and storage spanning across all aspects of an individual's or machine's lifespan (e.g. Apple's iPhone, Intel's microprocessors) – some go as far as calling all that collected data "the new oil" [6], [10], [14], [15].

To loop back to the emergence of AI, new technological advances have been shifting the boundaries of how data can be put into context [16]. In this research, the focus is on personal data or personally identifiable information (PII) as Americans call it [16]. The definition of PII changes with the development of those technologies that increase the chance to re-identify data, using multiple sources [16]. Today almost every digital device that is used by humans and connected to the internet can be used to trace back to its origin [17]. As this kind of data is often closely linked to the identity of a human, it should therefore be protected to the same extend as other rights this individual has.

One successful approach towards regulating what happens to our personal data and the human right of privacy was taken by the European Union (EU) in order harmonize data protection across Europe and strengthen its digital single market strategy [18], [4]. The General Data Protection Regulation (GDPR) that has been put into place in May 2016, will help to achieve exactly that. Its enforcement will prevail after May 25th, 2018 and significantly increase the value of personal data and shift the ownership of it back to the individual [19], [20].

With blockchain creating new paradigms and regulation that imposes a fundamental change to the way personal data is currently being processed, it is important to look at these topics and figure out how they can benefit and not hinder each other to reach their full potential and intended purposes [21].

1.2. Research Goal

The objective of this research is:

Developing theoretical frameworks and practical recommendations to improve the mutual relationships between blockchain and the GDPR.

This research objective led to the following key research question:

Where are interrelationships between blockchain and the GDPR?

The main question can be composed into sub-questions by looking at it from different angles. From the point of view of a blockchain expert the questions arise *[22]*:

1. *What is the impact and relevance of the regulation towards the development of blockchain technology?*
2. *How to make a blockchain compliant to the new regulation?*
3. *How could a blockchain be used as an application for GDPR compliance?*

From a regulatory (data protection expert) perspective, on the other hand the questions arise [18]:

1. *What should be done to help blockchain developers to become GDPR compliant, without hindering its innovative impact?*
2. *Can a blockchain be privacy-friendly by being developed along the principles of privacy by design?*
3. *How could a blockchain help regulatory bodies?*

Since the key research question is due to its many factors of uncertainty and unknown future dependencies truly complex, answering the sub-questions in a structured manner will help finding answers to it. The relevance of this exploratory Delphi study is discussed next.

1.3. Theoretical Relevance

This research aims to add new knowledge to the understanding of blockchain and privacy, specifically with regards to a strict data protection regulation like the GDPR. As the GDPR lays the foundation for privacy regulations worldwide, the results of this study will help to enable international discussions and future research in topics related to technology, legal and business contexts [20], [21], [23], [24].

Further research can use the frameworks, and expert knowledge gathered in this study to develop detailed scientific work to help blockchains inventing and implementing the right balance with privacy concerns, described by Berberich and Steiner (2016) as [21]:

"The strength of BC [blockchain] is creating trust in the authenticity of information and the safety of transactions. These objectives should be balanced with privacy concerns."

The research results can further be used to fill a gap in understanding the relationship between blockchain and the GDPR. By providing a high-level overview of an aggregated framework and thoughts collected from 25 subject matter experts, many research pitfalls can be avoided.

1.4. Practical Relevance

As previously stated, the topic can again be seen from different points of view. This time the regulatory view is inspected first, as the latest annual report of the European Data Protection Supervisor (EDPS) perfectly describes the practical importance for the regulatory authorities and data protection experts [18]:

"It is essential that data protection experts begin to examine the concepts behind blockchain technology and how it is implemented in order to better understand how data protection principles can be applied to it. An integral part of this process should be the development of a privacy-friendly blockchain technology, based on the principles of privacy by design."

From the blockchain experts point of view, the uptake and traction the topic has gained are indicated by customer requests that the authors' company BigchainDB GmbH receives, as well as the active participation at an overbooked presentation held by the author [25]. Additionally, whitepapers that serve mainly as marketing material, but do present relevant content, have recently been published by law firms and identity management software providers [26], [27].

Another point of view can be taken from the authors work in the German mirror committee of the International Organization for Standardization (for the ISO TC 307) that currently aims to create international standards for blockchain technology. The topic of the GDPR was raised in the identity, privacy and security working groups [28], [29].

It shows that this research can help set a practical and theoretical foundation for the future development of blockchain and privacy enhancing technology as well as legal frameworks. The author hopes to spark further dialogue between regulators, governments and innovators to drive this topic towards a more equal and fair future for everyone. To draw an accurate picture of future scenarios, this thesis leverages the Delphi method for its core research procedure.

1.5. Research Process

The research process presents a high-level overview of the research design and shows how the Delphi method fits it. After initial reviews about potential research topics and brainstorming sessions with colleagues and friends, initial hypotheses were formed that helped to define the research question of this thesis further. These first hypotheses-drafts were presented to the academic supervisors of the author, after which the decision was made to conduct an exploratory study within the field of Future Research Methodologies [30]. After an initial recommendation through one of the supervisors, further literature was reviewed to finalize the choice for conducting a Delphi study.

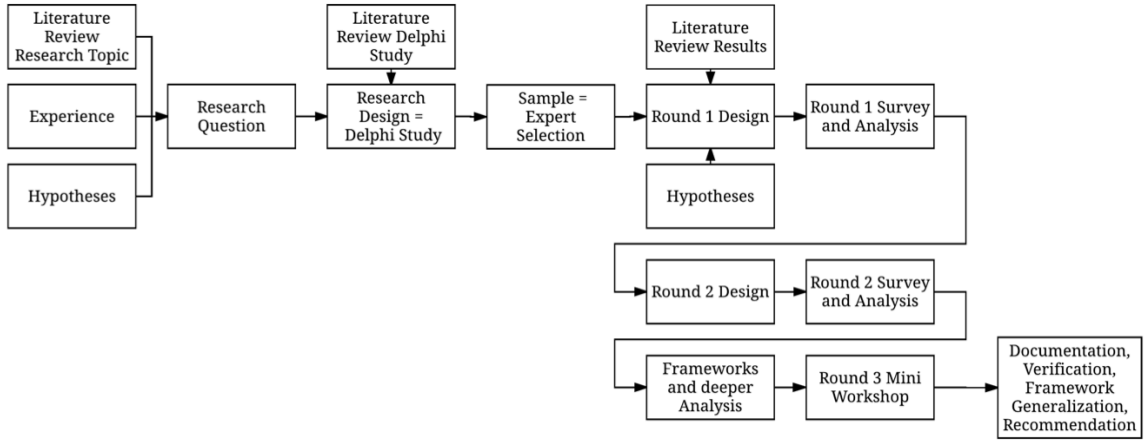


Figure 1: Research process (own presentation) partly adapted from Linstone and Turloff (2002) [31]

Deeper analysis, conceptualized frameworks and recommendations are discussed to conclude the thesis. The following outline will summarize the structure along the lines of this process and help to navigate through the thesis [32].

1.6. Outline

The outlined structure of the thesis closes ***Chapter: Introduction*** about the opening remarks of the mutual relationships between blockchain and the GDPR.

Chapter: Background and Literature Review

The theoretical groundwork and background on blockchain, the GDPR and existing privacy solutions for blockchain are provided through the results of an extensive literature review. From here hypotheses are concluded that build the foundation for the Delhi study.

Chapter: Research Methodology

The research methodology and Delphi study are demonstrated to prepare the necessary information for its analysis and framework development.

Appendices A to D show the actual questionnaires and complete results of the Delphi study.

Chapter: Results

Firstly, the data gathered in the Delphi method is analyzed and put into perspective. Secondly, a framework of a privacy impact assessment for blockchain technology, comprising guidance for practitioners and researchers, is proposed and discussed.

Conclusion

The studies implications, limitations and recommendations with final remarks are presented, including concrete recommendations for further research.

2. Chapter: Background and Literature Review

Within this chapter, the results of an extensive literature review lay the theoretical foundation for this thesis.

The author decided to focus his search on the main terms closely related to the topic of this thesis, namely blockchain (also called "distributed ledger" technology by some part of the ecosystem, the term "Bitcoin" was avoided on purpose, as it only presents one use case of blockchain technology) and the GDPR (which includes "privacy" and "data protection regulation") [33], [34]. Literature about the research methodology (see Methodology - Background) was collected as well but is not an integral part of this main review.

These main keywords are summarized in Table 1 (it is assumed that well-known abbreviations do not have to be written out as words outside the List of Abbreviations) that also shows the main sources of the literature review. Besides brief internet searches, six main categories with 13 specific sources were identified to find approximately 150 different pieces of literature (including e.g. scientific journal articles, books, whitepaper and so forth). These have been selected for their relevance to this paper and credibility based on their authors and publication audience. Peer-reviewed literature hardly exists, as both fields are relatively new [34], [35], [36].

Table 1: Literature Review - Keywords and Sources

Keywords	
blockchain (distributed ledger) GDPR (privacy, data protection regulation)	
Sources	
Peer Reviewed Journals	IEEE, ACM, Web of Science
Open Science	Researchgate, academia.edu
Meta Search Engine	google scholar, google books
Market Research Institute	Forrester, Gartner
International Organizations	WEF, IMF
Regulatory Bodies	EU Commission, EDPS

Within the scope of this thesis, the following chapter outlines a strongly compacted summary of the main topics. In the first part, the data protection regulations in the EU are revised, and the main challenges of the GDPR implementation with regards to blockchain are described. In the second part, the main concepts of blockchain will be defined and explained for further use in outlining existing privacy solutions for blockchain. In a third part, this theoretical foundation is used to create the main hypotheses as a basis for further investigation within the Delphi study.

2.1. Data Protection Regulation in the EU

"The improvement in substance is that there's far more transparency under the new rules, which means that you will have more detailed information policies about what your data are processed for, which purposes if they are given to others, and there will be also in general more possibilities to get a view of

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

which data are there about you. And you have new rights like data portability and the right to be forgotten. So, it will be far easier for consumers to control their personal data."

Jan Philipp Albrecht summarizes the substance of the new data protection regulation in the EU [37]. As a member of the European Parliament (MEP) he became known as the father of the GDPR and the author is happy to have gained him as a participant in the Delphi study. [38]. The next section will discover the journey of data protection regulations towards the GDPR.

2.1.1. Before the GDPR

Data protection law in the EU goes along very carefully with the development of information technology (IT) as shown in Figure 2. Without going into every detail of this chart, the most important points along the journey towards the GDPR (this chart was created in January 2016, therefore the question marks about the actual adoption) will be mentioned.

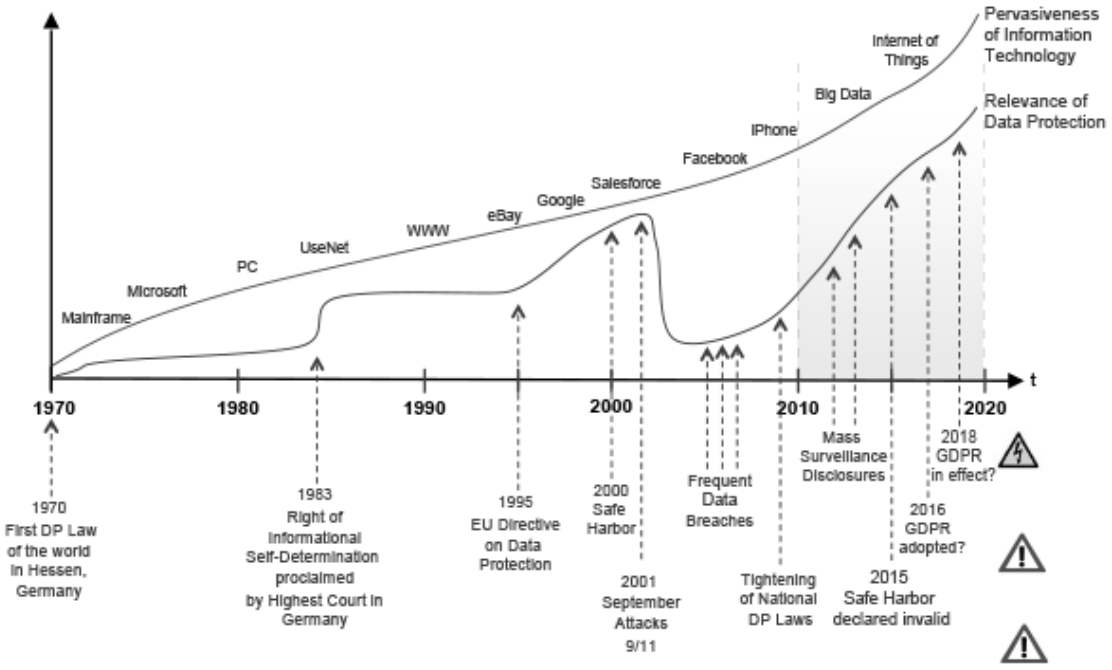


Figure 2: A brief history of the General Data Protection Regulation by Wilhelm (2016) [39]

Adding to the historical perspective of the very detailed work of Van Alsenoy (2016), who identified four main periods, each of which will be related to the pervasiveness of IT (from the previous Figure) during that time [40]. This relation will give a broader implicit perspective of the necessity of data protection regulations during those periods:

1. *The emergence of national data protection laws (1970-1980)*

Van Alsenoy further describes the appearance of data protection as a kind of policy issue, that was bound to the 1960's transition to a post-industrial economy, as a time of extensive social and economic change. To administer this change governments began to use the advances in computing technologies to

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

gather data about citizens that led to a paradigm shift of rethinking the nature of the relationship of the state to the individual [40]. The first data protection laws were adopted by the German State Hesse in 1970, followed by the country of Sweden in 1973 and Germany, France, Denmark, Norway and Austria in 1978 [40], [41].

This period was the time that Xerox invented the Ethernet and Microsoft got founded to put the first personal computers (PC) moved into individuals' households [42].

2. *Internationalization (1980-1981)*

The Organization for Economic Co-Operation and Development (OECD) formalized its first initiative (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) to prevent the growing national concerns about cross-border data flows that were seen as potential threads that would lead to losing legal control over data processing activities [40]. The success of this first international guidelines is described by further quoting Van Alsenoy:

"By incorporating a certain degree of abstraction, the OECD managed to forge a consensus among experts from both sides of the Atlantic, who at times hold very diverging views on how to best implement privacy protections."

The PC was going into a phase of mass adaption, and the first computer games appeared on the markets [43].

3. *National implementation (1982-1994)*

During this timeframe, national bodies started to adapt their national data protection laws to the OECD guidelines. Specifically, the UK Data Protection Act of 1984 and the Belgian Data Protection Act of 1992 are seen to be major milestones towards an EU-wide data protection framework, as they were both characterized as "rush jobs" that would further force the EU to push for a harmonized action [40].

The development of PCs (Apple and Microsoft) and microprocessors ran in rapid exponential growth and led to the development of the Domain Name System and ultimately the first implementations of websites on the internet as it is known today [43], [44].

4. *European harmonization (1995-2016)*

The EU managed to publish the European Data Protection Directive (DPD) on the protection of individuals privacy with regards to the processing of personal data and the free movement of such data [45]. The directive still only served as a guideline that did not require implementation measures for national bodies. It had two goals [19]:

"[...]to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States."

Several directives to specify forms of digital communication were submitted in the subsequent years, until finally the Article 29 Working Party – an independent EU advisory board, established in 1996, that includes data protection authorities of each EU members state, the EDPS and the EU Commission – made a reform proposal in 2012 for an EU wide data protection regulation [45], [46]. A regulation differs to a directive, in that it overrides national law immediately upon activation while adding strong

enforcement mechanisms [19]. It took another two years until the European Parliament (EP) finally adopted the GDPR proposal in 2014 and another two years to finalize the proposal and action plan for its implementation [45]. Finally, after months of intense lobbying that included more than 3500 amendments, the GDPR enters into force on April 27th, 2016 – 20 days after publication in the Official Journal of the EU [40], [45]. The GDPR will apply and be enforceable within two years, after May 28th, 2018. The intention was to give organizations those two years to be able to implement the correct changes to their privacy processes and policies in order to be compliant [45].

Till now, Silicon Valley companies spread their services across the whole world, including massive sales of personal phones (Apple iPhones), online advertising services (Google Adds) and other centralized services [43]. Using new technologies that led to massive data collection possibilities through IoT and Big Data, personal data moved further into the possession of a few huge multinational companies [47]. It was time to look at new technologies that would enable the first step towards digital decentralization, as for why blockchain could be next on the top line of the graph in Figure 2 [48], [49].

After giving a brief overview of what led to the GDPR, the next sections introduce the main concepts of the GDPR and its main implications towards blockchain based on existing literature.

2.1.2. Introduction to the GDPR

This section will outline the purpose and structure of the GDPR. It will then describe its impact on the EU and present the key definitions and concepts.

2.1.2.1. Purpose

With the previously described DPD the minimum standard for data protection law in the EU was set, but it still made it very difficult for organizations to determine which member states law applies when dealing with cross-border data flows. The EU commission finally decided that a single harmonized and enforceable law for all member states should achieve two main goals [19]:

1. Protecting the rights, privacy and freedoms of natural persons in the EU.
2. Reducing barriers to business by facilitating the free movement of data throughout the EU.

These goals go along the line of the new overall single market strategy of the EU [18], [50]:

"The Single Market is at the heart of the European project, enabling people, services, goods and capital to move more freely, offering opportunities for European businesses and greater choice and lower prices for consumers. It enables citizens to travel, live, work or study wherever they wish."

This is achieved by the aforementioned differentiation to a directive. Regulations are, hence, an efficient mechanism to apply a consistent approach to all 500 million people in 28 member states – and frequently beyond [19].

2.1.2.2. Structure

The GDPR is split up into two broader sections, which is standard for EU directives and regulations [20]. The first section contains the recitals, which essentially provide broader context, direction and guidance for better understanding the explicit requirements set out in the articles in section two [51]. These articles provide the scope to which entities must comply. A summary of the articles, which are

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

categorized in chapters, is shown in Figure 3. This helps professionals to navigate through the regulation, as not every article applies to a single organization – often only a few articles are relevant for a specific case. [52].

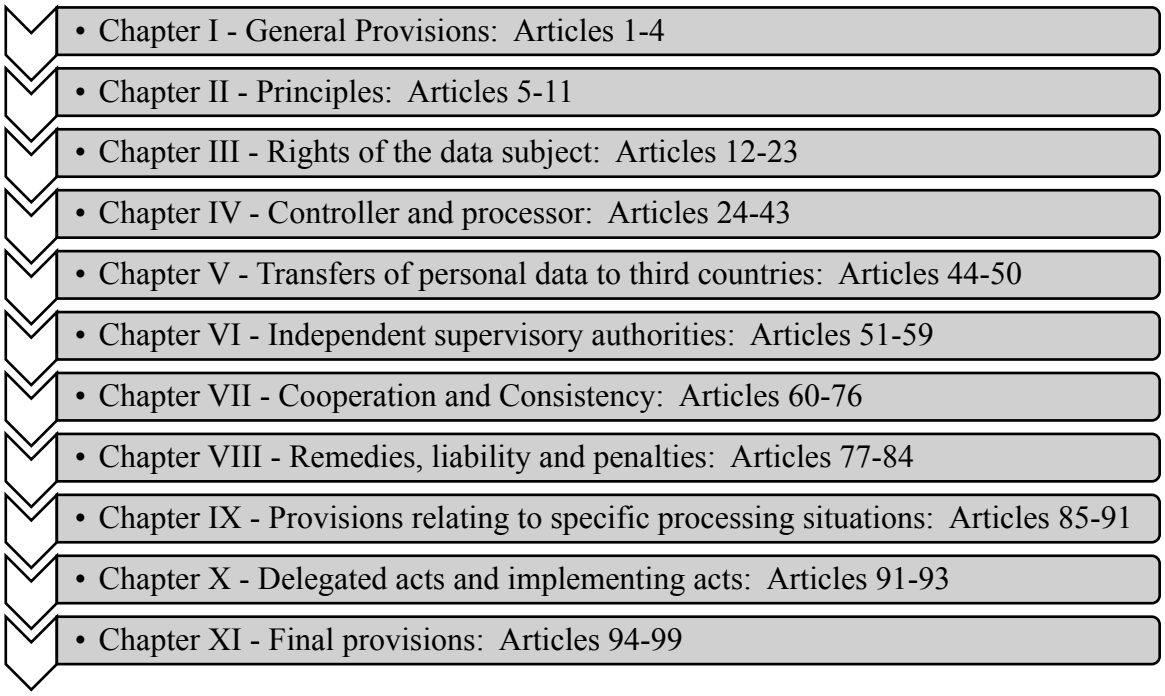


Figure 3: Eleven chapters of the GDPR (own presentation) [51]

2.1.2.3. Impact on the EU

The GDPR tries to set out specific restrictions on the usage and storage of personal data while preserving the interests of both the EU citizen and the organizations that do business within it. An organization that is acting quickly to ensure compliance with the GDPR will thrive in the evolving regulatory environment, potentially also using its compliance as a marketing advantage [53]. In the way of improving existing business practices, some organizations will be able to make essential process improvements and use the standardized regulation to streamline these processes for EU and pan-EU operations for significant efficiency gains [41], [46]. It will further lay a foundation for new proposals on specific digital laws, like the e-privacy directive (especially about internet cookies) for electronic communications [19].

2.1.2.4. Key definition and concepts

The definitions and concepts of this section are limited to provide a minimum understanding of the topic. As the GDPR has around 200 pages, it would be out of the scope of this thesis to provide a very detailed overview [19]. Further definitions and concepts might be introduced in the context of other parts of this thesis later. Others (relating to specific articles or recitals) might not at all be looked at. This study is not a juristic research; hence it is recommended to check the reference section to open the actual legal text if deeper clarification is needed.

The following five terms are used throughout the thesis and should be clearly understood from the outset [51]:

Personal data and data subject (Article 5, Clause 1)

*'**personal data**' means any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

It means that the information is not personal data (or anonymized data) only if there is no way imaginable to link it to a person, pseudonymized data, on the other hand, is data that cannot directly be re-identified. [52]. The personal data definition specifically includes specific data types, such as biometric, genetic and health information, as well as online identifiers. It does not extend any rights to deceased persons [52].

Controller (Article 4, Clause 7)

*'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

This means that the controller determines the purpose and the processing that will be done. To give an example (similar to one from [19]): if a firm X hires a marketing agency to profile and analyze customers, it is very likely that it will only see a result and no actual data points. Given that it determined the purpose for which that data was processed, however, it stays the data controller and the marketing agency the processor. This means that firm X could be made responsible for how the marketing agency handles that data collection.

Processor (Article 4, Clause 8)

*'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

As stated before, these are any organizations or entities that process PII in the name of a data controller. Data processing is essentially considered anything that is done to the data, including its storage. An organization or entity can be both data controller and processor [19]. This point is specifically important for any considerations of processors (third party service providers) outside the EU, as the data controller could still be made responsible by a supervisory authority in such case [52].

Supervisory authority (Article 4, Clause 21)

*'**supervisory authority**' means an independent public authority which is established by a Member State pursuant to Article 51;*

The supervisory authority in other words, is the governmental organisation in each member state that will be responsible for the enforcement of the GDPR [52]. The EPDS is the supervisor of the national

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

authorities that monitors the processing of the national bodies and can step in for specific adequacy decisions in which a national body is not able to conclude a neutral assessment [18].

Other important concepts relevant for understanding are summarized in the following section from a guideline from different law firms and the EDPS annual report [54], [18], [27].

- *The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right: it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights [...], in particular [...] freedom to conduct a business [...].* (Recital 4)
- All personal data of all EU citizens are subject to comply to the GDPR. This means Non-EU companies that aim to process personal data of EU citizens must abide by the GDPR (Territorial Scope, Article 3).
- Automated data processing: *This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.* (Material Scope, Article 2)
- The Right to be forgotten (RTBF) – a data subject has the right to have all related personal data erased (Article 17).
- Consent – the data subject has the right to timeliness, erasure, rectification, access, restriction of usage and portability for their personal data. Information provided should be in clear and plain language stating a specific purpose for using the data. All policies, i.e. terms and conditions, should now be transparent and easily accessible (Article 6-9 and its recitals according to [51]).
- Six privacy principles (Article 5) are applied, namely 1) Lawfulness, fairness and transparency, 2) Purpose limitation, 3) Data minimization, 4) Accuracy, 5) Storage limitation, 6) Integrity and confidentiality.
- Mandatory 72-hour data breach notification to the supervisory authority (Article 33, Clause 1).
- Strong Sanctions – in the case of failure to comply, administrative fines are defined to the limit of 20 million Euros or 4% of global revenue, whichever is higher (Article 83, Clause 5).
- Data protection by design and by default (Article 25) is supposed to address privacy risks not only as a legal restriction for processing personal data, but to meet privacy concerns in the early stage of IT architecture design: *When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.* (Recital 78)

2.1.3. Implications of the GDPR for blockchain

The following Table 2 summarizes the findings of literature – mainly consisting of articles from legal journals or whitepaper of legal and blockchain companies – that specifically included a view on blockchain and the GDPR. After the main topic, the mentioned articles and recitals of the GDPR (only the ones mentioned in the original literature) help to prove the statement, after which the implication for blockchain summarizes the content relating to it. These will be the basis to form the hypotheses by the end of this second chapter.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 2: Mentions of the GDPR and blockchain in existing literature

Topic	GDPR Article/ Recital	Implications for blockchain
Blockchain for GDPR compliance [55]		Usage of BC for an audit trail.
Territorial scope [21], [26]	Art. 3(1)/ Rec. 22, 23	The debate of public versus private BC and who would become the (joint) data controller if data is stored on multiple locations in and outside the EU?
Personal data on the blockchain [21], [26], [24]	Art. 4(1), 6(4),32/ Rec. 26	Can PD be stored on the blockchain or must be off-chain? The connection between pseudonymised and anonymised data and the data subject.
Accountability of data controller [21], [26]	Art. 26(1)/ Rec. 79	Private versus public BC and the accountability of a (joint) data controller.
Privacy by Design versus blockchain core features [21], [27]	Art. 25/ Rec. 78	BC runs counter to data minimisation, storage limitations and a clearly determined data controller, raising the question whether it is in line with 'Privacy by Design' (PbD). Privacy risks of entire IT-architecture, including BC. Solutions could be Enigma or differential privacy or future more secure BCs.
Right to be forgotten (RTBF) and functioning principle [21], [26],[56]	Art. 17,17(1)(a,b), 6(1)(b,f)/ Rec. 69	Can data on a blockchain be deleted in accordance to the RTBF and what would happen if not – could the functioning principle take over that allows for specific interpretations of the GDPR, as BC is at its core designed not to be compliant to the RTBF.
Technical neutrality of the GDPR [21]		Weighing the objectives of BC versus privacy concerns. PbD could be achieved by mitigation measures, lack of data controller could pose the biggest challenge.
Private vs public and permissioned vs non-permissioned BC [21], [26]		This relates to accountability, material and territorial scope.
Data protection impact assessment (DPIA) [26]		Through append-only function BCs often use very sensitive data, resulting in a high risk to the rights and freedom of the data subject (DS) – would always make a DPIA mandatory.
Lawful Processing in the EU [27]	Art. 6	Six reasons can be used to comply with lawful processing, and a data sharing agreement can be recorded on a BC.
Certification for blockchain [24]		Similar to existing regulations (e.g., information security or electronic identity) it is suggested to create a certificate for trusted blockchain users.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

2.2. Blockchain

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete."

This quote from Buckminster Fuller, who was an outstanding American architect and systems theorist, is often used by blockchain enthusiasts to describe the phenomenon of the new digital systems of values that were created and co-existed in parallel to traditional systems [57], [58]. Its best example is the well-known cryptocurrency Bitcoin [59].

The following part will firstly dive into the explanation of blockchain and its main concepts before it summarizes existing privacy solutions that are applied or conceptualized for existing blockchains.

2.2.1. Background and definition

To stay within the scope of this thesis this part will be limited to the main concepts and definitions. The same principle as for the previous part about the GDPR applies, in that further definitions and concepts might be introduced in the context of other parts of this thesis (especially the Delphi study), whereas others might not at all be looked at. The first two sections will look at a brief background and detailed definition of a blockchain. Following a similar structure of the GDPR's Key definition and concepts, other key concepts will be summarized in the third section.

Background

The evolution of blockchain technology began in 2008 with a whitepaper – introduced in a private mailing list called cypherpunks – by an anonymous author or group of authors, who called themselves Satoshi Nakamato: "*Bitcoin: A Peer-to-Peer Electronic Cash System*" [60], [8], [61]. The first use case of blockchain was digital money, also called cryptocurrency (because of the cryptographic technology used for it) [62]. It was created to solve the problem, that individuals must trust centralized financial institutions to manage all digital payments and keep transactions, funds and privacy secure [59], [63].

Trust is the essential element here. The new concept introduced direct digital interactions without trust towards a central intermediary [62]. After other attempts before Bitcoin, it was the first to succeed finally [62].

The second main innovation in the blockchain field followed 6 years later in 2014, by proposing the concept of a decentralized worldwide super computer that can be used for more than just digital money transfers. Intelligent computer algorithms were introduced that can execute code autonomously – a concept called "Smart Contracts" – was presented by Vitalk Buterin and the founders of Ethereum [62], [64], [65].

Along the roads of these two major innovations, it was understood that the underlying technology "blockchain" and thought-concept following it, could be used for decentralizing and decoupling intermediaries in any industry or sector as its know today (e.g. BigchainDB for data storage, or ascribe.io for fair digital art distribution and contribution) [7], [13], [66].

Definition

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Blockchain technology is still under very active development, as for why a formal definition of the terminology has not been established yet [12]. Another challenge presented are the different perspectives blockchain can be viewed from. One ontological approach to describe these views is taken by categorizing blockchain terminology into three layers seen from a transactional perspective shown in Figure 4 [67].

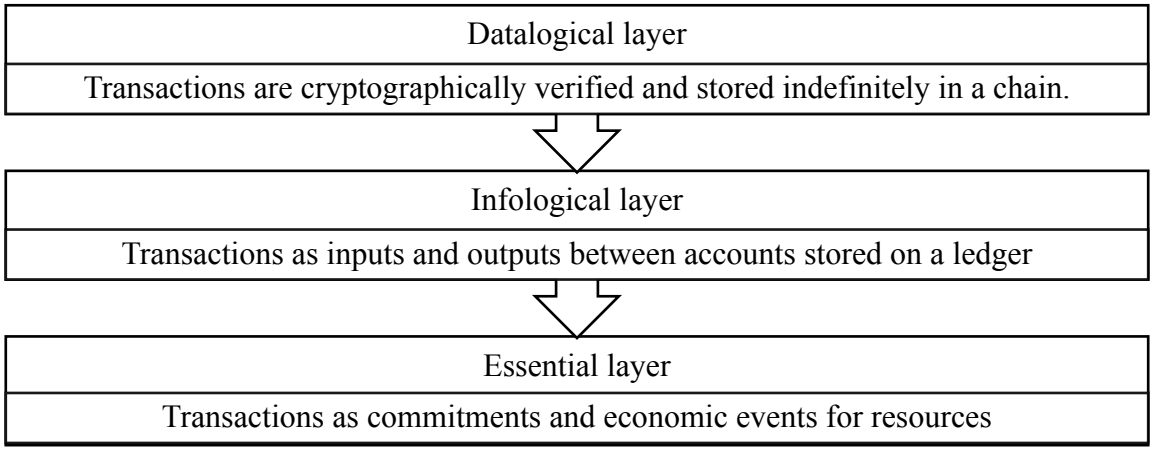


Figure 4: Ontology layers of blockchain transactions based on de Kruijff and Weigand (2016) [67]

The datalogical layer uses a technical view that describes blockchain as a data structure in a technical sense. This is further described in the next section [60], [67]. The infological layer helps to abstract the data structure level by adding information that makes it more accessible for a nontechnical point of view [67]. The term "distributed ledger technology" (DLT) is an example of this layer and adds a new, arguably financially motivated, aspect to it by abstracting the linked list of transactions to a "ledger" [12], [28], [56]. The term DLT is often used interchangeably with blockchain [28]. The essential layer is what is created directly or indirectly by communication, meaning it can present the business, legal or process improving an aspect of a blockchain [68], [69].

To put the last two layers into the context of the potential social change that blockchain brings along, de Kruijff and Weigand describe it as followed [67]:

"Communicative acts typically establish or evaluate commitments. In a narrower sense, a commitment (promise, commissive) is about what an actor is bound to do (so what is right in a future situation). Such a commitment being agreed upon by two parties is a change in the social reality, as is the agreed upon fulfilment of that commitment.

Given the institutional context to be in place, an infological blockchain transaction moving some value from one account to another represents a change in this social reality (e.g. transfer of ownership). Such a change is what we identify as the essential blockchain transaction."

Another angle to defining blockchain terminology is taken by an initiative within the official international standardization work [28], [29]. The author is part of one project that feeds into this work within the German national standardization body – German Institute for Standardization (DIN) – that aims to create a blockchain terminology [70]. In the resulting definition of blockchain, one can implicitly find the aforementioned ontological approach again. As the work is still in progress the

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

outcome presented reflects only the current state of the blockchain definition (it is agreed with the committee to share this information in the context of this thesis). Hence a blockchain is:

A distributed database that is practically immutable by being maintained by a decentralized P2P network using a consensus mechanism, cryptography and back-referencing blocks to order and validate transactions.

Note 1 to entry: A blockchain has a tree shaped structure where each element in the tree is a block that starts with the genesis block at the root, with each block potentially having multiple child blocks. Each child block, besides the genesis block, contains a hash-value of its parent block.

Note 2 to entry: Since adding a child block to the tree involves calculating a new hash over its parent, no block in a tree path can be changed without invalidating the hash of the child block.

Note 3 to entry: Practically immutable means that within the confines of current technology and known attack vectors records are immutable.

Note 4 to entry: Usual blockchain applications connect child and parent blocks to lists, which is only a specific form of the more general tree.

The next section will explore how the blockchain works in more detail, adding more context to the definition.

2.2.2. How blockchains work

This section will take a systematic approach to describing how a blockchain works in more detail. To sum up the previous definition, a blockchain is an innovation that itself relies on three concepts: ***peer-to-peer networks***, ***cryptography***, and distributed ***consensus*** using the resolution of a randomized mathematical riddle. None of these concepts is by itself new but in combination allowed for the computing breakthrough of the blockchain. More details of cryptography used in the blockchain will follow in the next main section: Existing privacy solutions.

2.2.2.1. Exchange of digital values

Decentralized ***peer-to-peer (P2P) networks*** have existed with Freenet or BitTorrent [71]. The blockchain now enables an exchange of values (often referred to as a token), instead of media [62], [72], [73]. These P2P networks are distributed systems that must solve a difficult computer science problem: the resolution of conflicts, or reconciliation [74]. Traditional databases, like relational or object oriented databases, offer referential integrity, but in a distributed system this does not exist [74]. To arrive at a consistent value, the system needs to have rules in place to determine which value is considered valid. One of the toughest problems to solve is the double spending problem, in which one instance sends the same value to the network twice, but only the one arriving first will be excepted as such [63]. The other one will be made invalid. To guarantee integrity within a P2P network, every participant needs, to, therefore agree on the order those values arrive [60]. For that, a consensus mechanism is required. Consensus algorithms for distributed systems have been actively researched for decades (e.g. Paxos and Raft algorithms).

The blockchain uses different ***consensus algorithms***. Currently, the most used algorithm is called proof-of-work consensus, using mined blocks based on electricity power [60].

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

2.2.2.2. Hashes and blocks

A blockchain functions by storing its transaction data (e.g., transfer of value) in digital containers called blocks [10], [60]. Each block is linked to its parent block through unique digital fingerprints termed hashes [10], [60]. A hash is a simply a ***cryptographic*** function that maps data of any arbitrary size to a fixed size, called hash value (or hash) [10], [60].

This is a cryptographic hash value of the first-round Delphi questionnaire word document (see Appendix A), simply created using an online hash generator [75]:

25644cccfd395429c9462929cdfbc5b6d6cd952aed30a432501c847e17883249

By making a trivial change to it (adding a single letter to correct a spelling mistake), the same algorithm produces the following outcome:

7845a160ca8a4ba6691f9dfa2d3342c51b7572e8fbd82727606a9a27fbc9814e

As evidenced before, both hashes are different but have the same length. There is currently no known way to reverse engineer the original input from the cryptographic hash (hashes can be broken, but it is assumed that they are developed along the same time line as the algorithms able to break them) [64], [72]. Figure 5 shows the simplification of a chain of blocks that further uses timestamped hashes in a header at the top of each block of information (the Merkle root, which is basically a hash of all hashes that helps to create a Merkle tree to trace the Bitcoin blockchain transactions without having to download the full blockchain, was left unexplained on purpose as it is out of scope of this explanation) [76].

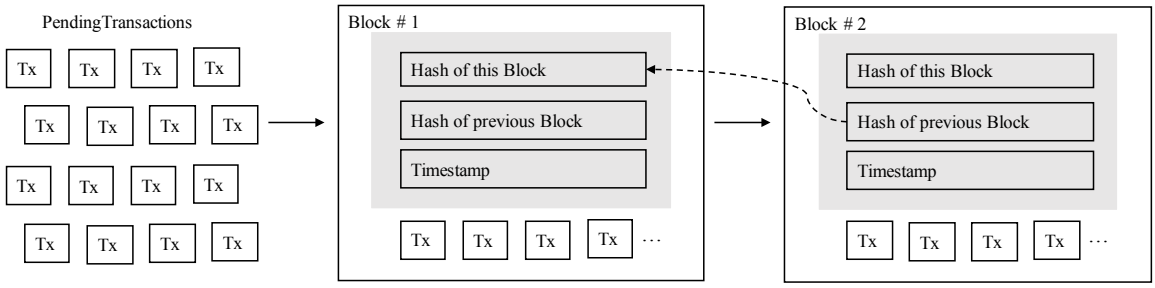


Figure 5: Transactions written to a block chain (own presentation) based on Tschorsch (2015)

This history of transactions stored in the blocks is linked back to the initial or genesis block (for a Bitcoin specific consensus algorithm called proof of work an additional string called nonce is used together with a hash function – can be ignored here) [60]. The information stored in blocks is to its current measures highly tamper resistant (practically immutable) even by those who store and process the information [12]. This is made possible by independent validation nodes that come to a decentralized consensus for every transaction that has occurred [60], [77]. Consensus algorithms ensure that the participants of the P2P network agree on one truth (e.g. Bitcoin uses electricity in their proof of work consensus, other consensus algorithms are used for specific needs and not to be discussed in more detail in the scope of this thesis) [60], [77].

2.2.2.3. Mining

The process of looking for blocks and creating consensus is called mining because block mining brings an economic reward - some form of value (e.g. Gold) [60], [62]. This is the reason why nodes in a blockchain are also called miners. Not every node has to be a mining node; this is a voluntary process that each owner of a node can choose to enable [62]. The process in Figure 6 shows that nodes in the chain create a new local block with pending transactions.

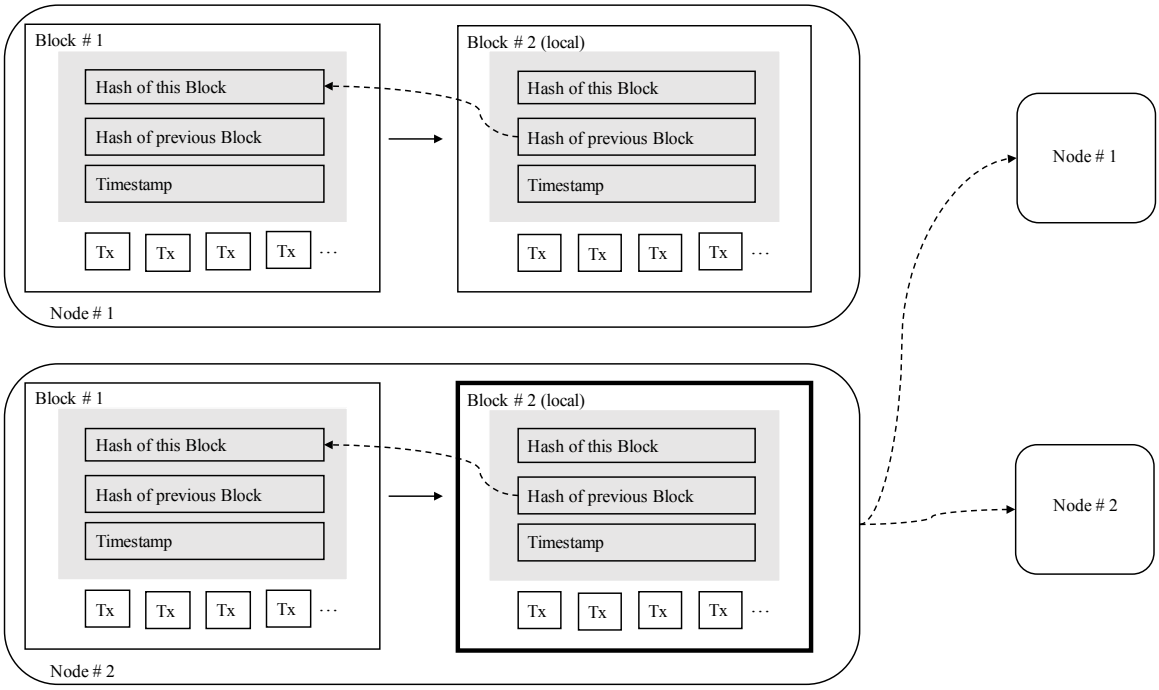


Figure 6: The mining process (own presentation) partly based on Tschorsch (2015)

They compete to find out if their local block becomes the next block in the chain for the entire network, by solving a cryptographic puzzle [60], [76]. If a node solves the puzzle first, then it earns the ability to publish their local block, and all transactions in this block become confirmed [60], [76]. This block is sent to all other nodes in the network. All nodes then again check that the block is correct, add it to their copy of the chain, and try to build a new block with new pending transactions [60], [76]. Finding the random solution and winning the race to validate a block is by design extremely difficult. This further prevents fraud and makes the network safer (unless a false actor owns more than half of all nodes in the network) [60], [76] [12]. Consequently, new blocks get published to the chain at a fixed time interval (in Bitcoin, blocks are on average published every 10 minutes). To not only use the blockchain for storing and exchanging value through transactions, intelligent computer algorithms (or programs) were added to the construct [78], [79].

2.2.2.4. Smart contracts

A blockchain can execute so called smart contracts, which are programs that replicate together with the transactions, and every node executing them when receiving these transactions [78], [79]. This allows for a distributed consensus on the execution of a promise coded into the blockchain. The idea of pre-

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

programmed conditions, interfaced with the real world, and broadcasted to everyone, is the second core reason for the blockchain evolution [78], [79], [64], [65].

A legal contract in the real world is a promise that signing parties agree to make legally-enforceable [80]. A smart contract is essentially the same, except being truly deterministic and only technical enforceable [64], [65]. Smart contracts in a blockchain could allow getting rid of the bank, the lawyer, and the court by just writing a program that defines how much money should be transferred in response to certain conditions [78], [79], [64], [65]. To interact with the real world, blockchains need sensors and actuators. The applications relying on smart contracts are called Decentralized Apps (DApps) [78], [79], [64], [65]. The next step in the blockchain revolution is therefore directly dependent on the evolvement of mainstream IoT adoption [78].

The strength of the Bitcoin and Ethereum blockchain lies in there fully decentralized characteristic, which also brings many downsides when thinking about values and transactions that need to be kept private [64].

2.2.2.5. Public, private, permissioned and permission less

Just like a database, a blockchain can be private or public and permissioned or permission less [12], [73].

A public blockchain (e.g. Bitcoin or Ethereum) is characterized by being open to any entities that want to join the P2P network, on the other hand, a private blockchain only allows pre-selected participants in the P2P network [12], [73].

The other differentiate the entities that are authorized to conduct the consensus process. In a permissioned blockchain, these entities are pre-selected, whereas in the permission less blockchain anyone is allowed to participate in that process (e.g. Bitcoin miners) [12], [73].

To list a few examples, a group of the largest banks around the world is working on a private, permissioned blockchain that enables global payments for its internal use, called Ripple [49]. Another blockchain network called Interplanetary Database (IPDB) offers a permissioned public blockchain with the aim of allowing anyone to store data immutably, but by pre-selecting the consensus processing nodes to provide fair governance [81].

Governance is one of the big pain points of existing blockchain solutions, as it becomes difficult to make a bad actor accountable for his behavior in a fully decentralized system [82]. This directly relates to the issue of privacy [83]. Since the invention of blockchain in 2008 many approaches and potential solutions have been thought of to solve the issue of privacy, the next section will explore which ones.

2.2.3. Existing privacy solutions

Privacy concerns in blockchain solutions should be differentiated for private and public blockchains, but in both cases present a valid concern [84]. For public blockchains statistical tools, like a graph analysis in combination with web scraping tools have been used to re-identify Bitcoin wallet holders and private keys [84]. It works by tracking transactions on multiple layers and combining them with many data sources (e.g., public Bitcoin transactions with IP addresses) [84]. The same issues arise for private blockchains, adding to it, regulatory and security concerns that need to be solved to make blockchains usable for real business cases [84], [48].

The cryptography used in current blockchain implementations is called asymmetric cryptography, which uses a pair of keys [72], [85]. One that is designated the private key and kept secret and the other that is called the public key is made available – this is also referred to as public key cryptography and was found by Diffie, Hellman and Merkle (1980) [86]. It is best described by a figurative vault that has two locks, one to lock it and one to open it [86]:

1. X (sender) and Y (receiver) each generate a key pair and make one public.
2. X can use their private (locking) key to lock a message in a vault.
3. X can then put this message vault into another larger vault and lock it with Y's public key.
4. Y can then open this larger vault with their private key and get X's message vault.
5. Y completes the magic (figuratively) by using X's public key to open the message vault.

This mechanism solved the problem of intent, thus creating a digital signature [87]. These signatures are currently used for blockchain wallets and cryptocurrency exchanges [88]. To increase privacy in public and private blockchains cryptographers have come up with many techniques to avoid any re-identification through statistical analysis. Since cryptography is a highly complex topic, the following two tables take an approach to briefly summarize these techniques through a comparison based mainly on two blog articles from Buterin (2016) and Samman (2016) [87], [88]. Table 3 showed the well-known and tested cryptography (run over many years and mostly already broken by someone), whereas Table 4 is showing cutting-edge cryptographic techniques [87], [88].

The tables name the techniques, followed by an explanation and their limitation. Application using the technique presents the last column. Often the practical applications will use a combination of techniques to increase security and privacy. This fact is indicated by an application being underlined and employed in multiple parts of the tables (e.g., Monero uses stealth addresses and ring signatures).

Table 3: Well-known cryptographic techniques [87], [88], [84]

Technique	Explanation	Limitation	Application
One-time keys	New keys are generated for each transaction.	Accounts can be linked if the keys are consumed by two at the same time. Managing accounts is bound to human error.	Zcash, TrumbleBit [89], [90]
Stealth Addresses	One time transaction address is created that uses hashed one-time keys.	Privacy only for a limited time, if transactions are later stored in public BC transactions are again traceable.	CryptoNote protocol used by Monero and Bitcoin wallets, TrumbleBit [82], [83]
Mixing and washing	Obfuscates accounts (senders and receivers) through mixing them together, so that the transaction cannot be seen anymore.	Trust on third party providers to do the mixing or danger of mixing that can be untangled.	CoinJoin (has been broken by CoinJoin Sudoku. TrumbleBit [93], [94]
State Channels	Maintains authentication benefits (additionally to	Ones the blog is moved to the BC, its last state will still	TrumbleBit,

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

	privacy) by moving transaction of one block into off-chain channels for the same set of participants (multi-signatures), while business logic can be hashed into the BC, comparable to escrows.	be visible again, this risk can be reduced by a combination of other techniques.	Litecoin (for Bitcoin BC), Raiden (for ethereum BC) [95], [96]

Another explanation of encryption in the words of Breitman (2016), another thought leader in encryption and identity, helps to understand the next table better [97]:

"Encryption refers to the operation of disguising plaintext, information to be concealed. The set of rules to encrypt the text is called the encryption algorithm. The operation of an algorithm depends on the encryption key, or an input to the algorithm with the message. For a user to obtain a message from the output of an algorithm, there must be a decryption algorithm which, when used with a decryption key, reproduces the plaintext."

Table 4: Cutting edge cryptographic solutions [87], [88], [84]

Technique	Explanation	Limitation	Application
Ring signatures	(Hashes) keys are put into a key ring that allows for a digital signature to be derived from a group of possible public keys.	Hard to integrate into protocols, as it involves complicated cryptography.	Monero
Zero knowledge proofs (or zk-SNARKs)	Each party will only get a binary reply to a privacy related question, i.e. a Yes or a No without the need to know the actual content of the reply (e.g., age for a driving license has to be over 18 in Germany, only that has to be known to drive, not the actual age).	Heavy computation needed, eventually dependent on the third party to provide the proof (e.g., government)	Zcash, Hawk [64]
Commitment schemes	A message is sent to a receiver, but can only be opened later, after a certain commitment has been fulfilled.	Not a stand-alone solution.	Zcash, Blockstream [98]
Sidechains	Similar the escrow idea of state channels, but bound to a certain commitment before being activated.	Only in combination with other techniques truly able to increase privacy.	Blockstream (enables so called confidential transactions)

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Homomorphic encryption	Homomorphic encryption is a used to perform calculations on encrypted information without decrypting them first.	Heavily increased computation times.	Blockstream
Indistinguish-ability obfuscation	A program is put into a black box, while keeping its internal logic unknown and still creating the same input and output.	Very high computational power, very complex to set it up.	Not used in practice yet

In private blockchain environments, often consortiums are formed in which the members compete, but see a benefit of using a shared, secure and unchangeable data source for transactions between them (e.g. R3 with Ripple) [49], [92]. Another consortium is the Digital Asset group, which conducted one of the most conclusive studies on privacy solutions for blockchain, finding that personal data should never be stored on a blockchain [99]:

"Reflecting the requirements of both customers and their regulators, it is Digital Asset's position that confidential data should never be stored by a party not entitled to view that information, even if obfuscated or encrypted."

Vitalik Buterin, the founder of Ethereum, adds to this by summing up privacy related issues to blockchain in the following way [87]*:*

"In these cases [blockchain used for more data-centric application like timestamping, high-value data storage, proof of existence (or proof of inexistence, as in the case of certificate revocations)], it is once again important to note that blockchains do NOT solve privacy issues and are an authenticity solution only. Hence, putting medical records in plaintext onto a blockchain is a Very Bad Idea. However, they can be combined with other technologies that do offer privacy in order to create a holistic solution for many industries that does accomplish the desired goals, with blockchains being a vendor-neutral platform where some data can be stored in order to provide authenticity guarantees."

This thesis aims to find out how such authenticity guarantees could look like with regards to the GDPR and in what context personal data could be protected in a solution that includes a blockchain in its architecture.

The next section will explore the hypotheses which were from with the knowledge of parts above of this chapter.

2.3. Hypotheses

The main research hypotheses are supposed to provide the basis for the creation of the first set of questions for round one of the Delphi study as well as answering the open questions presented in the literature review. The primary objectives of this thesis, as drawn up in the Research Goal section, were to find out about the *"interrelationships between blockchain and the GDPR".*

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

To conclude with five general research hypotheses, the six research questions (three from each view) from the same section were put into perspective of the literature review:

1. *What is the impact and relevance of the regulation towards the development of blockchain technology?*

   What should be done to help blockchain developers to become GDPR compliant, without hindering its innovative impact?

The previous section about the Implications of the GDPR for blockchain reflected the limited current state of research about both topics relationship to each other. The hypotheses drawn from it are:

H1: Blockchains have an impact on personal data.

H2: Data protection regulations will have a relevant impact on blockchains related to personal data.

2. *How to make a blockchain compliant to the new regulation?*
   Can a blockchain be privacy-friendly by being developed along the principles of privacy by design?

Looking at the same part, but also keeping in mind the Existing privacy solutions, the following two hypotheses are formulated:

H3: Personal data cannot be stored on the blockchain directly, but indirectly.

H4: Blockchains can be designed in a privacy-friendly manner by using the approach of privacy by design.

3. *How could a blockchain be used as an application for GDPR compliance?*
   How could a blockchain help regulatory bodies?

To create the two-sided perspective and relating to both previously mentioned parts the following hypothesis finalizes this view:

H5: Blockchains can help to solve (privacy) challenges accompanying the implementation of the new GDPR.

The next chapter will explore the research methodology, using the knowledge gathered and the hypotheses drawn to design and formulate the Delphi study questionnaires.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

3. Chapter: Research Methodology

This chapter provides an overview of the chosen methodology, the Delphi method (interchangeable with "Delphi" and "Delphi study).

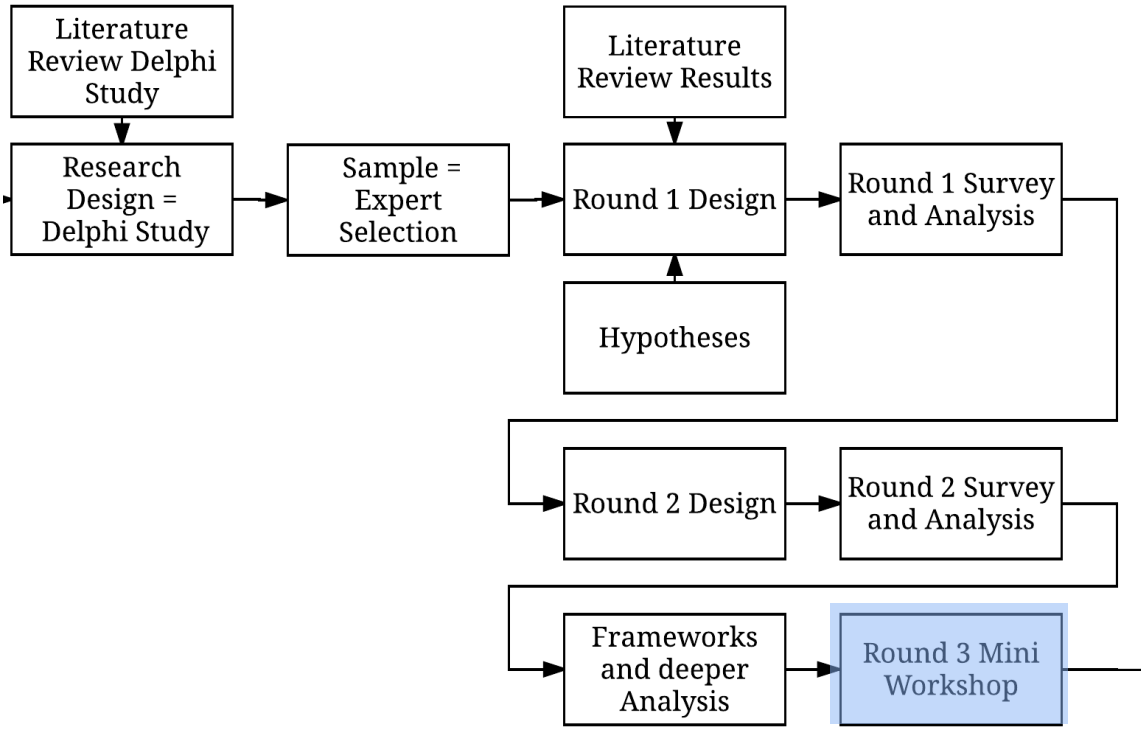


Figure 7: Zoomed in Delphi study in Research Process cut out from 1.

Along the lines of the high-level research process, Figure 7 visualizes how this chapter will start with the background of the Delphi method succeeded by its suitability assessment. In an upcoming step, the selection procedure and background of the expert panel (the research sample) are introduced. Followed by the questionnaire design, that includes the research hypotheses, and in between analysis, the chapter ends with the actual data collection. Deeper analysis, framework concepts and recommendations are discussed in the subsequent chapters.

3.1. The Delphi Method

3.1.1. Background

The Delphi method is an iterative and structured group interaction process used for obtaining consensus and gathering future outlooks on a complex topic [100]. First developed by the military backed RAND corporation in the 1950s, the objective of the original study was to "obtain the most reliable consensus of a group of experts ... by a series of intensive questionnaires interspersed with controlled opinion feedback." [31].

The typical Delphi steps (simplified) are shown in Figure 8:

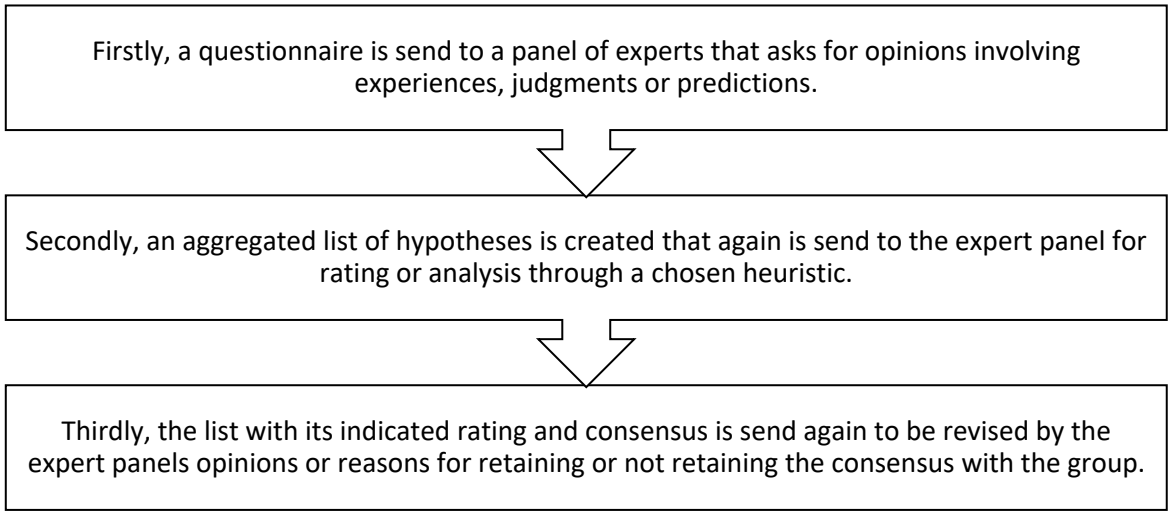


Figure 8: Typical Delphi steps - (own presentation) based on Pfeiffer (1968) [101]

Today, the Delphi method is used to form diagnosis, prognosis and prescriptions in a variety of research areas [33]. The number of rounds and participants of a study depends on the convergence or cohesion of the respondents, and not necessarily on the consensus. Coates (1975) found that [102]:

"The value of the Delphi is not in reporting high reliability consensus data, but rather in alerting the participants to the complexity of issues by forcing, cajoling, urging, luring them to think, by having them challenge their assumptions."

This research aims to discover mutual relationships between blockchain and the GDPR - while triggering new thought processes, gathering diverse opinions and strengthening the topics understanding – of an expert panel.

Regarding this study and the diverse subject of blockchain on the one hand and data protection, in the form of the GDPR, on the contrary– two different fields were looked at. As blockchain at its core belongs to the technology sector and the GDPR to the policy sector, propriety is proven by looking at previous uses of the Delphi method in these fields.

In Information Technology (IT) and Information Systems (IS) research, the Delphi study has been used to specify and determine project requirements and criteria for prototyping or ranking of technology management issues in new product development projects [103]. The method has since been modified in many ways, and while a typical Delphi study consists of three rounds, many subsequent studies have used one, two or four rounds. According to Skulmoski, Hartman and Krahn (2007), sample sizes within these studies varied from 4 to 171 experts [103].

Policy Delphi studies, which seek to generate the strongest possible opposing viewpoints on a policy issue from expert panels, have been used since 1980's and are used in actual policy evaluation and development, e.g. by the European Commission JRC [104]. These studies can consist of multiple expert panels in different fields, and sample sizes are significantly bigger, as these studies are often well funded and led by expert teams [104].

The following strengths and limitations play to suitability section that follows and were considered when designing the questionnaires for each Delphi round.

Strengths

According to Yousuf (2007), the Delphi method is useful when other methods are not adequate or appropriate for collecting data of a complex topic [101]. The method is described to be particularly useful when:

1. *The problem does not lend itself to precise analytical techniques but can benefit from subjective judgments on a collective basis.*
2. *The individuals needed to contribute to the examination of a broad or complex problem have no history of adequate communication and may represent diverse backgrounds concerning experience and expertise.*
3. *More individuals are needed than can effectively interact in a face-to-face exchange.*
4. *Time and cost make frequent group meetings infeasible.*
5. *The efficiency of face-to-face meetings can be increased by a supplemental group communication process.*
6. *Disagreements among individuals are so severe or politically unpalatable that the communication process must be referred or anonymity assured.*
7. *The heterogeneity of the participants must be preserved to ensure the validity of the results, i.e., avoidance of domination by quantity or by the strength of personality.*

Weaknesses

Linstone and Turoff (2002) identified five main reasons for Delphi studies to fail or not work as intended *[31]*:

1. *Imposing monitor views and preconceptions of a problem upon the respondent group by over specifying the structure of the Delphi and not allowing for a contribution of other perspectives related to the problem.*
2. *Assuming, that Delphi can be a surrogate for all other human communications in a given situation.*
3. *Poor techniques of summarizing and presenting the group response and ensuring common interpretations of the evaluation scales utilized in the exercise.*
4. *Ignoring and not exploring disagreement so that discouraged dissenters drop out and an artificial consensus is generated.*
5. *Understanding the demanding nature of a Delphi and the fact that the respondents should be recognized as consultants and adequately compensated for their time if the Delphi is not an integral part of their job function.*

3.1.2. Suitability

As Delphi is not the only option for exploring theory from qualitative data, the choice of the method is based on considerations of a) the nature of the research problem, b) interaction and consensus within an expert group, c) practical feasibility and d) comparison to other methodologies.

a) Nature of the research problem

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

As proven in Chapter: Background and Literature Review, both research topics are very new and hugely complex, hence subject to unknown circumstances. This means it does not lend itself to precise analytical analysis, which plays to the strength of the Delphi study to benefit from "subjective judgments on a collective basis" [101].

b) Interaction and consensus within an expert group

As defined previously, the Delphi method helps to structure a process for communication between individuals. These individuals are expected to have different views on the topics, as they come from various fields of expertise. The Delphi study helps to conclude with general frameworks that summarize collected consensus and dissent. It also prevents the bias through its following core characteristics, identified by Dalkey (1967) as [101]:

1. Anonymity – the participants, will not know of each other;
2. Controlled feedback from the interaction – reduction of disorder among participants through aggregated hypotheses during the interview rounds to evaluate answers in comparison to the groups' opinions; and
3. Statistical group response – the individual views can be analyzed through quantitative and statistical measures to be compared to a final group response.

c) Practical feasibility

Many experts would not be able to attend a personal meeting at a pre-determined place and time, as they usually adhere to time and location constraints within their professional obligations. The Delphi study overcomes these constraints, by giving the respondents flexibility towards answering the questionnaires digitally and in their own time.

d) Comparison to other methodologies

In the following Table 5, specialists from the European Commission have compared different research methods to understand their applicability. It is not within the scope of this research to examine each methodology in more detail.

For understanding the suitability of the Delphi method for this study, the table shows its benefits across all factors considered. Specifically, it is exploratory but still structured (not open) nature, and its quantitative and qualitative capabilities benefit to the purpose of this research on the GDPR and blockchain.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 5: Comparison of Research Methods and Tools, created and adapted by the EU JRC from the Futures Research Methodology [30], [104]

Methods & Tools	Diagnosis		Prescription		Qualitative		Exploratory		Open
		Prognosis		Quantitative		Normative		Predictive	
Environmental Scanning & Monitoring	XX			X	X				
System Dynamics	XX			X	X		X	X	
Structural Analysis (e.g. MICMAC)	XX			X	X		X	X	
Agent Modelling (e.g. MACTOR)	XX				X		X	X	
SWOT Analysis	XX	X			X		X	X	
Trend Intra & Extrapolation	X	XX		X	X		X	X	
Modelling & Simulation	X	XX		X			X	X	
Gaming	X	XX			X		X		X
Creativity Methods (Brainstorming, Mindmapping…)	X	XX	X		X	X	X		X
Expert Panels		XX	X		X	X	X		X
Delphi survey	X	X	X	X	X	X	XX	X	
Backcasting		X	XX	X	X	X		X	
S&T Roadmapping		X	X		X	XX	X	X	
Critical & Key Technology Study	X	X	XX	X	X	X		X	
Scenario Building		XX			X	X	X		X
Morphological Analysis & Relevance Trees		XX	X		X	X			X
Cross-Impact Analysis (e.g. SMIC)		XX		X	X		X		X
Multi-Criteria Analysis (e.g. MULTIPOL)			XX	X	X	X		X	

The Delphi method has finally been chosen as it is not a substitute for other scientific examination, but rather an option for complex and intertwined subjects that cross over disciplinary boundaries [100]. It is proposed to conclude practical recommendations and aggregated frameworks, that help better understand the implications of the interrelationships between blockchain and the GDPR.

3.1.3. Participant Selection and Background

To select an appropriate expert panel the following four requirements have been identified (Ashton 1986; Bolger & Wright 1994; Parente, Anderson, Myers, & O'Brien, 1994) for "expertise" [103], [91]:

a) Knowledge and experience about the topic

As blockchain is a relatively new topic, whereas personal data protection (includes the GDPR) is not, experts with different measures for expertise were selected from the field of data protection and blockchain, or both. Since experts with extensive knowledge or experience in both areas are difficult to find, some participants had knowledge of blockchain or data protection, but were still regarded as able to provide useful input. Blockchain experts come from various backgrounds, because the technology brings together legal (private and public law), business and technological expertise. Figure 9 shows the combined expertise of 643 years across the 4 categories of considered important for this study. It considers all experts replies that took part in either round one or round two of this Delphi study and proofs a high degree of collective knowledge and experience. To put this number into a vague perspective – the first data protection regulation was proposed 47 years ago and the first mention of

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

blockchain in the context of this research 9 years ago (see Chapter: Background and Literature Review for clarification).

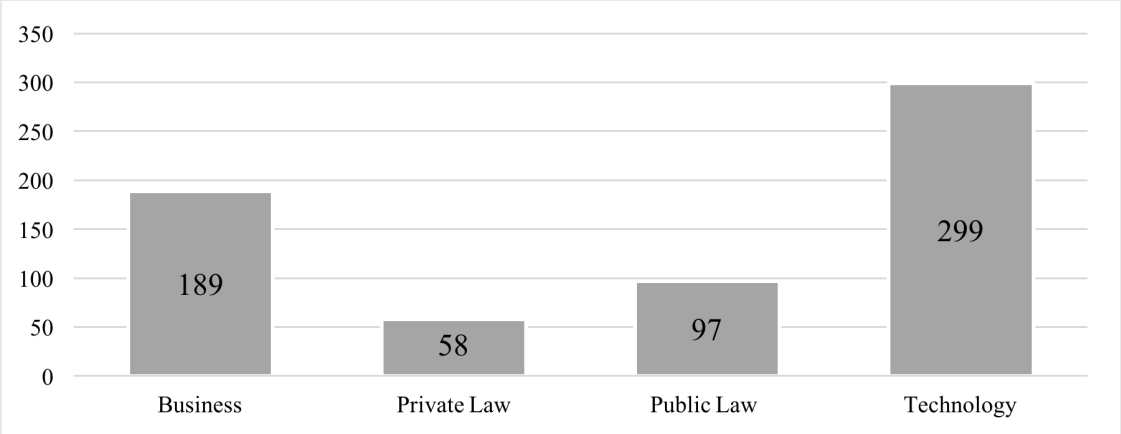


Figure 9: Combined experience in years of the expert panel in 4 categories (own presentation)

This information has been drawn from a self-assessment section that was added to each rounds questionnaire to further determine the experience and knowledge of the experts, based on a similarly described Delphi study (Schmidt, 1997) [105]. As an additional measure of expertise, it was asked how many years were spend in study specific fields (blockchain and data protection regulation) and how many study specific projects have been conducted. A project, defined by the Cambridge Dictionary as "a piece of planned work or an activity that is finished over a period of time and intended to achieve a particular purpose", helps to further evaluate the level of experience [31], [106]. The concluding data will follow in the next sub-chapter about the Data Collection and Questionnaire Design. To summarise, for this study the experts are pragmatically defined along the lines of the Oxford Dictionary as [107]:

Specialists in either or one field mentioned before, that bring along enough experience and knowledge to be able to provide grounded in-depth answers to the questions in each round of this Delphi study.

b) Capacity and willingness to participate

All experts have been individually invited to participate on a voluntary basis and where only bound to their own interest in the study itself.

c) Sufficient time to participate

In each round the experts had approximately two weeks to participate. A regular reminder was send and the total time effort to answer each questionnaire varied from 20 to 60 minutes.

d) Effective communication skills

In the time the survey was send, each expert worked in an institution that requires excellent communication skills to be able to exceed in their field.

The experts where selected and contacted based on recommendations through business contacts sponsored by BigchainDB GmbH, outreach to regulatory and government officials through official

channels (e.g., contact form of EPDS, website of Jan Philipp Albrecht) and personal contacts made through the authors work in standardisation committees (e.g., work on international blockchain standards in the German mirror committee for the ISO TC 307) [47]–[50]. Additional contacts where found through research and outreach to journal and magazine authors (e.g., c't articles, IEEE and ACM paper) and research on LinkedIn [96]–[99].

Experts where invited from different EU countries, as the GDPR is of substantial interest for this localization. One exception was made for an expert from South Korea, who is leading the international standardisation initiative about blockchain and identity. Figure 10 shows the countries of residence of the experts that participated in at least one round. Most of the participants live and work in Germany, which is also the authors country of residence. The focus on Germany can be considered a good choice and not a bias, because on the one hand it is known for its high expertise and strictness in privacy regulations and on the other hand it provides a central hub for blockchain technology experts from all over the world, i.e. the country of residence does not equal the country of origin and therefore does not create biased opinions [113], [114].

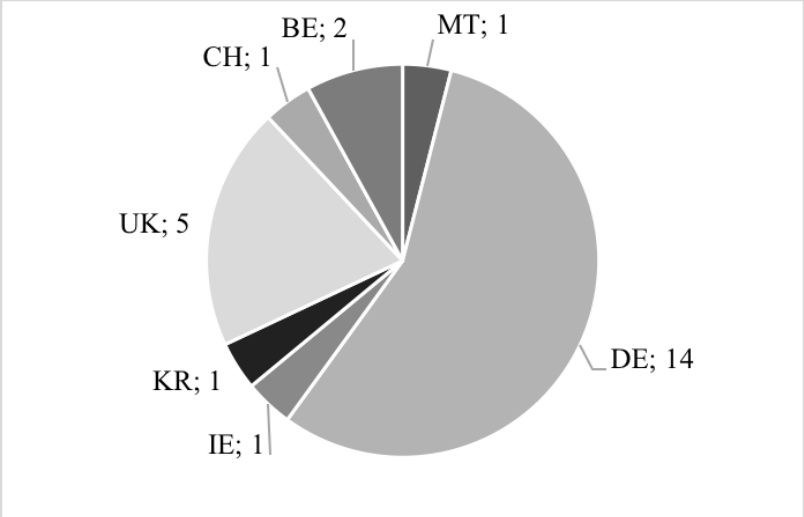


Figure 10: Country of residence of the expert panel (own presentation)

3.1.4. Questionnaire Design

Before jumping into the specifics of how round one and round two of the Delphi survey were created, it is noted that the questionnaire designs within a Delphi study vary greatly[74], [77], [78]. This is partly based on the nature of the research question and partly on the subjective view and creativity of the researcher [33], [103]. The author decided to use the structure of a Delphi study of one of his supervisors as a benchmark to design the Delphi along those lines [77]. Round one of the study is used to ask semi-structured questions related to the initial research hypotheses. Round two aggregates the replies of round one and gives the expert panel the opportunity to rank these along a Likert Scale, still allowing for additional comments [116]. Because of the nature of the research topic – a complex future focused topic, that increases difficulties for consensus, because it draws from opinions of predictive and subjective nature – and in contrary to traditional Delphi studies, an optional round three in the form of a mini-workshop was suggested to discuss resulting frameworks and recommendations in a face to face setting.

Each round was performed as an asynchronous study via E-Mail – which in contrary to a synchronous study with immediate replies (like an interview) – leaves the experts the time to reply to the questionnaires in their convenient time and location. Through to consideration of the experts limited time constraints, each round was designed for a possible completion under 30 minutes. In the spirit of the GDPR each expert was additionally given the option to consent to agreeing to have his name published with regards to this study.

3.1.4.1. Delphi round one

The first round of the Delphi study was send as a Microsoft-Word document. None of the participants had trouble using this format. To make sure the questionnaire is well perceived, extra care was taken to properly design this first round.

In Figure 11 the structure of the first document shows that participants firstly received information on the background of the study and its organizational questions (in FAQ form) in alignment to the key question of an information brochure, as Grisham (2008) calls it [79]. It included the option to participate via verbal communication, which was not taken by any participant. A self-assessment helped to identify the panelists' background in the next part, followed by knowledge material and the main definitions of the GDPR. The author purposefully did not include such material for the blockchain topic, for the following reasons:

1. The GDPR precisely defines its content, whereas blockchain is not yet clearly defined or standardized in a uniform way (see Chapter II).
2. The experts in the panel received a link to the same objective informational website, if they did not already have at least a basic understanding of blockchain [96].
3. To further ensure that experts only replied within their own level of expertise, it was clearly stated in round one and two, that participants could choose to answer only the questions (and detail) of their comfort zone.

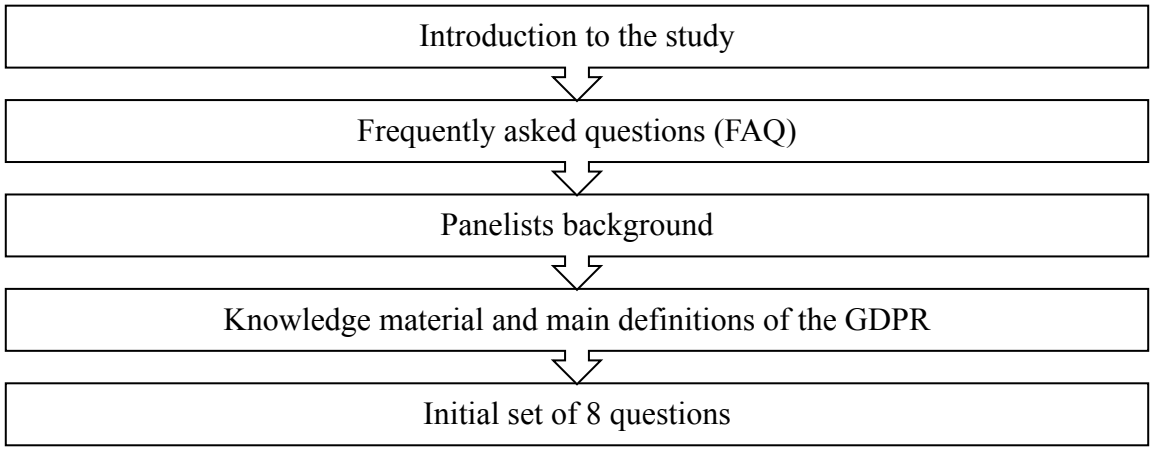


Figure 11: Structure of Delphi round one (own presentation)

The introductory parts mentioned above led to the last and core section of this questionnaire – the initial set of 8 partially structured or open ended questions based on the Hypotheses drawn in Chapter: Background and Literature Review [118]:

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

H1: Blockchains have an impact on personal data.

Question 1: In what area do you believe blockchain technology will have the most significant impact with regards to personal data?

H2: Data protection regulations will have a relevant impact on blockchains related to personal data.

Question 1.1: In the area you specified, do you feel the consideration of data protection regulation to be relevant when developing blockchain technology? Elaborate shortly.

H3: Personal data cannot be stored on the blockchain directly, but indirectly.

Question 1.2: When developing blockchain in this area, what constitutes personal data in that context?

Question 1.3: Now consider the development of blockchain technology in this area. How would you store this type of personal data on a public blockchain?

H4: Blockchains can be designed in a privacy-friendly manner by using the approach of privacy by design.

Question 1.4: Keep considering the development of blockchain technology in this area. Will blockchain technology be compatible with the personal data protection system by design and by default? Elaborate.

H5: Blockchains can help to solve (privacy) challenges accompanying the implementation of new the GDPR.

Question 1.5: Now consider the perspective of a regulator. What role could blockchain play to help regulate personal data protection?

Question 1.6: Keep considering the perspective of a regulator. What data protection problems can you see blockchain technology to be solving?

Question 2: From your own perspective and outside the scope of the chosen area. What relationship between blockchain and personal data regulation would you wish for in the future?

The questions were written based on the hypotheses from Chapter II. The first set of questions under 1 were asked from a specific point of view, to give the expert the chance to put an answer into perspective. Questions 1 to 1.4 consider the implications the GDPR has for blockchain, questions 1.5 and 1.6 review the other position by asking how blockchain can be of help for the GDPR and its authorities. Question 2 asks an open-ended question specifically about a future for the two topics.

The completion of this first round by 19 experts resulted in a list of 145 statements, grouped into the 8 questions above. All answers were transferred to a Microsoft Excel table, coded into indexes and broken down to fragments, that helped to add up statements with duplicated content. The indexes were used to rank these statements to see a first expert consensus through the number of duplicates. This left a list with 93 statements, forming the basis for the design of the second Delphi round.

3.1.4.2. Delphi round two

For the second Delphi round the list with 93 statements was taken and the statements were re-written and aggregated to 72 hypotheses (can contain formulated hypothesis and longer statements) categorized in limitations, opportunities and general hypotheses. A self-assessment section was left optional and only to be filled out by the participants that did not participate in round one.

The final list was rated and commented on by the 18 experts through a "Google Form" questionnaire within the categories shown in Figure 12, that are aligned to the initial 8 questions from round one.

I.	Blockchain	
	I.	Blockchains impact on personal data
	II.	Relevance of data protection regulations for blockchain applications using personal data
	III.	Defining Personal Data
	IV.	Storing personal data on the blockchain
	V.	Privacy by Design and blockchain
II.	Personal Data Protection Regulations	
	V.	Blockchains role for data protection regulation
	VI.	Blockchain solving data protection problems
	VII.	Recommendations and Expectations for blockchain and data protection

Figure 12: Categories for Delphi round two (from actual questionnaire, own presentation)

The experts were asked to select their level of agreement on a five-point Likert scale for each hypothesis [49]. Inspired by a design thinking mind-set and through to the challenge of the summarization task (it turned out to be a real challenge, that was only solved through this very systematic approach and the consideration of design thinking) many initial statements were left unchanged [119]. On the one hand, the author meant to avoid research bias and felt that the implied context could get lost, on the other it was intended that these made it harder to be answered with one level of agreement so that this would trigger the creative minds of the experts and inspire them to leave thoughtful comments. This intention led to critique from some experts in the feedback section but gathered insightful replies from others.

Additionally, for some hypotheses the experts were asked to rate its technical and legal feasibilities. This way the chance of technical implementation and the possibility to fit into legal structures could be separated from the value of the initial ideas. The experts were further encouraged to provide comments and arguments on their choices and on the hypotheses in general.

3.1.4.3. Delphi round three

Within the existing time constraints of the author, it was planned to conduct a third Delphi round in the form of a face to face workshop with a few participants to gather detailed feedback about the

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

frameworks and analysis resulting from round two. Unfortunately, due to the time constraints, this third round could not be conducted. It does, however, present a logical next step for further research.

3.1.5. Data Collection

In total 45 experts, according to the pragmatic definition, were contacted. 35 of these replied of whom 25 responded positively and the major reason for a negative response was time. 19 experts completed the first questionnaire and 18 the second with an average response rate of around 75%. For the Delphi method group size does not depend on the statistical power, but rather on the size with the highest chance on arriving at a consensus that covers the important issues [120]. For this reason, Ludwig (1997) had documented the "majority of Delphi studies have used between 15-20 respondents and run over periods of several weeks" [120]. This Delphi study lies well within these parameters.

Table 6: Experts' backgrounds, response rates and time durations

		Responded	Accepted	Round 1	Round 2
Duration		7 days		16 days	15 days
Panel Size	Blockchain Vendor	11	8	7	6
	Consultant	11	6	5	4
	Researcher	8	6	4	6
	Client	3	3	2	1
	Government Agency	2	2	1	1
	Total	35	25	19	18
Response Rate		78% of 45 invited	71% of 35 responded	76% of 25 accepted	72% of 25 accepted

A summary of the self-assessment section in Table 6 shows the response rates and the time duration experts were given for their replies. Some experts only replied to the first round of the questionnaire, whereas others only to the second. It further shows the panels' professional background. To reduce bias towards one profession and gather as many diverse opinions as possible the following five professions have been identified:

a) Blockchain Vendor

Blockchain start-ups and venture capitalists that provide or invest in a software solution related to blockchain technology.

b) Consultant

Blockchain and legal consultants, including lawyers from law firms, independent contractors and employees of well-known consultancies (e.g., Big 4 Accounting Firms) [121].

c) Researcher

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Researchers and journalists of either the topic of blockchain or privacy regulations from universities and private research institutes.

d) Client

Large enterprises working on implementing blockchain and privacy solutions.

e) Government Agency

Governmental authorities that are part of either creating or enforcing privacy policies and regulations.

Table 7 confirms the previously mentioned study specific experience, measured in number of years and number of projects. It is concluded that participants within the data protection field have considerably more experience in their field, as blockchain is still a relatively new topic (see Chapter: Background and Literature Review). Experts in both fields seemed to have touched both topics along their careers. It is possible to conclude that the two topics are of interest to each other, as only five people in each field seem to have no experience in the other field. The discrepancy between number of years and projects on the left side shows that experts at some point had to at least educate themselves about the topic of blockchain (5 people have no "Years" experience, but 8 have no "Projects"). On the contrary, for personal data protection, it seems understandable that most experts touched the topic in some way or the other in a project related matter (5 people have no "Years" experience, but only 4 have not done a project).

Table 7: Participants' study specific experience

Blockchain				Personal Data Protection			
No. Years		No. Projects		No. Years		No. Projects	
0	5	0	8	0	5	0	4
1-3	12	1-3	6	1-5	5	1-5	12
4-6	6	4-8	6	6-10	7	6-15	0
>6	2	>8	5	>10	8	>15	9

The next chapter will analyze the replies of the experts in more depth and propose a practical framework.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

4. Chapter: Results

The collected data of the Delphi study will be evaluated in detail, and a recommendation for a framework using the data will be made. The results of the first round of the questionnaire were mainly used to create the second round. Therefore, this chapter will focus only on the 72 evaluated hypotheses (or statements) of the second round.

4.1. Analysis

This section will put the collected hypotheses (and statements) from the questionnaire into the perspective of the main research hypotheses of this thesis, by describing the ratings and consensus of the experts, while adding their given comments if applicable. Since the hypotheses are very diverse and multi-faceted, most are only described briefly. These results present a subjective view of the participants and might include bias of the author of this thesis. Consequently, they should not be regarded as facts. Table 8 shows the distribution of the categories from the second-round Delphi and its relation to the main research hypothesis, sorted into opportunities, limitations and general statements. Technical and legal feasibility show categories for which some hypotheses were additionally evaluated. In total, 72 hypotheses have been evaluated. As a result, 44 opportunities, 22 limitations, 6 general statements as well as 9 technical and 8 legal feasibilities were generated. Each section in the questionnaire included comment fields which helped where the experts could justify their ratings. The following sub-chapters will look at the results about each research hypothesis more in-depth.

Table 9 to Table 17 contain the hypotheses that were used in the second research questionnaire and summarized the results obtained in that round. The following elements are used for the summary:

- Statement number (#) included to be able to refer to the statement in the text;
- Number of times a specific content was mentioned by experts in the round one (R1);
- Mean of the general Likert scale ratings ($\bar{x}$) was regarded the most important measure and the statements in each table have been ordered accordingly;
- Standard deviation of the general Likert scale ratings (s);
- Mean of the technical feasibility ratings ($\bar{tf}$);
- Standard deviation of the technical feasibility ratings (tf s);
- Mean of the legal feasibility ratings ($\bar{lf}$); and
- Standard deviation of the legal feasibility ratings (lf s).

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

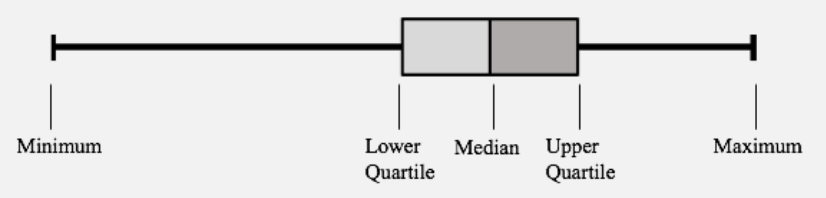


Figure 13: Boxplot (own presentation)

- Boxplot (Figure 13) – graphically plots the range of values from minimum to maximum, median, lower quartile (light grey) and upper quartile (dark grey) on the five-point Likert scale from -2 to 2, which can be found at the bottom of each table. The box plot represents only overall ratings and not the technical or legal feasibility ratings. For a quick comparison, a comparatively short box plot suggests higher consensus than a longer one.

Table 8: Distribution of answers over categories (questions and hypotheses)

	Total	H1	Blockchains impact on personal data	H2	Relevance of data protection regulations for blockchains using personal data	H3	Defining Personal Data	Storing personal data on the blockchain	H4	Privacy by design and blockchain	H5	Blockchains role for data protection regulation	Blockchain solving data protection problems	Recommendations and expectations for blockchain and data protection
Opportunities	44	**18**	18	**5**	5	**10**	5	5	**3**	3	**9**	2	2	5
Limitations	22	**2**	2	**6**	6	**5**	1	4	**4**	4	**3**	1	-	2
Technical feasibility	9	-	-	-	-	**6**	-	6	**1**	1	**2**	1	1	-
Legal feasibility	8	-	-	-	-	**5**	-	5	**1**	1	**2**	1	-	1
General	6	-	-	**2**	2	**1**	-	1	**2**	2	**2**	-	1	1

4.1.1. H1: Blockchains have an impact on personal data.

The first research hypothesis looked at the impact blockchains could have on personal data. It was executed in the questionnaire by listing the different fields it could affect, identified by the experts in round one. In total 20 fields have been identified, 18 of which considered opportunities (Table 9), and 2 limitations (Table 10).

Opportunities

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Electronic identity (opportunity 1; $\bar{x}$ = 1,3) and its possibly unified implementation (opportunity 2; $\bar{x}$ = 1,3) will most likely be impacted by blockchain, as they have been mentioned by many experts in round one and also gotten the highest rating and a strong consensus, but "*with respect to self-sovereign personal data, such a system would need to be incredibly easy to use, limit the number of decisions users are forced to make, and brings huge risks - lost keys, carelessness, inability to manage keys properly.*" (comment from an expert – will be used in this "*formatting style*" within this and the following parts of the Analysis section). The concept of self-sovereign identity was introduced in the context of blockchain by Christopher Allen (2016), who defined it as "individual control across any number of authorities" [122]. The identity layer is believed to be the core problem that needs to be solved to enable decentralized systems, including blockchains [122].

One promising impact building on the identity layer, could be better documentation of personal data processes (opportunity 3; $\bar{x}$ = 1,3), which is often accompanied by contract relationships (opportunity 4; $\bar{x}$ = 1,2), supply chain management (opportunity 5; $\bar{x}$ = 1,1) and public filing cabinets (opportunity 6; $\bar{x}$ = 1,1) – each with a relatively high consensus, among the experts' opinions. Blockchains are impacting these through efficiency gains and cost reduction, e.g. through smart contracts within supply chains that could use information from public filing cabinets automatically. Authorities could use the documentation of the data processes to enforce its legal services. This could even be imagined being done by some kind of AI [2].

Governmental services (opportunity 9; $\bar{x}$ = 1,0) and electronic currencies with enforced identity checks (opportunity 10; $\bar{x}$ = 0,9) were still seen as possible opportunities, but already received more divergent consensus. Blockchains impact on healthcare (opportunity 15; $\bar{x}$ = 0,6) and science (opportunity 17; $\bar{x}$ = 0,5) is seen much more controversial with low consensus and it remains unclear if these will be influenced. Some experts even fully disagreed with blockchain impacting any governmental services, healthcare or science and survey data. This is because all three manage data that is considered by the GDPR article 9 under special categories of personal data, including the processing of biometric and genetic data or data revealing political opinions, ethnic origin or philosophical and religious beliefs [51].

Relating to the rights of the individual's blockchain could potentially impact the enforcement of the requirements which set by the individuals (opportunity 13; $\bar{x}$ = 0,8). This relates to the consent requirements proposed by the GDPR (Key definition and concepts from Chapter II).

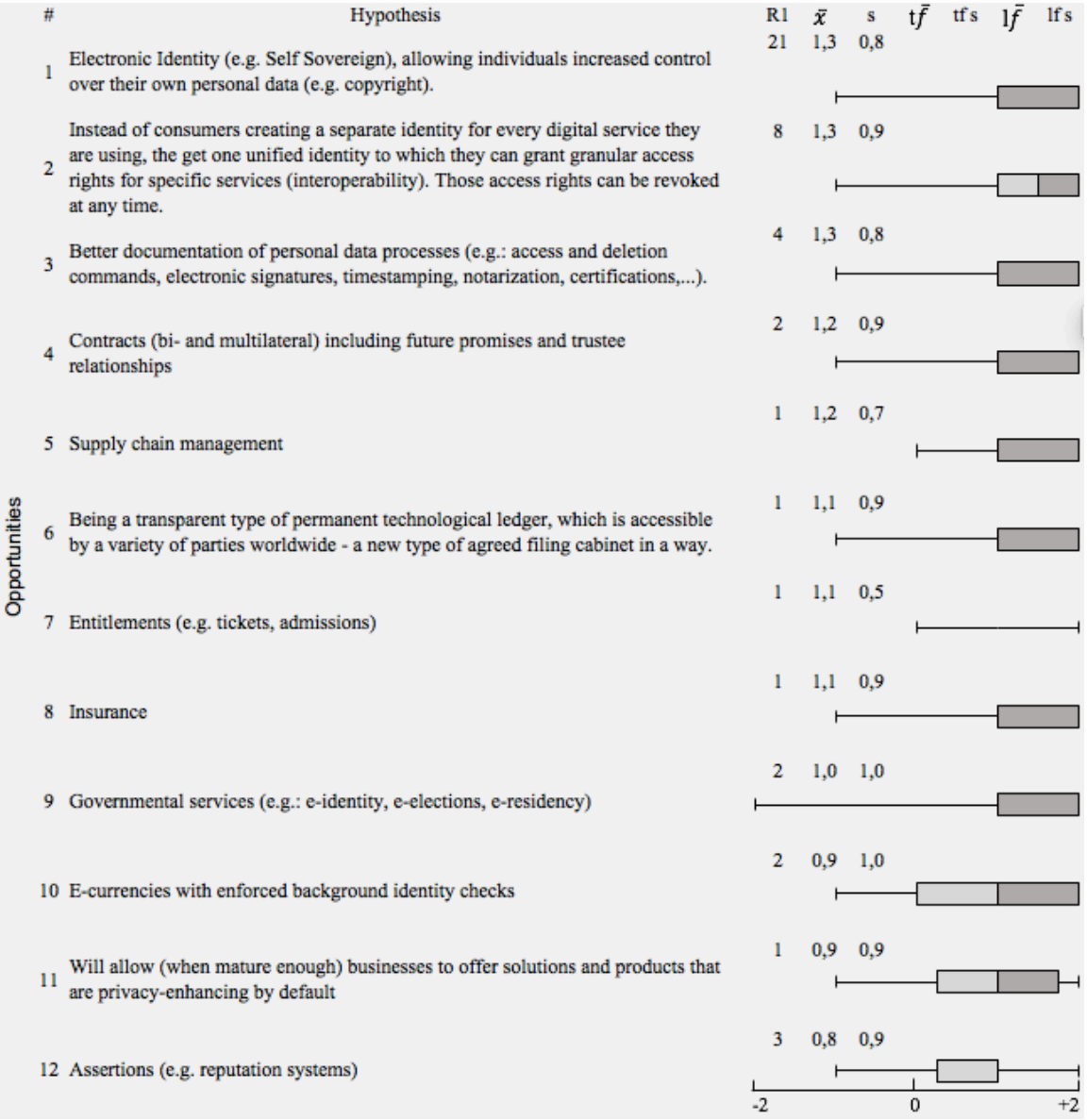
Within the field of commercial usage of blockchain technology, entitlements (opportunity 7; $\bar{x}$ = 1,1), insurance (opportunity 8; $\bar{x}$ = 1,1), assertions (opportunity 12; $\bar{x}$ = 0,8) and privacy enhancing business solutions (opportunity 11; $\bar{x}$ = 0,9) were seen to be impacted with high consensus. Each of them is already impacted by disruptive companies, and practical blockchain use cases within these fields include P2P insurance, event ticketing and nearly untraceable cryptocurrencies [69]. The impact on marketing activities and advertisement surveillance (opportunity 18; $\bar{x}$ = 0,4) has a relatively high dissent, probably as centralised companies, such as Google and Facebook are believed to keep controlling this market – at least in the near term.

On a technological level blockchain is supposed to remove data silos in organizations (opportunity 14; $\bar{x}$ = 0,8), but not many experts fully agree to this standpoint, which could be because of missing technical knowledge. Another perspective states that blockchain will be the essential part for bridging the relationships between humans and technology (opportunity 16; $\bar{x}$ = 0,5). The consensus for this hypothesis is relatively low since "*Blockchain may be AN essential technology, but not THE essential technology. There will be a number of parallel technologies that work together to enable these things and it is unrealistic to say that one will be THE essential tech.*".

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 9: Results for Hypothesis 1 (part 1)

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

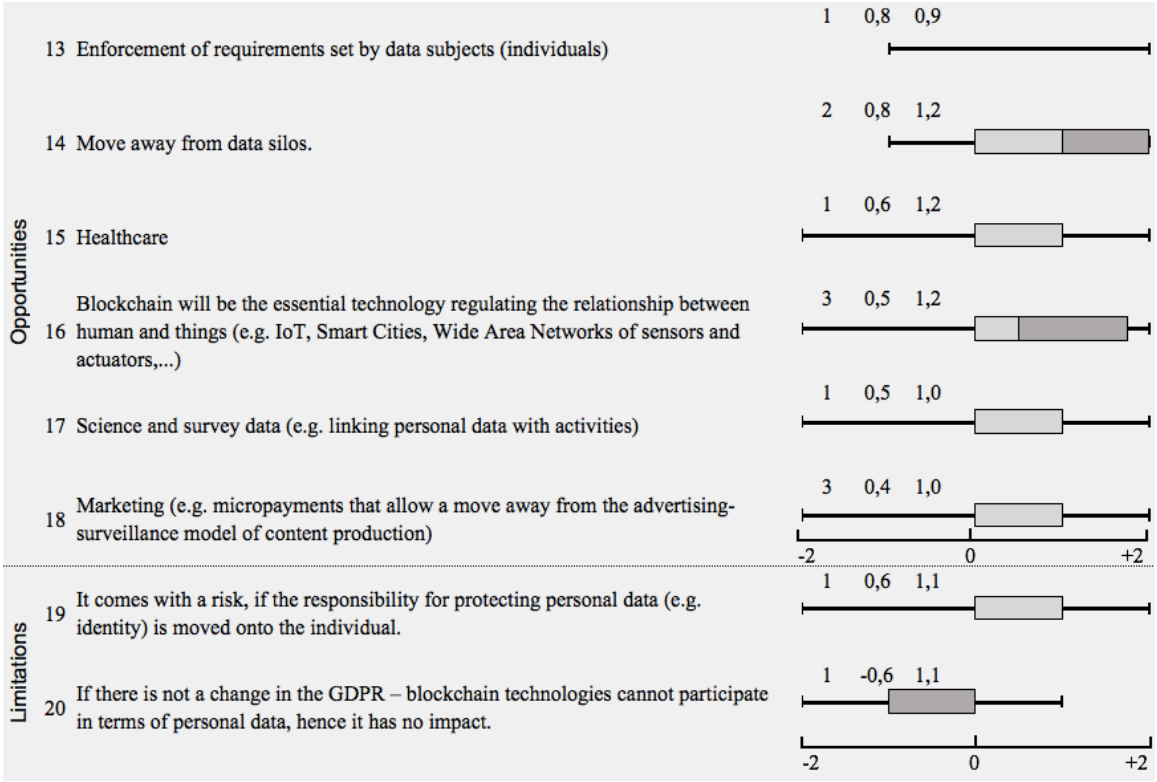


Limitations

Risks related to identity and the protection of personal data being shifted to the individual (limitation 19; $\bar{x}$ = 0,6) are seen on a very diverse spectrum from full agreement to full disagreement with weak consensus. Risks will always exist when dealing with identities [80]. The very limiting hypothesis that blockchains cannot be GDPR conform within current measures (limitation 20; $\bar{x}$ = 0,6) has majorly been disagreed on.

Table 10: Results for Hypothesis 1 (part 2)

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association



4.1.2. H2: Data protection regulations will have an impact on blockchains related to personal data.

The second research hypothesis aims to find out if privacy regulations will be relevant for blockchain technology with regards to personal data. In total (Table 11), 13 fields have been identified including 5 opportunities, 6 limitations and 2 general statements.

Opportunities

Even though the hypothesis was just mentioned by one expert in round one, most participants agree with a high consensus that regulations should provide a minimum standard for user data security and data transparency (opportunity 21; $\bar{x}$ = 1,6). Initiatives in that direction are taking by standardization organizations. It could be interesting to see a decentralized approach in these regards. The same applies for the increase of data security and protection (opportunity 23; $\bar{x}$ = 1,0) through the requirement of PbD (opportunity 22; $\bar{x}$ = 1,1). Blockchain as an identity solution is again mentioned with consensus, this time for the benefit to provide data portability (opportunity 24; $\bar{x}$ = 0,9). The GDPR article 13 will require organizations to accept user requests that order to port the data from one to another service provider of their choice [51]. In this context, the use of blockchain for keeping a record of processing activities is proposed under the circumstance that data could be potentially deleted on a blockchain – more details on that topic will follow in a later part about the RTBF (opportunity 25; $\bar{x}$ = 0,8).

Limitations

The highest agreement was surprisingly on a hypothesis only mentioned once in round one discussing the use of personal data for digital avatars – where people share many PII about themselves online (limitation 26; $\bar{x}$ = 1,6). Blockchain could be highly relevant for that subject by creating transparency

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

about the usage of this data. It was further agreed upon between the experts that any public blockchain would bring along many challenges that need to be solved (limitation 27; $\bar{x}$ = 1,3) – saying blockchain technology could mean social disruption if privacy (limitation 28; $\bar{x}$ = 1,2) would not be considered. This is underlined by a comment to "*not put personal data "on" any blockchain. Metadata trawling can be defended.*"

There is also a high consensus about policy makers currently being ignorant about the implications blockchains provide to society (limitation 29; $\bar{x}$ = 1,6) which further confirms the necessity of this research and a more engaged dialogue between regulators and the blockchain ecosystems. The first step in that direction has been taken by the Blockchain4EU initiative which claims to be a forward looking sociotechnical exploration of existing, emerging and potential blockchain applications for industrial/non-financial sectors [123].

Even though many experts mentioned it in the first round, the RTBF that relates to the ability to combine transactional privacy and immutability (limitation 31; $\bar{x}$ = 0,8) is seen with rather a low consensus to be considered an actual challenge (limitation 30; $\bar{x}$ = 1,1). A reason could be the proposal to allow lost private keys to account for data being deleted. This will be reflected in more detail within H4 – ***General statements*** in this chapter.

General statements

Both statements were specifically intended to trigger comments by the experts. Hence the results of the ratings do not play a significant role here as the statements might have more than one argument in them.

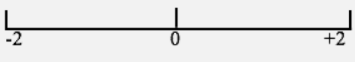
However, the first statement summarizes the view on the relevance matter of the GDPR for blockchain by stressing the importance of the consideration of privacy in the EU (general 32). Most experts agreed on this statement, and many comments were given, one of them summarizes the content of those well: "*Not sure how far the GDPR influences world-hosted networks without specific jurisdiction. So, having blockchain as a substrate to enforce GDPR won't work. It would work as a tool to help auditing the liability and data-privacy protocols on a per-company basis (those that are subjected to GDPR).*"

The second statement provides an even more extensive summary that goes from the argument of BCs core innovation seen as a decentralized trust model that cuts out all different kinds of middlemen (general 33). Some interesting comments argued that on the contrary BCs *"innovation is the cutting out of middle persons. They will always have a role as matchmakers.".* Additionally, the comment is made on blockchains need for maturity adaption, as it *"will not provide all the answers from the beginning. It needs valuable applicability in business, ASAP. It needs measurable business cases. Otherwise its adoption will suffer.".*

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 11: Results for Hypothesis 2

	#	Hypothesis	R1	$\bar{x}$	s	$t\bar{f}$ tf s	$l\bar{f}$ lf s
Opportunities	21	There should be minimum standards for security and ability for users to manage who can see what.	1	1,6	0,5		
	22	Allows for privacy-by-design solutions	2	1,1	0,7		
	23	Increase of data security and protection	2	1	0,8		
	24	Self-sovereign identity is probably the best way to provide data portability.	3	0,9	0,8		
	25	Used wisely, blockchain may be used according to GDPR Article 30 as "Record of processing activities" – used wisely means: You need to solve the deleting issue.	1	0,8	0,8		
Limitations	26	Particular care towards personal data should be considered when dealing with Digital avatars – where people gather, socialize and share information lies the potential for strong abuses in marketing, targeting and discrimination – based on their online behaviours, profiles and social graphs.	1	1,4	0,7		
	27	With regards to data, including metadata, data protection law applies. A public leger containing personal data (wide interpretation used by the European Court of Justice) presents significant challenges for the blockchain technology.	3	1,3	0,9		
	28	Blockchain development without focus on data protection and privacy would mean social disruption.	1	1,2	0,9		
	29	Today, policy-makers are ignorant about the implications and impacts of blockchain technology.	1	1,2	0,8		
	30	As data in the blockchain cannot be altered or removed this may compromise for example the "right to be forgotten" (RTBF) whereby data subjects can demand that their personal data to be erased. Existing dominant implementations of blockchains will need to be tweaked to solve these	6	1,1	1,1		
	31	Today's blockchain paradigm has difficulties to combine both immutability and transactional privacy.	4	0,8	1,4		
General	32	The GDPR is the EU's legal base for processing personal data. Hence, it has to be considered for any technology once personal data is processed. The European Data Protection Board will ensure that the regulation is applied consistently across the EU. Blockchain technology involves risks regarding personal data and privacy that should not be denied.	3	0,9	1,1		
	33	The core innovation is the decentralization of trust, whether cutting out the middleman or creating middleman competition or by allowing decentralized cooperation/coordination. This means, that (quasi-) anonymous actors can more or less freely (public/private) join the network and interact there. Such activity is observed and at least currently re-traceable to the physical person. An innovation that links individuals, algorithms and machines as well as organizations into a decentralized network which activities may also be of concern to the public or the government (and may it be to protect less-knowledgeable individuals), is by its digital nature always of great concern for data protection.	6	0,8	1,3		



The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

4.1.3. H3: Personal data cannot be stored on the blockchain directly, but indirectly.

The third research hypothesis explored the understanding of personal data and further the question how personal data could be stored on a (public) blockchain, if at all. It also introduces the evaluation of technical and legal feasibility. In total, 16 fields have been identified with 10 opportunities (Table 12), 5 limitations and 1 general statement (Table 13).

Opportunities

The first set of statements looked at the perception of personal data. A high rating and high consensus were given to its description as personally identifiable content, metadata and transactions (opportunity 34; $\bar{x}$ = 1,1). The much lower consensus was found in defining it as reputational data (opportunity 36; $\bar{x}$ = 0,7), but *"If we decide to make reputational data public it will be important to have the source visible as well. However, we will have to be careful about vindictive behavior by people who were rated poorly."* Within the same parameters as the previous hypothesis but with a little higher consensus, many experts agreed that a public key of a blockchain can be considered PII (opportunity 37; $\bar{x}$ = 0,7). The hypothesis that the explanation depends on the content of a smart contract (opportunity 38; $\bar{x}$ = 0,6) stays undecided. Many experts mentioned in round one that it should be defined according to the definition in the GDPR (opportunity 45; $\bar{x}$ = 1,1), plus any information that can be considered personal based on every individuals' definition (opportunity 42; $\bar{x}$ = 1,1). The pure definition taken from the GDPR is put into the limitation section since it leaves room for arguments. One argument against this kind of definition gave an example that could be considered when defining personal data: "*Tarzana23 although a virtual identity (associated with reputation, etc.) is not personal data. A picture of a face is not (search Google images for "doppelganger"). An IP should not. A retina scan is. A fingerprint might be."* One thing is clear though that from next year onwards the definition as in the GDPR will be the dominant legal ground concerning personal data of EU citizens (see Chapter II: Key definition and concepts).

The second set of statements focused more on a technical part and the possibilities to add support for privacy to blockchains. This has been identified as the level of identity (mixing keys), value transfer (zero knowledge proofs) and data payloads (opportunity 35; $\bar{x}$ = 0,8) – through methods that were previously discussed in Chapter II about Existing privacy solutions. The suggested solution for data payloads includes encryption and read permissions as assets. These are usage permissions defined on an asset level with possible time limitations, similar to access control tokens [72], [124]. They would enable granular data sharing, based on a token that defines the access level of the granularity. Combined with smart contracts, this could provide a great use case for many application (e.g. IoT sensors, smart home, smart factory and others) [14], [48].

Overall these supposed technical solutions are seen controversially and have a rather uncertain outcome, including its technical feasibility. "*As always, it's not much a matter of technology but of human preparedness to change."* Surprisingly, the chance to use public key encryption to store and transfer data on the blockchain based on the users' preferences (opportunity 39; $\bar{x}$ = 0,4) has meagre rating and weak consensus, even though its technical feasibility is rated high ($\bar{x}$ = 1,1). Another proposition with very similar parameters for its rating and technical feasibility is based on encryption techniques relating to obfuscation (e.g. the solutions Blockstream uses – mentioned as well in Chapter II) that would only store the reference on the blockchain that link to where the PII is stored –using tokenization and hardware components in control of the individual (opportunity 40 and 41; $\bar{x}$ = 0,3 and $\bar{x}$ = 0,2), [72], [124]. Some experts *"tend to dislike solutions that are too hardware dependent on the user side, although with smart phones this is not an issue."*, but also contradict themselves.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

A solution that got rejected by a majority (opportunity 43; $\bar{x}$ = -0,4) recommended that a public blockchain solution should allow everyone to read from it, but only pre-defined parties to write and add claims to it.

Limitations

The concerns regarding blockchain storage have also been rated on legal feasibility to find out if there is a chance that law and regulations will live up to this innovation. Since blockchains work by the principles of a decentralized P2P network, it becomes complicated to determine the data controller (limitation 44, $\bar{x}$ = 0,7). This statement reached relatively small consensus, "*but if it's designed from the start...why not?".* The possible effect on quantum computing to the blockchain and the question if hashes and encryption will be accepted to count as compliant to the GDPR are undecided with low consensus (limitation 46 and 47, $\bar{x}$ = 0,6 and $\bar{x}$ = 0,5).

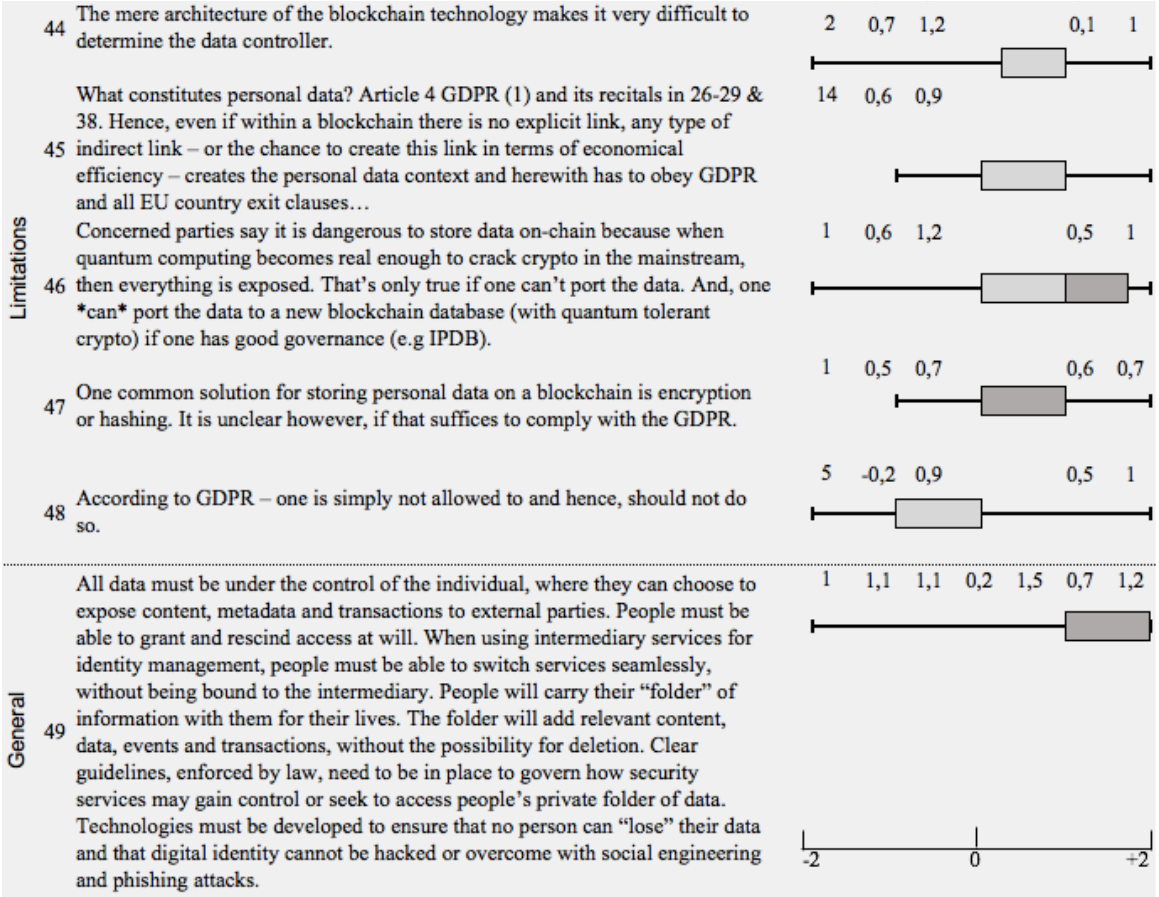
Table 12: Results for Hypothesis 3 (part 1)

	#	Hypothesis	R1	$\bar{x}$	s	$t\bar{f}$	tf s	$1\bar{f}$	lf s
Opportunities	34	What constitutes personal data? Personal data is personally identifiable content, metadata, and transactions.	2	1,1	0,9				
	35	With blockchain you can add in support for privacy. At the level of identity (e.g. by mixing keys), the level of value transfer (e.g. zero knowledge proofs), and at the level of data payloads (e.g. encrypting; or even better "read permissions as assets").	6	0,8	1,1	0,9	1		
	36	What constitutes personal data? Reputational data including the source of that reputation.	1	0,7	1,3				
	37	What constitutes personal data? A public key, i.e. the handle by which user accounts on a blockchain are identifiable.	1	0,7	1,1				
	38	What constitutes personal data? It depends on what data is stored on the blockchain with regard to the smart contracts (parties, nature of the transaction).	1	0,6	1,0				
	39	PKI-encrypted in such a way that only the owner of the data can decide how (and with whom) to share it. When sharing over the public blockchain, the data would be PKI-encrypted so that only the receiver(s) can decrypt it.	5	0,4	1,3	1,1	0,7		
	40	As obfuscated strings in the form of tokens or as tokenised references to encrypted data repositories. The necessary token services should be delivered from individual hardware in possession of the individual user. Not from business driven token service providers representing predominantly financial industry and public authorities.	5	0,3	0,8	0,8	1,2		
	41	Private blockchain: private cold storage with permissioned side-chains.	1	0,2	1,0	0,7	1,1		
	42	What constitutes personal data? As defined in the GDPR, plus data that the individual considers to be personal, something that varies from person to person	1	0,1	1,2				
	43	On-chain: public-read that allows everyone to read, no writing or linking & public-write that allow different roles to add claims to the identity	1	-0,4	0,9	0,4	1		

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

The statement that blockchain will never be accepted under the GDPR was rejected by a majority (limitation 48, $\bar{x}$ = -0,2) even though it was mentioned 5 times in round one. It is to conclude that none of the above statements is seen to be legally feasible, probably because of the very nature of legal procedures relating to the GDPR – that will wait until a case goes to a court before any next action is taken [19]. However, *"interpretation guidelines or amended legislation could make this clearer."*.

Table 13: Results for Hypothesis 3 (part 2)



General statements

The statement argues that individuals will be in full control of their PII and that exact mechanisms need to be in place to make this possible for the case a physical device is lost or a password forgot (general 49). The intent was to leave the ratings of general statements out of perspective, as this statement implicitly aimed to gather comments from the experts. But one interesting fact is that its legal feasibility was rated comparatively high ($\bar{x}$ = 0,7) and received positive comments: *"Legally I see no issues. It is actually a solution adumbrated in the GDPR itself."* Overall most comments mentioned the need for further improvement on the blockchain technology before this kind of solution could be provided partly with the help of blockchain:

"A research and development on both technological and legal aspects must be undertaken before the proliferation of blockchain technologies, understood limitations, and possibly unleashed identification in the way that is feasibly to offer useful services."

4.1.4. H4: Blockchains can be designed in a privacy-friendly manner by using the approach of privacy by design.

The fourth research hypothesis investigates the requirement set by the GDPR of privacy by design and its relation to blockchain development. In total (Table 14) 9 fields have been identified with 3 opportunities, 4 limitations and 2 general statements.

Opportunities

One opportunity has been mentioned 13 times in round one and has an exceptional rating and high consensus. It states that blockchain can be compliant to PbD under the circumstance that it is not a sole solution, but rather part of a stack that intervenes with other technology to make up for its weaknesses (opportunity 50, $\bar{x}$ = 1,6). To ensure the integrity of the data within such a solution, it is agreed that supportive, open standards should be developed (opportunity 51, $\bar{x}$ = 1,4). Initiatives in that direction have only just started. Compliance to the GDPR only through the use hash values and public key cryptography is not seen to be guaranteeing PbD (opportunity 51, $\bar{x}$ = -0,3).

Limitations

Relating to PbD, the biggest concern with high consensus is the recovery of secret information and private keys (limitation 53, $\bar{x}$ = 0,9). Solutions could include social validations in the form of multiple signatures of spouses that help to recover such a key, included could as well be a governmental official [64].

A suggested partial solution for a public blockchain is de-indexing like Google's search engines, which received a low rating and high dissent (limitation 54, $\bar{x}$ = 0,5). Personal data that can be found can always be subject to malicious behaviour.

Public blockchains' incompatibility to comply to PbD is left undecided, as opinions diverge strongly (limitation 55 and 56, $\bar{x}$ = 0,3 and $\bar{x}$ = 0,2). Some efforts described in Chapter II (Existing privacy solutions) are already considered to apply PbD principles, but most of them have not been tested long enough yet.

General statements

The same applies as in the previous "General statements" sections. The first general statement about copyright law and the challenge that "*rarely governments and law makers can be as fast as technology*" (general 57) unfortunately got many comments about the disability to understand its content fully. It should have been formulated more precise. Though one positive comment mentioned that *"One can think of personal data as of Copyrighted data. I believe it can be managed with blockchain.".*

The second statement refers to the challenge of immutability about the enforcement of the RTBF and the question if a lost private key in a blockchain can be stated as forgotten (also referred to as "burned" – also mentioned with low rating by opportunity 65, $\bar{x}$ = 0,3). It further suggests particularly decentralised storage solutions and asks if those can be considered blockchains and if so how they would interact with a public BC (general 58). As expected, this statement did not get a high rating. Nevertheless, its technical feasibility referring to the connection of those storage solutions to a public blockchain gained a strong consensus on a medium high rating ($\bar{x}$ = 0,6). *"Again, let us not forget the*

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

leeway the EUGH and other courts give private contracts and allow for balance of interests;" – it remains an open question what interests are the ones that need to be balanced.

Table 14: Results for Hypothesis 4

	#	Hypothesis	R1	$\bar{x}$	s	$t\bar{f}$	tf s	$l\bar{f}$	lf s
Opportunitie	50	In terms of privacy by design, it could be compliant. But it cannot do it alone, it is part of a software stack, rather than a sole solution. So, it needs to be integrated wisely with all its strength and complemented with appropriate technology where it's not strong.	13	1,6	0,6				
	51	Basic design principles need to be established by open standards (with open source developments) to ensure that blockchain (and Distributed Ledger Technology) maintains personal data integrity.	1	1,4	0,9				
	52	It will comply to Privacy by Design, because it allows participants to hide their true identity behind one or more pairs of private/public keys and also to use hash values instead of plain text data.	1	-0,3	1,1				
Limitations	53	Private secret (and private key) management & recovery.	1	0,9	0,7				
	54	Because public blockchains are immutable, one cannot remove that data directly. That's the challenge. A partial solution: one *can* de-index it. This is exactly like the Web today. We cannot take down servers in some jurisdictions, but at least Google and other search engines can de-index it.	1	0,5	1,2				
	55	In terms of Privacy by Default, blockchains are – in terms of personal data (pd) – at least when public per definition not compatible.	7	0,3	0,8				
	56	Since blockchains are public and immutable databases, they seem to violate privacy by design in the sense that they are "public by design".	5	0,2	1,2				
General	57	Can the internet be compatible with copyright? When technologies, systems and the law work together in a cohesive manner, blockchain can be compatible. However, the complexity of the challenge is immense. Knowing the far-reaching possibilities for blockchain technologies also compels governments to get ahead of the technology as quickly as possible.	13	0,5	1,1				
	58	In some situations, where RTBF is asked to be enforced, we will have to see if making that data unreadable and/or inaccessible complies to the law or not. (e.g. Private key has been thrown away, "burned" in a blockchain sense. Burning a key should = forgotten.)It depends if IPFS, Filecoin, Siacoin, etc. count as blockchain technology, and how often decentralised storage interacts with public chains. I struggle to see how we can have immutability and RTBF.	8	0,4	1,1	0,6	0,8	0,3	1

4.1.5. H5: Blockchains can help to solve (privacy) challenges accompanying the implementation of the new GDPR.

This last research hypothesis looks at blockchains' role for data protection regulations and how it could solve data protection challenges. It also looks at the future relationship between the two topics. In total, 14 fields have been identified with a majority of 9 opportunities (Table 15 and Table 16), 3 limitations and 2 general statements (

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 17).

Opportunities

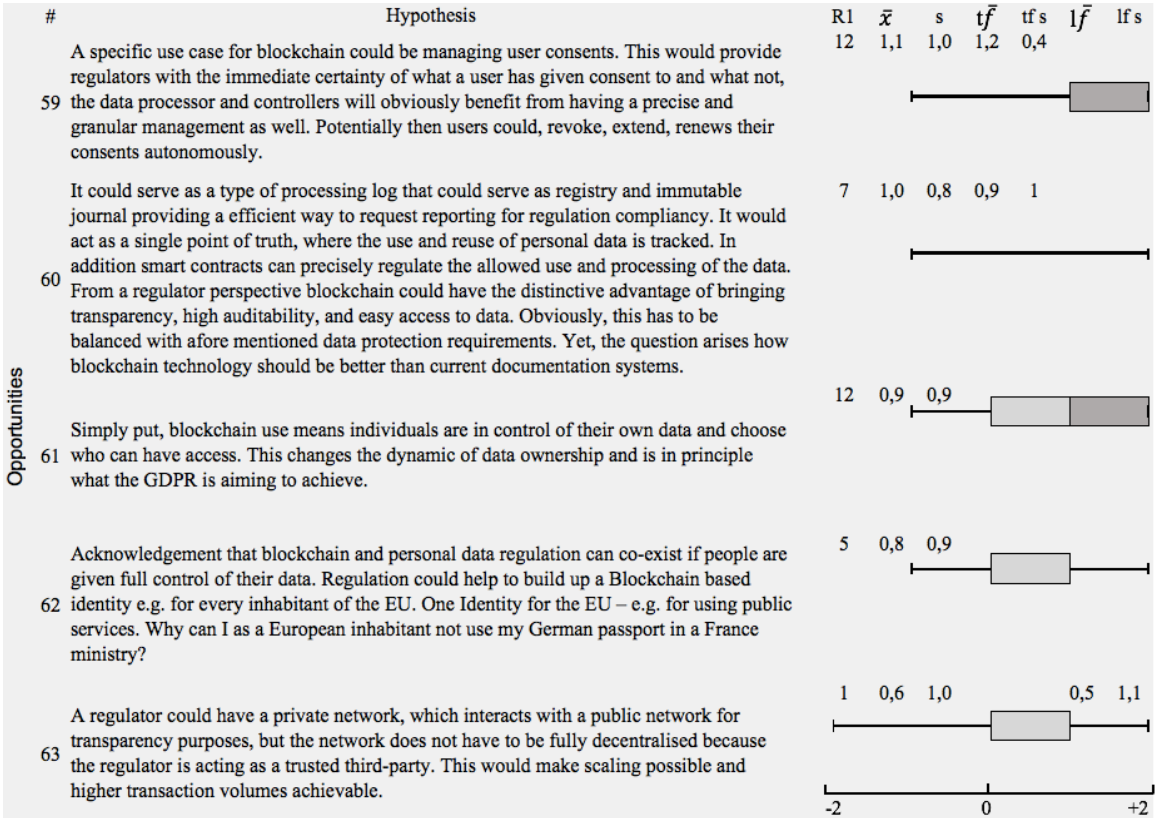
The management of user consent has been identified as a particular use case by many experts during the first round and has received a very high rating in the second round. It would provide regulators and individuals with certainty about their given consent to collected data. Companies (data processors and data controllers) would benefit through well-defined user management. Potential users could revoke, extend and renew their consents autonomously (opportunity 59, $\bar{x}$ = 1,1). Even though there is just an average consensus on that hypothesis, its technical feasibility is rated very high with high consensus. These statements have been commented to be a *"great use case"* and two experts stated that it is *"one use case we ourselves are looking into".* Efforts to solve this problem are already being developed by for example the smart consent protocol, that aims to implement consent receipts, similar to traditional receipts that one would receive when buying a good in a supermarket [125].

The realization of such a solution could be provided through blockchain serving as a type of processing log that creates a single point of truth and uses smart contracts to regulate the processing permissions (opportunity 60, $\bar{x}$ = 1,1) – *"transparency, high auditability, and easy access to data are very powerful features. Having near certain proof that data has not been tampered with is of paramount important. even more so if the proof comes from an independent third party, that cannot be corrupted... knowing that that data is correct not because the government says so, but because it's mathematically provable, is a great feature.".*

Experts agreed that blockchain enables a change of the dynamics of data ownership and aligns with the goal that the GDPR aims to achieve (opportunity 61, $\bar{x}$ = 0,9). This could happen by providing an identity for each EU citizen that is kept in full control of that individual (opportunity 62, $\bar{x}$ = 0,8). This could be done through giving regulators a scalable private network, that interacts with a public network for transparency purposes – its implementation is not seen as technically realistic in the near term (opportunity 63, $\bar{x}$ = 0,6). To conclude this statement: *"governments in Europe might be trustworthy to have a private network as a service; however even in Germany in general everything is federated already; this should be standard if trust is involved; smaller states could federate with other states, EU partner states, etc.".*

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 15: Results for Hypothesis 5 (part 1)



The next opportunity proposes that regulators shall start at the protocol level, which stayed in an open state (opportunity 64, $\bar{x}$ = 0,4). Among these are identity, taxation, property and others. If regulators would start to fulfil those tasks based on a blockchain infrastructure, blockchain protocols could become more attractive (opportunity 66, $\bar{x}$ = 0,2). Following this, there are two opposing perspectives from the experts. One expert mentions that: "*from the regulator point of view there are already some examples of technology / regulatory interoperability, for example digital signatures are handled this way, where a regulation like eIDAS defines various levels, what legal value they have, and give technical guidelines through standards."* Another expert openly opposed by commenting that "*Regulators will never approve protocols. They don't typically issue pre-emptive approvals of things. It's about how the protocol is used, not what the protocol is. So, for evidence, they will define a certain standard of*

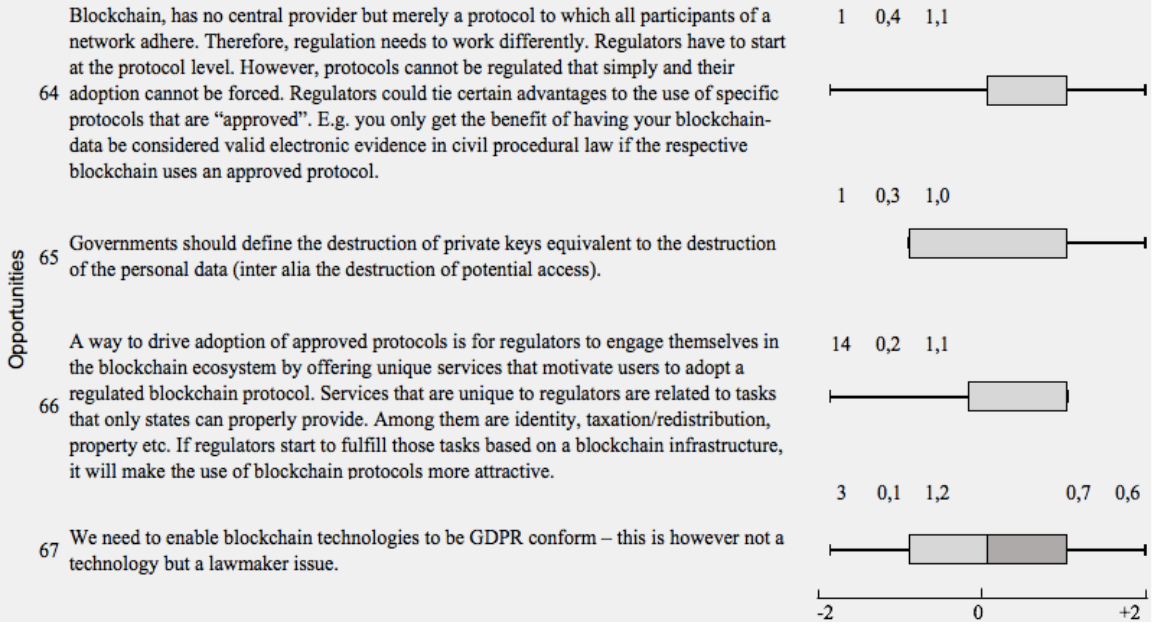
The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

certainty that needs to be met and then it will be up to you to demonstrate that you've met that standard. Eventually norms will develop but they will not be defined by regulators."

The statement – that the conformity of blockchain and the GDPR is not a technology issue, but rather a lawmaker issue stays undecided with low consensus and high divergence between agreement, but its legal feasibility is rated positively with strong consensus ($\bar{x}$= 0,7).

A very similar approach is taken by one limitation. It states that regulators should provide the correct legal framework and use the new technology to enforce their law also on a digital level (limitation 69, $\bar{x}$ = 0,8). This statement received a comparably high score in this section with average consensus and was mentioned by many in the first Delphi round.

Table 16: Results for Hypothesis 5 (part 2)



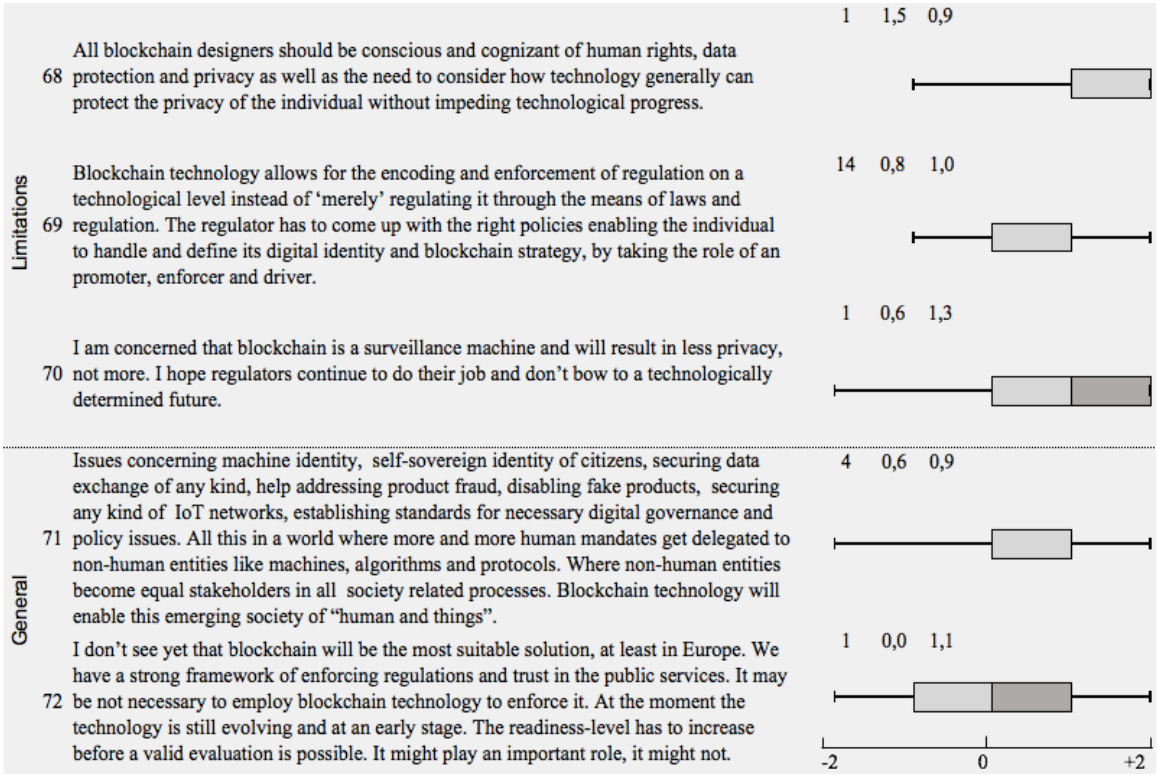
Limitations

This first limitation is directly quoted from the questionnaire. All blockchain developers should be conscious of human rights, data protection and privacy as well as the need to consider how technology generally can protect the privacy of the individual without impeding technological progress (limitation 68, $\bar{x}$ = 1,5). It received a very high rating and relatively high consensus, even though it could limit the innovation of blockchain to some extent.

Since blockchains propose new trust in technology and enforces transparency with immutability, one fear is that it could become another surveillance machine (limitation 70, $\bar{x}$ =0,6) however, this statement has not been rated strongly.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

Table 17: Results for Hypothesis 5 (part 3)



General statements

The first statement summarizes general issues such as machine identity, self-sovereign identity of citizens, secure data exchanges of any kind, product fraud, disabling fake products, securing any IoT networks, establishing standards for necessary digital governance and policy issues. It mentions that in a world where more and more human mandates get delegated to non-human entities like machines, algorithms and protocols – non-human entities become equal stakeholders in all society related processes. It concludes that Blockchain technology will enable this emerging society of "humans and things" (general 71). Many comments followed this statement. One expert agrees: *"Blockchain to me is a tool which can be used for human and things and for enabling the machine of things equally. The*

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

GDPR should regulate the use of the machine of things." Others see it as *"[...] just an idea. Humans must wait and see huge utility in creating such a world."*

The last statement argues that current blockchain technology will not be the most suitable solution, but in the future, it might be (general 72).

The next two comments conclude this section about the analysis of the second Delphi round from two perspectives – a blockchain developer and a data protection lawyer.

The viewpoint of the blockchain developer and experienced AI-scientist, Trent McConaghy:

"I believe there is a long-term need for self-sovereign identity, but in the short-term in order to avoid AI-based corporate manipulation and public control. The majority of individuals will never take full responsibility for their own data and identity. The state has reasonably successfully played this role for hundreds of years. I think blockchains and crypto-based decentralization enable more localization, but I don't think it necessarily needs to extend all the way to the individual. There could be a role for co-operative movements or trusted social organizations to manage data and identity for its members. Similar to the labor movements of the late 20th century."

The viewpoint of the data protection lawyer with specific expertise on the GDPR, Jan Philipp Albrecht:

"Blockchain can help and can be used to be technically compliant with GDPR which is technology neutral."

The first statement draws a comparison to history and proposes a community-based approach towards self-sovereign identity solutions, whereas the second one stresses the technical neutrality of the GDPR. The joined outcome is that both topics should work together to benefit and not hinder each other in the future.

The next sub-chapters will propose suggestions to make the technology compliant with the GDPR, as it is supposed to be possible and necessary under within the current systems of power.

4.1.6. Interim Summary

This section concludes the analysis by summarising the most relevant results from the Delphi study about the research hypotheses. For this purpose, the highest rated statements of each main research hypothesis were collected and summarised in the following Table 18.

Table 18: Summary of highest rated Delphi results

H1: Blockchains have an impact on personal data.	• Electronic identity for which consumers create a separate identity for every digital service they are using, to which they can grant granular access rights for specific services (interoperability). • Blockchains help to improve documentation of personal data processes.
H2: Data protection regulations will have an impact on blockchains related to personal data.	• There should be minimum standards for security and the ability for users to manage consent.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

H3: Personal data cannot be stored on the blockchain directly, but indirectly. H4: Blockchains can be designed in a privacy-friendly manner by using the approach of privacy by design. H5: Blockchains can help to solve (privacy) challenges accompanying the implementation of the new GDPR.	• Particular care towards personal data should be considered when dealing with digital avatars. • With regards to blockchains personal data is considered personally identifiable content, metadata and transactions. • In terms of privacy by design blockchains could be compliant but should not do it alone. • Basic design principles need to be established by open standards to ensure that blockchains maintain personal data integrity. • All blockchain designers should be conscious of human rights, data protection and privacy as well as the need to consider how technology generally can protect the privacy of the individual without impeding technological progress.

4.1.7. Statistical analysis

The Delphi study conducted in this thesis is more of qualitative and descriptive nature and not very useful for a more in-depth quantitative analysis. This is mainly because of the intention of this study, the complex topic and time-constraints that only enabled two Delphi rounds. Other Delphi studies used statistical analysis to compare multiple rating rounds, evaluate ranked replies or forecasted numbers (e.g. stock prices) [31], [33]. Further research should use the results of this study for a quantitative survey.

The only test that has been applied to the set of means of the opportunities and limitations is Duncan's multiple range test (MRT) [115], [126]. The results in Table 19 were calculated with a significance level of $p < 0{,}05$ and show a strong overlap of means between all hypotheses, which means that these have rather insignificantly different ratings.

Table 19: Results of Duncan's MRT

Category	LS means(x)
opportunities	0,773
limitations	0,700

4.2. Blockchain privacy impact assessment (bPIA) canvas

Based on the knowledge obtained from the Delphi study and the literature review, this section proposes a framework that can be used in practice to increase the probability for blockchain developed applications and solutions to comply to the GDPR. It outlines the framework only to a high-level degree, as it is not within the scope of this thesis to provide a detailed solution. The framework proposes a privacy impact assessment (PIA) for blockchains, which aims to prepare researchers and developers to consider the right questions to design their solutions and software architecture in a privacy-friendly manner.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

A privacy impact assessment is a specific process mandated by the GDPR, which calls it data protection impact assessment (DPIA) – for any practical purposes PIA and DPIA are considered the same thing [51]. This process helps organizations to identify and minimize privacy risks and is usually conducted in developing and implementing new processes, projects, policies and systems. It is considered also to help organizations to improve the previously named benefits, to secure relationships with users, customers and stakeholders [19]. Recital 85 of the GDPR, describes its purpose in the following context:

In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

In Article 35 the GDPR further sets out that a DPIA must contain at a minimum [20], [51], [127]:

- A description of processing activities and purposes;
- legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedom of the data subjects;
- the correct measures to address those risks;
- all safeguards and security actions to demonstrate compliance;
- an indication of timeframes if processing relates to erasure;
- evidence of any data protection by design and default measures;
- a list of recipients of personal data;
- confirmation of compliance with approved codes of conduct; and
- details of whether data subjects have been consulted to prove consent.

Before the GDPR, PIAs were considered best practice by regulators, including the Information Commissioner Office (ICO) – a UK independent authority that is set up to uphold information rights in the public interest, while promoting openness of public bodies and data privacy for individuals [128]. Figure 14 proposes seven steps of guidance from the ICO for a PIA, which will likely uphold to the new requirements of the GDPR (there has not been any detailed source of how a DPIA should look like).

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

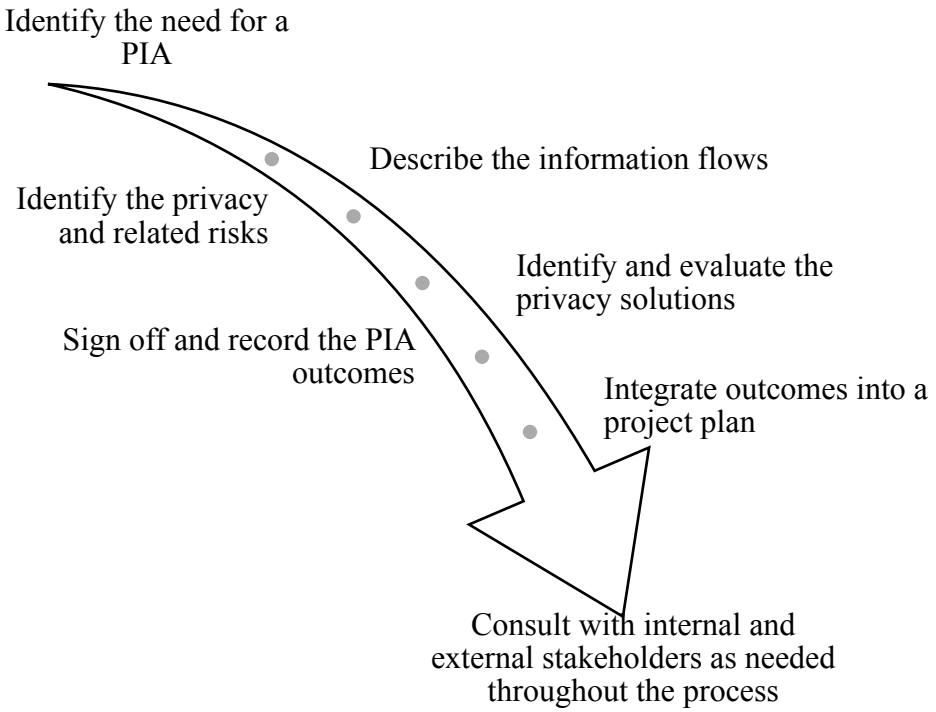


Figure 14: Specific steps of the PIA process (own presentation) adapted from ICO's guidance [129]

The framework for the blockchain privacy impact assessment was created in a canvas style overview (known from the "business model canvas")[130]. Each step draws a reference to the PIAs' implications for blockchain technology while presenting the information to conduct the bPIA in an aggregated view that fits on one page. Each point is looked at in a little more detail in the following sections. The first paragraphs show the wording from the actual canvas, whereas the second paragraphs add additional insights.

(1) Identify the need for a PIA with regards to personal data (PD)

1. According to applicable law: a) high risk to rights and freedom of an individual b) automated processing or profiling c) systematic monitoring or effect (of a publicly accessible area) on a large scale.
2. Organisation s own risk assessment requirements, e.g. expensive data processing, highly sensitive data, strategic business decisions based on data.

1. *Private and public blockchains generally fall under the need for a PIA, specifically since private and public keys are most likely always regarded personal data to begin with.*
2. *Since blockchain applications often are used to increase trust, meaning increased security – which makes a PIA essential to every blockchain use case.*

From the information gathered in the previous sections, the conclusion can be drawn that blockchain will most likely always require a PIA, be it for legal or business reasons. For the technology to succeed

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

as an innovation, it will be necessary to consider privacy impacts that it conflicts with, today. Properly conducted bPIAs could be the next step towards that direction.

(2) Describe the information flows

Four process elements to consider:

1. Data items – e.g. all information about the data subject
2. Formats – e.g. paper, photos, digital (with sub-formats)
3. Transfer Methods – physical or digital movement of information
4. Locations - physical or digital location of information

Six process questions to answer:

a. How is the PD collected?
b. Who is accountable for the PD?
c. Where is the PD stored?
d. Who has access to the PD?
e. Is the PD closed or shared with anyone?
f. Does the system share data with other systems?

For blockchain this brings many specific challenges, specifically about process elements 3 and 4 and process questions b, c, d, e and f. Clear answers to those points should be defined to start being compliant and understand the blockchain solution that is built at its full potential.

This is also a good place to insert business logic and processes that have been identified for blockchain solutions to work in practice – as it will help to review those processes in more depth and from a different perspective. It will also provide visibility for regulators into understanding the new asset-centric-view of data structures data blockchains impose.

Though not directly required by law, data mapping provides an organization with a clear overview of its data processing activities, that can be leveraged for continuous improvement across several internal and external business interests. If a blockchain solution manages to define proper data maps and answers to these questions than additional competitive advantages are surely a consequence.

Blockchains also imply to understand current and future data architectures and computing stacks in order to better understand the new decentralized internet of value and contracts [131], [132].

(3) Identify the privacy and related risks

Application of risk management strategies to catalogue a range of possible threats and vulnerabilities along the line of the information flow process and according to the rights and freedom of the data subject.

Blockchain applications need to develop a risk treatment plan (RTP), with the help of a well-structured governance model that helps to understand the actions following these risks. Potentially broken encryption and immutability pose a high risk that needs a proposed solution.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

The RTP evaluates the impact, likelihood and response to potential vulnerabilities while identifying its owners and actions that need to be documented to develop best practices and better governance models for existing blockchain solutions [83], [133].

(4) Identify and evaluate the privacy solutions

Adding to the RTPs evaluation of risks, their likelihood, impact and action plan an outline of the operational requirements should be drawn to translate risks regarding decisions into reality.

It is recommended to link blockchain solutions to Privacy by Design strategies and tactics proposed by Colesky and Hoepman:

MINIMISE	**HIDE**	**SEPARATE**	**ABSTRACT**
EXCLUDE SELECT STRIP DESTROY	RESTRICT MIX OBFUSCATE DISSOCIATE	DISTRIBUTE ISOLATE	SUMMARIZE GROUP
INFORM	**CONTROL**	**ENFORCE**	**DEMONSTRATE**
SUPPLY NOTIFY EXPLAIN	CONSENT CHOOSE UPDATE RETRACT	CREATE MAINTAIN UPHOLD	AUDIT LOG REPORT

Figure 15: Strategies by tactics from Colesky and Hoepman (2016) [134]

The evaluations of privacy solutions should be accompanied by considering PbD strategies, Implications of the GDPR for blockchain and Existing privacy solutions as outlined in Chapter II. The strategies can be put in further detail by using other recommended frameworks of the Colesky and Hoepman, like the privacy design strategy framework shown in Figure 16. Additional information on both frameworks can be found in its original source, as they are mostly self-explanatory.

Strategy	Underlying Goals				Effects on Actions Regarding Personal Data										
ENFORCE	providing / ensuring	as *abundant*	**commitment**	as *possible* for	**creating, maintaining** and **upholding**	on policies and technical controls regarding	storage,	collection,	retention,	sharing,	changes, breaches	or operation on	personal data,	in a timely manner,	within the constraints of the agreed upon purposes.
DEMONSTRATE			**evidence**		**testing, auditing, logging,** and **reporting**										
CONTROL			**means**		**consenting** to, **choosing, updating,** and **retracting**	From									
INFORM			**clarity**		**supplying, explaining,** and **notifying**	On				sharing					
MINIMIZE	limiting		**usage**	as *much as possible* by	**excluding, selecting, stripping,** or **destroying**	Any			retention						
ABSTRACT			**detail**		**summarizing** or **grouping**			collection							
SEPARATE	preventing		**correlation**		**distributing** or **isolating**										
HIDE			**exposure**		**mixing, obfuscating, dissociating,** or **restricting** access to			sharing							

Figure 16: Privacy design strategy definition framework from Colesky and Hoepman (2016) [134]

(5) Sign off and record the PIA outcomes

All results of point (1) to (4) should be recorded, documented and signed off by the responsible party. The consolidated RTP should go to the management and potentially be made visible to all involved employees. A formal report of high quality and detail should outline all measures taken to provide accountability and transparency about the organization.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

For blockchain solutions this report could partly be made public or reproduced for anyone using blockchain, so that eventually every data controller that is part of the blockchain complies to the GDPR, this could even be on protocol level.

Blockchain solutions can strongly increase their likelihood to comply to the GDPR if they can provide a well-documented PIA, therefore it is important to take extra care when preparing the bPIA report. In case that public blockchain nodes and miners are to be considered joint data controllers, the benefits of having a valid and reproducible bPIA that could be integrated part of the blockchain would be tremendous.

(6) Integrate outcomes into a project plan

All decisions are now translated into defined actions to make sure they are correctly and effectively mitigated. This step should also account for an implementation plan that sets up identified processing functions. This should include periodic reviews and observation of the RTP.

For blockchain solutions this would mean to put concrete technical work into the actual product roadmaps, including deadlines and dependencies, while considering maintenance measures. For a public blockchain this could include reviews by the blockchain community themselves to increase the likelihood of compliance and probabilities to be prepared for legal cases that blockchain use cases could face in the future.

Since blockchain research and applications are at an early stage, it is still highly possible to implement PbD measures. This would improve the solutions to make them future prove and compatible for mass adaption [85], [87].

(7) Consult with internal and external stakeholders as needed throughout the process

Along the process of the PIA one should consult all internal stakeholders and potentially also find an internal and/or external devil's advocate that properly examines the outcome from the view of a data subject. For best practice, this should include the consultation of a legal or data protection and privacy expert.

For blockchains this could be anyone from the community, a user, customer or external consultant. One suggestion could be to publicly review the PIA, just like Smart Contracts or other code is, today.

Since blockchain majorly plays a role in the digital world, it is still subject to hacks and money is stolen by criminals. To prevent this, the blockchain developer ecosystem uses systematic code reviews on a global basis [135]. Similar reviews could be used not only for such code, but potentially for PIA actions as well. Further recommendations are summarized in the next section.

4.3. Practical Recommendations

Based on the Delphi study and the review of the literature a brief list of practical recommendations has been prepared to provide practitioners with guidance on what steps are necessary to make blockchains more privacy-friendly. These recommendations are summarized in

Table 20.

Table 20: Practical recommendations for privacy-friendly blockchain development

Use cases for blockchain development	• Identity solutions that are combined with other technologies to return ownership of PII to the user • Process documentation in different verticals (e.g. supply chain, assertions) to provide accountability in form of log and metadata • Working Consent solution that includes a blockchain in the technology stack • Develop a bPIA on protocol level for public blockchains and implement privacy solutions into governance considerations
Compliance to the GDPR	• Always consider privacy principles when developing a blockchain solution, since transactions, metadata and content are considered PII • Conduct and document a well-structured and thorough PIA, preferably just as the bPIA canvas • Get together with industry participants with an effort to define open standards that will enable compliance across all verticals of blockchain applications
Encryption	• Encryption will help to increase privacy of blockchains, but will never be sufficient on its own • Hashing could be a valid solution to store PII on the blockchain
Mutual Impact	• Do not underestimate privacy regulations like the GDPR, nor other regulations when developing blockchain solutions • An increase in popularity could make authorities aware of blockchain technology rather earlier than later • Do not overestimate blockchain solutions to be solving problems by itself, it is at an early stage and should be combined with existing standards and software solutions • A scalable blockchain is mandatory to provide any kind of feasible solution ready for broad adaption
Political	• Deepen the existing efforts with regulatory and governmental bodies to provide clearer mutual understanding of blockchain and the GDPR • Create EU-wide lobbying efforts in order to solve blockchains challenges (e.g. the RTBF = burned keys) on an EU wide level within existing legal frameworks the EU has to offer
Social	• Education about privacy and blockchain for the blockchain ecosystem on the one hand and individuals across all impacted fields on the other hand • Create certification programs for blockchain privacy impact assessment

5. Chapter: Conclusion

"Friends don't spy; true friendship is about privacy, too."

The intention of this quote by Stephen King can be applied to the mutual relationship of blockchain and the GDPR that should represent a form of friendship [136].

5.1. Résumé

The motivation of this thesis was based on the (partly personal) realization that current systems of power demand a change in technology and the perception of human rights in a more and more digitized global world. Privacy protection received a proposed solution through the means of the GDPR, whereas the technology that connects individuals received a solution called blockchain. For a widespread innovation like blockchain to be realizable within the domains of current social and legal frameworks, it is necessary to start researching to evaluate how both topics interrelate and influence each other. This thesis is the first to provide an in-depth view into blockchain and the GDPR, by investigating the research objective of:

Developing theoretical frameworks and practical recommendations to improve the mutual relationships between blockchain and GDPR.

The key research questions about the interrelationships between blockchain and GDPR is composed into sub-questions that look at it from the perspective of a blockchain expert on the one hand and a regulatory authority (including data protection experts) on the contrary.

The blockchain expert can now conclude that the GDPR will have a significant impact on the development of blockchain technology, mainly because most blockchain solutions use public key cryptography. For now, every private or public key can be considered personal data. The regulation will, therefore, require blockchains to consider a privacy impact assessment and the principles of privacy by design (H3: Personal data cannot be stored on the blockchain directly, but indirectly.). A privacy impact assessment framework for blockchains is proposed to help understand these requirements and enable compliance to the GDPR. The thesis further finds that blockchains can be used to enhance GDPR compliance by using its "immutability"- characteristic to store data processing information in the form of metadata on the blockchain by creating a single source of trough about all personal data related processing (Opportunity 3 in H1: Blockchains have an impact on personal data.). Additionally, blockchain is considered a leading part in identity related software solutions, using its advanced cryptographic and decentralized capabilities (see chapter II: Existing privacy solutions).

From a regulatory perspective, blockchain is still perceived as a technological infant, but its potential impact on policies and politics is already understood and taken seriously. Regulators are asked to extend their dialogue with the blockchain ecosystem to create the right environment for the innovation of blockchain to unfold. An urgent need is an effort towards the implementation of open standards and certifications that are approved by the European Union. The question remains unanswered how this can be done without hindering the innovation of blockchain, but an active dialogue depicts the correct first step. A privacy-friendly blockchain has been demanded by the European data protection supervisory authority that is developed along the principles of privacy by design (see Chapter II - Implications of the GDPR for blockchain). The demand can be fulfilled only by both sides (blockchain developers and regulators) working together. The experts in this study consider it very likely that blockchain technology will be in alignment with these design principles. Eventually blockchains could

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

be part of EU wide administrative software architecture by combining public blockchains with private blockchains used by regulatory bodies (see Chapter IV- H5: Blockchains can help to solve (privacy) challenges accompanying the implementation of the new GDPR.).

The Delphi method, known from policy and IT research for its ability to aggregate expert opinions on a complex topic, was chosen to provide the research with data from a variety of industry and policy experts that helped to form a valid picture of these relationships [104].

The topicality of both topics demanded an extensive review of literature across diverse scientific and non-scientific sources to get an idea of the background of blockchain and the GDPR. After providing background on the most important changes and legal definitions of the GDPR, the implications of blockchain technology provide a first overview of the challenges and changes it is facing. The right to be forgotten and considerations of privacy by design principles are the most prominent challenges for blockchain development, whereas opportunities to improve privacy through improved accountability by immutable process monitoring are often not considered at first glance.

An attempt is taken to review a definition of blockchain technology from multiple perspectives. In brief, a blockchain is hence defined as a distributed database that is practically immutable by being maintained through a decentralized P2P network that uses consensus mechanisms, cryptography and back-referencing blocks to order and validate transactions that represent real digitized values.

Following a more in-depth review of what a blockchain is from a technical perspective and which concepts belong to it (e.g., smart contracts, mining, etc.), existing cryptographic solutions to enhance privacy within blockchains have been accumulated. The usage of zero knowledge proofs, the most prominent solution, enables validation of personal information through providing a binary output. The output shows if that personal information approves to a set of predefined rules. One example is the proof of age of a driving license that would not require an actual age anymore, but rather (only) a "Yes" or "No" if the individual is allowed to drive or not. The actual age remains a private information.

The second chapter about the background and definitions of both topics was closed with a set of hypotheses that reflected the research questions and objectives established in the introduction. These main research hypotheses were further used to lay the groundwork of the Delphi method, which is described in the third chapter. The main advantage of the Delphi method for this study was the incapability of the research problem, not lending itself to precise analytical techniques, but highly benefiting from subjective judgments on a collective basis.

A two round Delphi study with consecutive questionnaires was conducted with a total of 25 participants. The first one collected data according to semi-structured and open-ended questions that reflected on the main research hypotheses. The second questionnaire aggregated the replies of the first questionnaire to form statements and hypotheses that were rated (on) by experts in round two. A third round was planned, but due to time constraints not conducted. It, therefore, provides an opportunity to follow up with the third round to further research the topic.

An analysis of 72 statements, rated in round two, followed in fourth chapter. A summary of the statements was used to propose a blockchain privacy impact assessment canvas that could be operationally used along with a list of practical recommendations. The primary outcome is the realization that most probably every blockchain solution will have to comply with the strict requirements set by the GDPR. It was suggested to achieve this by developing open standards and protocols that can be used by every developer in the blockchain community. The principal use case for privacy and

blockchain is the management of identities that aims to return ownership of personal data to the individual, which perfectly aligns to the core intention of the GDPR to return the freedom of privacy as a human right to EU citizens.

5.2. Limitations and need for further research

Although the research has reached its goal, there are some precautionary measures relating to the risks of a Delphi study mentioned in Chapter III. Each risk will be reflected, and a recommendation for further research will be drawn from it.

First, there could be a bias created by over specifying the structure of the first Delphi round that might have led to the loss of some (possibly valuable) expert opinions

The method can be justified by the limited scope of this thesis, but certainly, other questions exist that require further research. Specific solutions (e.g. for a self-sovereign identity) should be identified and reviewed about their technical, social and legal implications.

Secondly, the assumption that a Delphi study can be a surrogate for other human communication leads to the digitally written style that was applied in this study. Some understanding and context can easily be lost that way. For this, the third optional Delphi round was proposed to take the form of a personal workshop with some of the participants. This will be the most recommended near-term goal for further research.

Thirdly, summarizing and presenting the questionnaire response from round one turned out to be a major challenge – partly because of the amount of information gathered and because of the wording and context used by the participants. This challenge is described in the third chapter, and a creative approach was used to (help) solve it.

For further research, it is recommended to take apart the hypotheses and statements gathered in this thesis to more detail. Those hypotheses could then be used for other forms of quantitative survey techniques, for example, rankings or concrete predictions of information.

Fourthly, not exploring disagreement or agreement in a third Delphi round, could have led to somehow artificial consensus. This point is addressed in the third chapter as well by stating that for this study the primary intent was to create an understanding of the complex topic that is still perceived differently by most experts.

Further research should divide this complex topic and focus on specific subjects and a review of either technical or legal solution.

Lastly, the choice of experts might have led to a selection bias of external validity influenced by the subjective decisions made during the selection process. The diverse opinions of different experts resulted in a truly sophisticated panel that provides valid and valuable research results.

Further research should focus on detailed technical solutions that provide blockchain architectures which follow privacy by design principles. Data mapping and new business processes for blockchain solutions should be included to extend the drive of detailed work on the bPIA canvas.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

A proposition should also be made for how the privacy impact assessment can be implemented to public blockchains under consideration of existing legal and governance frameworks. The result of such an implementation should compare the blockchain ecosystem to economic, political and social factors.

For both academics and practitioners, it is important to keep this changing nature of regulations and technology in mind when conducting research, implementing policies or developing blockchain solutions. The framework needs to be developed further by putting it into action and learning from its outcomes.

References

[1] "Right to Privacy Hearing: No democracy without the Right to Privacy," *Rethink Aadhaar*. [Online]. Available: https://rethinkaadhaar.in/blog/2017/7/20/right-to-privacy-hearing-day-2. [Accessed: 30-Jul-2017].

[2] T. McConaghy, "How Blockchains could transform Artificial Intelligence," *Dataconomy*, 21-Dec-2016. .

[3] S. Baller, S. Dutta, and B. Lanv*in, "The global information technology report 2016," in *World Economic Forum, Geneva*, 2016, pp. 1–307.

[4] "White paper on the future of Europe," *European Commission - European Commission*, 08-Mar-2017. [Online]. Available: https://ec.europa.eu/commission/white-paper-future-europe-reflections-and-scenarios-eu27_en. [Accessed: 17-Apr-2017].

[5] "Who has more users, Facebook or Google? - Quora." [Online]. Available: https://www.quora.com/Who-has-more-users-Facebook-or-Google. [Accessed: 22-Jul-2017].

[6] dsguaman, "Privacy vs. Data Protection vs. Information Security | Software and Services Engineering." .

[7] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, Oct. 2016.

[8] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, 2013, pp. 1–10.

[9] "Blockchain, IP and the fashion industry | Managing Intellectual Property." [Online]. Available: http://www.managingip.com/Article/3667444/Blockchain-IP-and-the-fashion-industry.html. [Accessed: 02-Aug-2017].

[10] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin, 2016.

[11] S. Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media, Inc., 2016.

[12] "Distributed Ledger Technology & Cybersecurity Improving information security in the financial sector." .

[13] S. Ølnes, "BEYOND BITCOIN-Public Sector Innovation Using the Bitcoin Blockchain Technology," in *Norsk konferanse for organisasjoners bruk av IT*, 2015, vol. 23.

[14] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of Empowered IoT Users," 2016, pp. 13–24.

[15] D. Roman and G. Stefano, "Towards a Reference Architecture for Trusted Data Marketplaces: The Credit Scoring Perspective," 2016, pp. 95–101.

[16] "Unlocking the Value of Personal Data: From Collection to Usage," *World Economic Forum*. [Online]. Available: https://www.weforum.org/reports/unlocking-value-personal-data-collection-usage. [Accessed: 17-Apr-2017].

[17] Y. LeCun, Y. Bengio, and G. Hinton, "Machine Learning with Personal Data," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.

[18] "European Data Protection Supervisor Annual Report," 2017. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf. [Accessed: 27-May-2017].
[19] I. G. Publishing, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Limited, 2016.
[20] I. G. Publishing, *Eu Gdpr: A Pocket Guide*. It Governance Limited, 2016.
[21] M. Berberich and M. Steiner, "Practitioner's Corner • Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?," *Eur. Data Prot. Law Rev.*, vol. 2, no. 3, pp. 422–426, 2016.
[22] "Blockchains and Personal Data Protection Regulations Explained," *CoinDesk*, 26-Apr-2017. [Online]. Available: http://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/. [Accessed: 21-Jul-2017].
[23] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," in *Privacy Technologies and Policy*, vol. 9857, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Cham: Springer International Publishing, 2016, pp. 21–37.
[24] P. Pesch and R. Böhme, "Datenschutz trotz öffentlicher Blockchain?," *Datenschutz Datensicherheit-DuD*, vol. 41, no. 2, pp. 93–98, 2017.
[25] C. Sheridan, "BigchainDB and IPDB Meetup Recap: Privacy on the Blockchain," *The BigchainDB Blog*, 21-Jun-2017. [Online]. Available: https://blog.bigchaindb.com/bigchaindb-and-ipdb-meetup-recap-privacy-on-the-blockchain-31884e73eb71. [Accessed: 21-Jul-2017].
[26] "Privacy security and blockchain_Vonne Laan_25 October 2016 (2).PDF." Van Doorne, 2016.
[27] "JLINC_WP_EnablingPrivacyByDesign_20160929_PrePub.pdf." .
[28] "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards." BSI.
[29] "ISO/TC 307 - Blockchain and distributed ledger technologies." [Online]. Available: https://www.iso.org/committee/6266604.html. [Accessed: 15-Jul-2017].
[30] "Futures Research Methodology." [Online]. Available: http://www.millennium-project.org/millennium/FRM-V3.html. [Accessed: 14-Jul-2017].
[31] H. A. Linstone and M. Turoff, "The Delphi Method," *Tech. Appl.*, vol. 53, 2002.
[32] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," 2015, pp. 104–121.
[33] S. Hanafin, "Review of literature on the Delphi Technique," *Dublin Natl. Child. Off.*, 2004.
[34] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," *PloS One*, vol. 11, no. 10, p. e0163477, 2016.
[35] R. Arnold, A. Hillebrand, and M. Waldburger, "Personal data and privacy," *Lond. Ofcom*, 2015.
[36] W. G. Voss, "European Union Data Privacy Law Developments," 2014.
[37] "Your data protection rights in Europe with Jan Philipp Albrecht MEP," *euronews*, 27-Jan-2017. [Online]. Available: http://www.euronews.com/2017/01/27/your-data-protection-rights-in-europe-with-jan-philipp-albrecht-mep. [Accessed: 23-Jul-2017].
[38] "Jan Philipp Albrecht, Grüner Europaabgeordneter für den Norden und innen- und justizpolitischer Sprecher der Grünen Europafraktion," *Jan Philipp Albrecht, MdEP*. [Online]. Available: https://www.janalbrecht.eu/. [Accessed: 15-Jul-2017].
[39] "A brief history of the General Data Protection Regulation." .
[40] B. VAN ALSENOY, "REGULATING DATA PROTECTION," 2016.
[41] Europäische Union, Ed., *Handbook on European data protection law*, Re-. Luxembourg: Publ. Office of the Europ. Union [u.a.], 2014.
[42] G. Press, "A Very Short History of Information Technology (IT)," *Forbes*. [Online]. Available: https://www.forbes.com/sites/gilpress/2013/04/08/a-very-short-history-of-information-technology-it/. [Accessed: 23-Jul-2017].

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

[43] "1981 | Timeline of Computer History | Computer History Museum." [Online]. Available: http://www.computerhistory.org/timeline/1981/. [Accessed: 23-Jul-2017].
[44] "History of the Internet." [Online]. Available: http://www.newmedia.org/history-of-the-internet.html?page=3. [Accessed: 23-Jul-2017].
[45] "The History of the General Data Protection Regulation," *European Data Protection Supervisor*. [Online]. Available: /data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [Accessed: 23-Jul-2017].
[46] P. De Hert, "Data Protection's Future without Democratic Bright Line Rules. Co-existing with Technologies in Europe after Breyer," *Eur. Data Prot. Law Rev.*, vol. 3, no. 1, pp. 20–35, 2017.
[47] S. Beardsley, L. Enriquez, F. Grijpink, S. Sandoval, S. Spittaels, and M. Strandell-Jansson, "Building Trust: The Role of Regulation in Unlocking the Value of Big Data," *Glob. Inf. Technol. Rep. 2014*, p. 73, 2014.
[48] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, vol. 520, Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Cham: Springer International Publishing, 2017, pp. 523–533.
[49] "The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services," *World Economic Forum*, 2016. [Online]. Available: https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services. [Accessed: 17-Apr-2017].
[50] "The Single Market Strategy - Growth - European Commission," *Growth*. [Online]. Available: /growth/single-market/strategy_en. [Accessed: 24-Jul-2017].
[51] "General Data Protection Regulation (GDPR) – Final text neatly arranged," *General Data Protection Regulation (GDPR)*. [Online]. Available: https://gdpr-info.eu/. [Accessed: 24-Jul-2017].
[52] T. Wybitul, *EU-Datenschutz-Grundverordnung im Unternehmen: Praxisleitfaden*. Fachmedien Recht und Wirtschaft, 2016.
[53] H. Gjermundrød, I. Dionysiou, and K. Costa, "privacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls," in *International Conference on Web Engineering*, 2016, pp. 3–15.
[54] "Preparing for the General Data Protection Regulation." ico - information commissioner office.
[55] "my health my data." 2016.
[56] "The Missing Links In The Chains? Mutual Distributed Ledger (aka blockchain) Standards." Long Finance, 2016.
[57] V. Voices, "How The Cryptoconomy Will Be Created," *Forbes*. [Online]. Available: http://www.forbes.com/sites/valleyvoices/2015/01/20/how-the-cryptoconomy-will-be-created/. [Accessed: 25-Jul-2017].
[58] "Talk:Buckminster Fuller - Wikiquote." [Online]. Available: https://en.wikiquote.org/wiki/Talk:Buckminster_Fuller. [Accessed: 25-Jul-2017].
[59] E. Sixt, *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie*. Springer-Verlag, 2016.
[60] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System Bitcoin: A Peer-to-Peer Electronic Cash System."
[61] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," *IEEE Secur. Priv.*, vol. 12, no. 3, pp. 54–60, May 2014.
[62] N. Koblitz and A. J. Menezes, "Cryptocash, cryptocurrencies, and cryptocontracts," *Des. Codes Cryptogr.*, vol. 78, no. 1, pp. 87–102, Jan. 2016.
[63] K. Chaudhary, A. Fehnker, J. van de Pol, and M. Stoelinga, "Modeling and Verification of the Bitcoin Protocol," *Electron. Proc. Theor. Comput. Sci.*, vol. 196, pp. 46–60, Nov. 2015.

[64] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Security and Privacy (SP), 2016 IEEE Symposium on*, 2016, pp. 839–858.
[65] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Proj. Yellow Pap.*, vol. 151, 2014.
[66] T. McConaghy *et al.*, "BigchainDB: A Scalable Blockchain Database," 2016.
[67] J. de Kruijff and H. Weigand, "Towards a Blockchain Ontology," 2016.
[68] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons, 2016.
[69] V. Morabito, *Business Innovation Through Blockchain: The B3 Perspective*. Springer, 2017.
[70] "DIN SPEC 16597:2017-04." [Online]. Available: http://www.din.de/en/about-standards/din-spec-en/business-plans/wdc-beuth:din21:273752635. [Accessed: 27-Jul-2017].
[71] M. Simantov, *p2p-index: A collection of peer-to-peer decentralized projects*. 2017.
[72] S. Díaz-Santiago, L. M. Rodriguez-Henriquez, and D. Chakraborty, "A cryptographic study of tokenization systems," in *2014 11th International Conference on Security and Cryptography (SECRYPT)*, 2014, pp. 1–6.
[73] "Finra: Distributed Ledger Technology: Implications of Blockchain for the Securities Industry." 2017.
[74] "Bitcoin and Cryptocurrency Technologies," *Goodreads*. [Online]. Available: https://www.goodreads.com/book/show/29452533-bitcoin-and-cryptocurrency-technologies. [Accessed: 27-Jul-2017].
[75] "Online MD5 Hash Generator & SHA1 Hash Generator." [Online]. Available: http://onlinemd5.com/. [Accessed: 25-Jul-2017].
[76] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 2084–2123, 2016.
[77] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer--Peer Netw. Appl.*, vol. 9, no. 2, pp. 397–413, Mar. 2016.
[78] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[79] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Consumer Electronics (ICCE), 2016 IEEE International Conference on*, 2016, pp. 467–468.
[80] A. Yasin and L. Liu, "An Online Identity and Smart Contract Management System," presented at the 2016 IEEE 40th Annual Computer Software and Applications Conference, 2016, pp. 192–198.
[81] "IPDB," *IPDB - Interplanetary Database Foundation*. [Online]. Available: http://ipdb.foundation/. [Accessed: 27-Jul-2017].
[82] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," 2015.
[83] W. Reijers, F. O'Brolcháin, and P. Haynes, "Governance in Blockchain Technologies & Social Contract Theories," *Ledger*, vol. 1, pp. 134–151, 2016.
[84] S. George, "THE TREND TOWARDS BLOCKCHAIN PRIVACY: ZERO KNOWLEDGE PROOFS." 2016.
[85] I. Bashir, *Mastering Blockchain*. Packt Publishing, Limited, 2017.
[86] R. C. Merkle, "Protocols for public key cryptosystems," in *Security and Privacy, 1980 IEEE Symposium on*, 1980, pp. 122–122.
[87] "Privacy on the Blockchain," *Ethereum Blog*, 15-Jan-2016. .
[88] "The Trend Towards Blockchain Privacy: Zero Knowledge Proofs," *SAMMANTICS*. [Online]. Available: http://sammantics.com/blog/2016/8/23/the-trend-towards-privacy-how-blockchains-plan-to-accomplish-this. [Accessed: 26-Jul-2017].

[89] "The First Bitcoin Wallet to Address Privacy Issues Without Any Forks," *CryptoCurry*, 02-Apr-2017. .
[90] "Zcash - All coins are created equal." [Online]. Available: https://z.cash/. [Accessed: 26-Jul-2017].
[91] "CryptoNote - the next generation cryptocurrency." [Online]. Available: https://cryptonote.org/. [Accessed: 26-Jul-2017].
[92] "Monero - secure, private, untraceable," *getmonero.org, The Monero Project*. [Online]. Available: https://getmonero.org/. [Accessed: 26-Jul-2017].
[93] A. van Wirdum, "CoinJoin: Combining Bitcoin Transactions to Obfuscate Trails and Increase Privacy," *Bitcoin Magazine*. [Online]. Available: https://bitcoinmagazine.com/articles/coinjoin-combining-bitcoin-transactions-to-obfuscate-trails-and-increase-privacy-1465235087/. [Accessed: 26-Jul-2017].
[94] "CoinJoin Sudoku | Weaknesses in SharedCoin, and CoinJoin research." .
[95] "Litecoin - Open source P2P digital currency." [Online]. Available: https://litecoin.org/. [Accessed: 26-Jul-2017].
[96] "Raiden Network." [Online]. Available: http://raiden.network/. [Accessed: 26-Jul-2017].
[97] "A Gentle Reminder About Encryption," *R3*. [Online]. Available: http://www.r3cev.com/blog/2016/8/24/a-gentle-reminder-about-encryption. [Accessed: 26-Jul-2017].
[98] "Blockstream." [Online]. Available: https://blockstream.com/. [Accessed: 26-Jul-2017].
[99] "Digital Asset Platform - Non-technical White Paper.pdf." [Online]. Available: http://hub.digitalasset.com/hubfs/Documents/Digital%20Asset%20Platform%20-%20Non-technical%20White%20Paper.pdf?submissionGuid=19b3704a-4934-4661-9920-2270d03db39. [Accessed: 27-Jul-2017].
[100] T. Grisham, "The Delphi technique: a method for testing complex and multifaceted topics," *Int. J. Manag. Proj. Bus.*, vol. 2, no. 1, pp. 112–130, Jan. 2009.
[101] M. I. Yousuf, "Using experts' opinions through Delphi technique," *Pract. Assess. Res. Eval.*, vol. 12, no. 4, pp. 1–8, 2007.
[102] "StewartDelphi1987.pdf." [Online]. Available: http://www.albany.edu/cpr/stewart/Papers/StewartDelphi1987.pdf. [Accessed: 03-Jul-2017].
[103] G. J. Skulmoski, F. T. Hartman, and J. Krahn, "The Delphi method for graduate research.," *J. Inf. Technol. Educ.*, vol. 6, 2007.
[104] "Delphi EU." [Online]. Available: http://forlearn.jrc.ec.europa.eu/guide/2_scoping/meth_delphi.htm#Examples. [Accessed: 03-Jul-2017].
[105] R. C. Schmidt, "Managing Delphi surveys using nonparametric statistical techniques," *Decis. Sci.*, vol. 28, no. 3, pp. 763–774, 1997.
[106] "project Meaning in the Cambridge English Dictionary." [Online]. Available: http://dictionary.cambridge.org/dictionary/english/project. [Accessed: 15-Jul-2017].
[107] "expert - definition of expert in English | Oxford Dictionaries," *Oxford Dictionaries | English*. [Online]. Available: https://en.oxforddictionaries.com/definition/expert. [Accessed: 15-Jul-2017].
[108] "European Data Protection Supervisor - The EU's independent data protection authority," *European Data Protection Supervisor*. [Online]. Available: /edps-homepage_en. [Accessed: 15-Jul-2017].
[109] "LinkedIn." [Online]. Available: https://www.linkedin.com/feed/. [Accessed: 16-Jul-2017].
[110] "Magazin für Computertechnik," *c't*. [Online]. Available: https://www.heise.de/ct/. [Accessed: 16-Jul-2017].
[111] "Association for Computing Machinery." [Online]. Available: http://www.acm.org/. [Accessed: 16-Jul-2017].
[112] "IEEE - The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity." [Online]. Available: https://www.ieee.org/index.html. [Accessed: 16-Jul-2017].

[113] "Niko Woischnik: Berlin will become the Blockchain capital," *YourStory.com*, 10-Jul-2017. [Online]. Available: https://yourstory.com/2017/07/niko-woischnik-berlin-blockchain-capital/. [Accessed: 15-Jul-2017].
[114] "German Parliament Passes New Federal Data Protection Act," *HL Chronicle of Data Protection*, 02-May-2017. [Online]. Available: http://www.hldataprotection.com/2017/05/articles/consumer-privacy/german-parliament-passes-new-federal-data-protection-act/. [Accessed: 15-Jul-2017].
[115] R. M. Müller, S. Linders, and L. F. Pires, "Business Intelligence and Service-oriented Architecture: A Delphi Study," *Inf. Syst. Manag.*, vol. 27, no. 2, pp. 168–187, Apr. 2010.
[116] R. Likert, *A Technique for the Measurement of Attitudes*. publisher not identified, 1932.
[117] "BlockchainHub," *BlockchainHub*. [Online]. Available: https://blockchainhub.net/. [Accessed: 18-Jul-2017].
[118] A. Thomas, *Research skills for management studies*, 1st ed. London ; New York: Routledge, 2004.
[119] "Mindset - Design Thinking." [Online]. Available: https://hpi.de/en/school-of-design-thinking/design-thinking/mindset.html. [Accessed: 18-Jul-2017].
[120] B. Ludwig, "Predicting the Future: Have you considered using the Delphi Methodology?," *J. Ext.*, vol. 35, no. 5, Oct. 1997.
[121] "Big 4 Accounting Firms - Who They Are, Facts and Information," *accountingverse.com*. [Online]. Available: http://www.accountingverse.com/articles/big-4-accounting-firms.html. [Accessed: 16-Jul-2017].
[122] "The Path to Self-Sovereign Identity." [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. [Accessed: 30-Jul-2017].
[123] "EU Policy Lab | Launch of the #Blockchain4EU project." .
[124] R. K. Garg and N. K. Garg, "Developing secured biometric payments model using Tokenization," in *2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)*, 2015, pp. 110–112.
[125] "smart-consent-protocol.pdf." 2017.
[126] R. J. Tallarida and R. B. Murray, "Duncan Multiple Range Test," in *Manual of Pharmacologic Calculations*, Springer, New York, NY, 1987, pp. 125–127.
[127] "IT Governance Ltd - GDPR compliance presentations." .
[128] "Overview of the General Data Protection Regulation (GDPR)," 28-Jul-2017. [Online]. Available: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/. [Accessed: 01-Aug-2017].
[129] "Accountability and governance," 28-Jul-2017. [Online]. Available: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/. [Accessed: 01-Aug-2017].
[130] "Strategyzer | Business Model Canvas." [Online]. Available: https://strategyzer.com/canvas/business-model-canvas. [Accessed: 01-Aug-2017].
[131] "The Internet of Agreements." [Online]. Available: http://internetofagreements.com/. [Accessed: 01-Aug-2017].
[132] T. McConaghy, "Blockchain Infrastructure Landscape: A First Principles Framing," *The BigchainDB Blog*, 15-Jul-2017. [Online]. Available: https://blog.bigchaindb.com/blockchain-infrastructure-landscape-a-first-principles-framing-92cc5549bafe. [Accessed: 01-Aug-2017].
[133] "First IPDB Caretaker Meeting: Governance & Technology." [Online]. Available: https://medium.com/ipdb-blog/first-ipdb-caretaker-meeting-governance-technology-295bfc45966a. [Accessed: 01-Aug-2017].
[134] M. Colesky, J.-H. Hoepman, and C. Hillen, "A Critical Analysis of Privacy Design Strategies," 2016, pp. 33–40.

The JBBA 2018 Vol 1, Issue 1 | Published by The Journal of The British Blockchain Association

[135] "Thoughts on The DAO Hack." [Online]. Available: http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/. [Accessed: 01-Aug-2017].
[136] "Quotes About Privacy (234 quotes)." [Online]. Available: https://www.goodreads.com/quotes/tag/privacy. [Accessed: 02-Aug-2017].