Tallinn University of Technology

School of Business and Governance

Department of Law

Yusef Ward

APPLICABILITY OF BLOCKCHAIN TECHNOLOGIES UNDER THE GENERAL DATA PROTECTION REGULATION AND CALIFORNIA CONSUMER PROTECTION ACT

Bachelor Thesis

Program HAJB, European Union and International Law

Supervisor: Thomas Hoffmann, Ph.D

Tallinn 2020

I declare that I have compiled the paper independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not been previously been presented for grading.

The document length is 8,282 words from the introduction to the end of conclusion.

Yusef Ward……

(signature, date)

Student code: 173639HAJB

Student e-mail address: yousefward@gmail.com

Supervisor: Thomas Hoffmann, Ph.D.

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Blockchain (BC) technologies are experiencing an age of evolution of rapid progress in the sphere of technology. The increased interest in transparency and privacy in recent years serve as some of the primary reasons for the evolution of BC. BC by its nature attempts to revolutionize the concept of transparency and privacy on the internet, by establishing a completely decentralized network for communication. The General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) attempt to provide persons a higher level of data privacy and transparency, through legislative measures. BC similarly attempts to provide persons a higher level of control over their data's privacy through the use of technical measures. In effect, the CCPA, GDPR and BC aim at achieving the same outcome of increased data privacy for individuals, though through differing means and methods.

The main aim of this thesis is to evaluate the applicability of BC under the GDPR and the CCPA. The thesis shall attempt to display and define to what extent and how the GDPR and CCPA shall affect the development of BC. The legal effects of the GDPR and CCPA on the development of BC technologies shall be evaluated. The outcome shall present the hypothesized points of contradictions between the two privacy laws and BC. A need for technologically centered legal policy development and particular exceptions towards BC based technology under the CCPA and GDPR shall be presented as solutions to alleviate the clash between the GDPR, CCPA and the development of BC.

Keywords: GDPR, CCPA, Blockchain, Incompatibility, Technology

INTRODUCTION

The exponentially growing and encompassing presence of technological implementation has become a part of practically every sector and aspect of human life. The in technological advancements has allowed the exchange of data to change from sparse to plentiful. The rapid integration of technology into daily life has sparked an urgent need to create guidelines on how the new currency, data, should be handled and used. In the new reality of data as currency, it has become a vital question on how to regulate the use of data to avoid manipulation and misuse of personal information. How the new currency of data should be handled has sparked manifold proposals and solutions, one of the most discussed and analyzed in recent years has been blockchain (BC), claimed by some as the next generation of the internet, internet 3.0[1] and a solution to ensuring data privacy.

The concept of blockchain based implementations have been present since the late 90's of the 20th century[2], yet the true spark of interest and research into this technology began with the publishing of the white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto in 2008[3]. The Bitcoin Blockchain is known as the first public blockchain system and has proven to be the most stable and known mass implementation of the blockchain technology to date. The Bitcoin blockchain is an implementation of a cryptocurrency. Blockchain is not limited as a technology to cryptocurrencies. In recent years, blockchain has spanned to be applicable to various

[1] Litan, A. (2019). Blockchain's Big Bang: Web 3.0 - Avivah Litan. Retrieved 8 April 2020, from https://blogs.gartner.com/avivah-litan/2019/08/08/blockchains-big-bang-web-3-0/
[2] Gupta, V. (2017). A Brief History of Blockchain. Retrieved 10 May 2020, from https://hbr.org/2017/02/a-brief-history-of-blockchain
[3] Nakamoto, Satoshi. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 8 April 2020, from https://bitcoin.org/bitcoin.pdf.

industries from healthcare to government. An example of this expansion would be the European blockchain partnership project signed and backed by 21 European Union (EU) member states and Norway, which is aimed to "support the delivery of cross-border digital public services, with the highest standards of security and privacy" [4]. The Commissioner for Digital Economy and Society, Mariya Gabriel stated that "In the future, all public services will use blockchain technology"[5]. This bold statement displays the direction that blockchain technology could head, paving the way for new privacy centred solutions on an individual, national and supra-national level. At a strikingly similar pace, legislative bodies, in light of the current exponential state of data usage have aimed to harmonize and consolidate the protection and privacy of such data. The European Union replaced Directive 95/46/EC (Data Protection Directive) of 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data with the General Data Protection Regulation (GDPR) that began to be enforced on 25th May, 2018. The GDPR could be noted as the first large-scale privacy regulation in the new era of technology and it is set to harmonize data privacy laws across Europe. Since the GDPR has been enforced, there are multiple questions to be addressed on how to apply the regulation and how to coordinate the regulation's application for businesses in the EU, including blockchain based businesses. The GDPR was built to focus on centralized data controllers[6]. This gives rise to the question of how the emerging blockchain technology, a decentralized technology should be applied and regulated under the General Data Protection Regulation. The maxim of take control of your personal data is an integral part of the GDPR and blockchain solutions, yet there appears to be contradictions in the applicability of BC to GDPR.

The same inquiries to the applicability of privacy laws to BC are ever so present in the United States (US), particularly in the state of California. The California Consumer Privacy Act (CCPA) is a bill which extends privacy rights of individuals in the state of California and has been effective

[4] Gabriel, M. (2018). European countries join Blockchain Partnership - Shaping Europe's digital future - European Commission. Retrieved 8 April 2020, from https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

[5] Ibid

[6] Truong, N. et al. (2019). Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things. *IEEE Transactions On Information Forensics And Security*, 14(10).

since the 1st of January of 2020[7]. It gives Californians the right to exercise their privacy rights. Both the GDPR and CCPA are initiatives to solidify and extend the rights to privacy and data security for individuals, yet at present, the practical applicability and effects of the legislations to novel technologies, such as BC are uncertain.

The following research shall firstly outline the basics of blockchain technologies and its functionality in the first chapter, followed by an introduction of the GDPR and CCPA and the concepts established by the two legal texts in the second chapter. This shall give way to a discussion of the material scope of applicability of blockchain under the CCPA and GDPR, an analysis of how the material scope is affected and regarded under the two privacy laws in the third chapter. This shall be followed by a comparison of the effect of the two laws on the progress of blockchain in the fourth chapter and finally a discussion on what approach must be taken towards blockchain technology under the GDPR and CCPA and the current state of the applicability of blockchain technologies to the GDPR and CCPA. This research aims to explore the applicability, compatibility and contradictions between BC technologies and the two legislative texts, the GDPR and CCPA. Additionally, providing proposals on the ways of mitigating the contradictions between the legal texts, GDPR, CCPA and BC technology established in this research.

[7] Davis L. (2020). The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation. *North Carolina Banking Institute*, (24)1.

1. BLOCKCHAIN TECHNOLOGY

A blockchain is a distributed ledger that operates on the basis of cryptographic and mathematical functions, which enables the security of the data stored on the blockchain[8]. Blockchain first arose in implementation by the creation of the first cryptocurrency, Bitcoin in 2009[9]. Yet, blockchain itself is not limited to bitcoin, or any other cryptocurrency for that matter. There are countless projects relying on blockchain technology. Merriam-Webster defines blockchain "as a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network"[10]. Vitalik Buterin, the co-founder of one of the largest financial BC solutions, Ethereum, notes, "A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible"[11]. The definition of blockchain can be encompassed under multiple terms. There are many varieties of executions of blockchain technologies, yet at core, a blockchain shall have a distributed ledger system, maintained by cryptography as a means of security. Blockchain is often referred to as trustless, that does not mean that the technology should not be trusted, but on the contrary. The essence of blockchain is that there is no trusted third party that verifies transactions on the system, but rather employs the use of group consensus, where the network ie. the technology itself by its nature verifies each transaction and authorizes its addition to the chain of other blocks of transactions[12]. The nature of a blockchain based system eliminates the need for trust in any third

[8] Morabito, V. (2017). *Business Innovation Through Blockchain*. *s.l.*: Springer International Publishing AG, 5.
[9] *Ibid.*
[10] Merriam-Webster Dictionary, 'blockchain' Retrieved 8 April 2020, from https://www.merriam-webster.com/dictionary/blockchain
[11] Buterin, Vitalik.Ethereum Blog. (2015) Visions, Part 1: The Value of Blockchain Technology. Retrieved 8 April from, https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/
[12] Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Beijing, China: O'Reilly, 2.

party, which is replaced by the technology itself[13]. Regardless of the definition of blockchain, each system implemented utilizing this technology has four identifying elements. Firstly, the BC is based on an append-only system and is permanently stored on the chain, related to previous transactions. Secondly, the BC is stored in a completely decentralized peer to peer network. Thirdly, the BC is asymmetrically encrypted meaning every user has a private and public key to verify and conclude transactions. Fourthly, the design of a blockchain entails a decentralized architecture, which makes it extremely difficult to tamper or reverse transactions in a blockchain. This chapter shall aim to describe and analyze these four identifying elements.

1.1 Functioning of the Blockchain

Blockchain technologies regardless of the particularities relies on a Distributed Ledger System ("DLT"), it is defined as a "distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information"[14]. In abstract terms, a blockchain is composed of three distinguishable parts – the block, the chain and the network. A block in the blockchain can be viewed as a record of a transaction, each block contains the transaction data, a timestamp of when the transaction was concluded, a block header and lastly a pointer to the previous block, known as a cryptographic hash. When a new block is being added to the previous block, the block header is used to create a mathematical function called a hash, which is an algorithm that takes an input and creates an output[15]. The hash may be viewed as a digital fingerprint, every block in the chain has a hash of the previous block. The hash outputs act as the chain. The last component of the blockchain is the network, which is composed of nodes ie. computers, each node is a participant of the blockchain. For a block containing a transaction to be verified and appended to the blockchain, each node must mathematically verify that the transaction is correct[16]. Each node contains a copy of the blockchain and a complete record of all transactions that occurred on the

[13] *Ibid.*
[14] Wright A., De Filippi P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*, 2.
[15] Pilkington M. (2015). Blockchain Technology: Principles and Applications Research Handbook on Digital Transformations. *Research Handbook on Digital Transformations*, 6.
[16] Evans J. (2018). Curb Your Enthusiasm: The Real Implications of Blockchain in the Legal Industry. *The Journal of Business, Entrepreneurship & Law*, 11(2), 276.

blockchain. The blocks themselves, depending on the system, are mainly produced by miners, a particular type of blockchain user. The miner creates the block most often by one of two ways, either by solving mathematical computations known as the proof of work or by a method named proof of stake[17].

[17] Pilkington, *supra nota* 15, 6-7.

2. THE CCPA AND GDPR

In the previous chapter the main features, principles and applications of blockchain technologies have been outlined. In order to discuss and analyze how the privacy legislatures, the GDPR and CCPA, are applicable to blockchain technologies, an outline of the two privacy legislations must be given. The outline shall shed light particularly on the features of the two documents that may possibly affect and apply to blockchain technologies.

2.1. General Data Protection Regulation

The GDPR entered into force on 25th May, 2018, since then it has affected the threshold of privacy standards for all European residents, and on the other hand impacted how businesses, small and large, handle and process data of these residents. The GDPR being applicable to EU citizens and residents established by the territorial scope of the regulation, ensures the impact of the document to be grand[18], having an impact on organizations dealing with personal data globally. Since the entry of the GDPR into force, the amount of GDPR related fines has grown to more than 200[19]. This displays how seriously European institutions have taken to uphold the core principle of the GDPR, which states in Article 1 Section 2 that the "… Regulation protects fundamental rights and freedoms of persons, in particular their right to protection of personal data"[20]. The principle of

[18] Goddard, M. (2017) .The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal Of Market Research*, 59(6), 703-705.

[19] More Than 200 GDPR Fines Issued Totaling €144 Million, New Study by Privacy Affairs Finds. (2020). Retrieved 10 May 2020, from https://martechseries.com/mts-insights/staff-writers/200-gdpr-fines-issued-totaling-e144-million-new-study-privacy-affairs-finds/

[20] *See* GDPR Article 1(2)

privacy as a fundamental human right gives effect to the six main principles laid out in the regulation, namely fairness and lawfulness, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality[21]. These principles are enriched by the concept of privacy by design.

2.2. California Consumer Protection Act

The saying "correlation does not mean causation" holds true, yet it could be argued that the GDPR has influenced legislators around the world to attempt to uphold the rights of persons in the context of data protection within their respective legislations. Shortly after the GDPR, known as the largest scale document of its kind, was enacted, the California State Legislature passed the California Consumer Privacy Act, officially named Assembly Bill No. 375 on the 28th of June 2018[22]. The CCPA became effective on January 1st of 2020. The act is the first broad privacy law ever passed in the United States(US). According to the Assembly Committee on Privacy and Consumer protection stated in the preamble of the CCPA, it gives residents of the state of California a right to have a privacy standard to rely on, by allowing Californian residents the right to know what personal information is being collected on them by a business, whether that personal information is sold by the business to third parties, the right to access the personal information, the right to request deletion of the personal information and lastly the right to "opt-out" to sale of their personal information[23]. All these newly given rights to the citizens of California, resemble and are in effect very similar in nature to the rights that had been given to European residents by the enactment of the GDPR. The legislators of California, the birthplace of the "Silicon Valley", have shown to follow closely the measures taken in Europe regarding data privacy, by enacting the CCPA and allowing a legal basis for upholding of the principle of privacy on the internet.

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[22] "Bill Text – AB-375 Privacy: personal information: businesses". (2018) *Leginfo.legislature.ca.gov.* (California Consumer Protection Act)
[23] *Ibid.*

2.3. The Concept of Personal Data in the General Data Protection Regulation and the California Consumer Protection Act

Both the CCPA and GDPR deal with data subjects as primary actors, and in fact the documents aim to protect the rights of these actors. Data subjects possess personal data that is connected to them; in the CCPA, the term is referred to as personal information, as opposed to personal data in the GDPR. The CCPA defines personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[24], while the GDPR defines personal data as "any information relating to an identified or identifiable natural person (data subject), directly or indirectly, in particular by reference to an identifier."[25] At first glance, the two definitions set out in the GDPR and CCPA seems quite similar. In fact, both definitions provide a broad scope of interpretation on what could be viewed as personal data. Another vital similarity is that both definitions categorize personal data as related to data that not only identifies a person directly, but any information that provides the opportunity for a person to be identified. This inclusive definition creates an opportunity to interpret personal data in an expansive manner, from the full name of the person identified, to the Internet Protocol (IP) address of an internet user. Additionally, both the CCPA and GDPR provide an opportunity for technical and organizational measures to create information that does not constitute personal data or personal information, through the use of anonymization techniques. In the case of the GDPR anonymized data is data that cannot be utilized to identify a data subject. In the case of the CCPA, the same principal applies to deidentified and aggregate data. "Deidentified" means information that cannot reasonably identify or be linked, directly or indirectly, to a particular consumer[26]. "Aggregate" consumer information is information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or

[24] *See* CCPA 1798.140(o)(1-2)
[25] See GDPR Article 4(1)
[26] Marini, A. et al. (2020) Future of Privacy Forum. Retrieved 8 April 2020, from https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

household, including via a device[27]. The basis of personal data for both the CCPA and GDPR is in principle very similar, taking an open and broad approach, while allowing for the opportunity for anonymizing of data to deidentify information from the data subject. The difference between personal data in the GDPR and personal information in the CCPA lies in the scope of application. The CCPA does not treat privacy of individuals as a human right, unlike the GDPR. As taken from the name of the document, California Consumer Privacy Act, the CCPA narrows the scope of application to consumers dealing with commercial entities[28], while the GDPR does not differentiate the scope of applicability, applying to all actors on the internet, consumer or not, in an equal manner.

2.4. Data on the Blockchain considering the General Data Protection Regulation and the California Consumer Protection Act

Prior to venturing on the applicability of blockchain technology to the GDPR and CCPA, it is vital to comprehend what information on a blockchain may be deemed personal data , to set a scope of applicability. It must be noted that a DLT, on which a blockchain is built on, relies on asymmetric encryption[29]to secure the transmission of data from one blockchain user to the other. Asymmetric encryption, is a method of encryption ensures trust in communication between users of a blockchain network. A block on a DLT, as mentioned previously, in its simplest form contains two parts, the header which is metadata and the block content itself, which is often encrypted. Taking into account the content of a block in the blockchain, the question to be posed is does data stored on a block qualify as personal data under the GDPR and as personal information under the CCPA?

[27] *Ibid.*
[28] Chander A *et al.* (2019, August 7). Catalyzing Privacy Law. *Georgetown Law Faculty Publications and Other Works*.
[29] Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Cambridge, United Kingdom: Cambridge University Press, 90.

2.4.1. Personal Data on Blockchain Under the GDPR

Under the GDPR there are different classifications of types of data such as personal data, pseudonymized data and anonymized data. Per the regulation, only data that is anonymized can no longer be considered personal data and can no longer identify a data subject[30]. As mentioned in the previous chapters, blockchain technology in its technical and organizational implementation may vary vastly, yet any block on the blockchain constitutes a transaction which can be of any type such a financial transaction or an exchange of information between two users. This transactional data is stored in one of three ways, as a plain text, in an encrypted form which is a two-way function or in a hashed form which is a one-way function[31]. For personal data to be anonymized there must be further action taken to anonymize it, clearly since plain text data is not processed in any form for anonymization to take place, it would constitute personal data whenever there is any data relating to a data subject in the plain text. The latter part of the discussion is on whether methods of two-way encryption and hashing may be viewed as a method of anonymization of personal data on a blockchain. The European Union Agency for Cybersecurity (ENISA), one of the most respected agencies of the EU on cybersecurity, have classed two-way encryption and hashing as pseudonymization techniques rather than an anonymization techniques[32]. Similarly, the Article 29 Data Protection Working Party has classified hashing as a pseudonymization technique, as it is possible to link the output of the hash function to the data subject[33]. Therefore, any type of transactional data on a blockchain may be viewed as personal data relating to a data subject under the GDPR. This conclusion is made based on the strict stance EU bodies and particularly data protection related bodies take towards what type of data may be considered personal data or already anonymized data. For example in the Case 582/14, Patrick Breyer v. Germany, both dynamic and static Internet Protocol (IP) addresses where established to be regarded as personal data, displayed the wide range of data that is considered personal data under the GDPR [34]. The sole action of irreversibility of data such as the technique of hashing does

[30] See GDPR Recital 26.
[31] *Ibid*, 17.
[32] ENISA. (2019, January 28). Pseudonymisation techniques and best practices, Recommendations on shaping technology according to data protection and privacy provisions. *European Union Agency for Cybersecurity*.
[33] *Ibid.*
[34] ECJ. (2018). 19.10.2017, Patrick Breyer v Bundesrepublik Deutschland, Case C–582/14, EU:C:2016:779

not necessarily cause data to no longer be singled out, inferred or linked to a data subject[35]. The EU sets a high standard on the definition of anonymized data, thus making it unlikely that any data on a blockchain could be considered fully anonymized, unless specific measures are established particularly to achieve this aim. The second aspect to a block on the blockchain other than what was referred to as transactional data is the public key. A public key supplied with no additional information could not be singled out, inferred or linked to a data subject, yet with a supply of such additional information either voluntarily or through mistake, the public key may be connected to a natural person[36] and thus be regarded as personal data under the GDPR. It must be concluded that both aspects of a blockchain, the public key and transactional data may be regarded as personal data. This in turn create the need to analyze and evaluate how the structure and technical aspects of blockchain must be implemented under the GDPR, and what substantive aspects of the regulation affect the application of blockchain under the GDPR regime.

2.4.2. Personal Information on Blockchain Under the CCPA

The CCPA seems to take a similarly broad stance on the what constitutes personal data, or personal information as described in the CCPA, in comparison to its European counterpart[37]. On the other hand, the CCPA has a more comprehensive list of 11 categories of what can be deemed personal information of a consumer. As discussed, a blockchain transaction shall always contain transactional data and a public key. The Lex Infromatica literature does not provide for substantial analysis on what could be deemed personal information on a blockchain in light of the CCPA. The comprehensive list of categories of personal information in the CCPA, in Section 1798.140(b)(o) of the Act shall not be listed, yet what must be brought to attention is the category known as identifiers and the category of commercial information. Identifiers refer to the full name, social security number or similarly as in the case of the GDPR, online automatic identifiers such as an IP address[38], while commercial information refers to records of personal property, such as

[35] Bolognini, L., Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review*, 33(2), 171-181.
[36] Reid F., Harrigan M. (2011). An Analysis of Anonymity in the Bitcoin System. *Cornell University*, 2.
[37] Kessler J. (2019). Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource". *Southern California Law Review*, 93(1), 108.
[38] Drake M. (2019). The California Consumer Privacy Act of 2018: Why It Matters to Clients in Arkansas. *The Arkansas Lawyer,* 54(1).

purchase history[39]. It could be argued that transactional data on a blockchain may fall under the definition of personal information, for example, if a person were to include any identifier the blockchain would potentially be subject to the CCPA. Blockchain is often used for commercial purposes such as banking services that would definitely include commercial information and thus fall under the CCPA. Similarly, a public key, if supplied with additional information would be rendered to be an identifier and thus be subject to the California act.

[39] *Ibid.*

3. BLOCKCHAIN'S APPLICABILITY TO THE GENERAL DATA PROTECTION REGULATION AND THE CALIFORNIA CONSUMER PROTECTION ACT

Concepts and aspects of the GDPR and CCPA that may determine the scope of the applicability of blockchain technologies to the privacy laws and what type of information on a blockchain system may be seen as being affected by the legislations has been reviewed in the previous chapter. This chapter shall provide an analysis on how this information on the blockchain shall be affected by the GDPR and CCPA, particularly how the rights afforded to persons under the privacy regimes shall affect blockchain based solutions and what risks and steps preclude blockchain solutions' sustainability under the GDPR and CCPA.

3.1. General Data Protection Regulation and Blockchain

From the previous discussion, it has been established that any information relating to a data subject, even if transformed into mathematical functions or other forms in an attempt to pseudonymize or anonymize such personal data, shall still be applicable under the GDPR, thus the material scope of the regulation's applicability to blockchain is broad. In effect, natural and legal persons who create such blockchain solutions must assess the rights of data subjects. Firstly, what must be assessed is who is responsible for ensuring that the rights of data subjects are regulated correctly. The GDPR defines a data controller as "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"[40].

Blockchain's underlying premise is in contrast with the GDPR's approach to data controllers, being assumed to be a single entity. Unlike most systems, there is no central figure that determines the purposes and means of the processing of personal data on a blockchain, particularly on a public blockchain system where there is no authoritative or moderating figure. A European Parliament report on Blockchain published in 2018 had highlighted "the fact that blockchain users may be both data controllers, for the personal data that they upload onto the ledger, and data processors, by virtue of storing a full copy of the ledger on their own computer"[41]. As there is no central authority it is truly difficult to determine how national data protection authorities shall define data controllers on a public blockchain. If a user known as a node would be a data controller, it would create a burden of legal obligation under the GDPR on every single user of the blockchain technology. Though structurally each node depends on the other for the functioning of the blockchain, each node does not have access to the information stored on other nodes in a non-encrypted and undecipherable manner. This would not allow for nodes to control the means and methods of processing as stipulated in the GDPR[42]. On the other hand, the choice of assigning each node as a data controller in relation to other nodes and vice versa creates a risk for the sustainability of the blockchain system itself. As previously mentioned in the introductory chapters, each node stores a copy of the blockchain in an encrypted manner, and must verify the existence of the copy of the node in order for a transaction to be possible on the blockchain. If we were to suppose that each node is a data controller, once one data controller is in breach of its obligations under the European Regulation, and a data protection authority requests it to suspend its function, then the entire blockchain would cease its ability to function[43]. Even though the European Parliament report characterizes users as data controllers, the consequences of such classification seem grave towards the development of the blockchain field, as it would create an unreasonable burden upon each user. Currently, there exists no exact definition of who is considered a data controller on a blockchain. Since at present it is not possible to precisely state who in fact acts as a data controller in a blockchain system, it is necessary to overlook the

[40] *See* GDPR Article 4(7).
[41] Committee on International Trade (2020). Report on Blockchain: a forward-looking trade policy. *Committee on International Trade*.
[42] Finck, *supra nota*, 27, 100-101.
[43] *Ibid.*

component of responsibility when analyzing the applicability of blockchain to the GDPR. It would be vital to assume the presence of a data controller, one which cannot be concretely named, to be able to discuss further the applicability of blockchain to the GDPR. Anyone considered a data controller implementing a blockchain would have to consider the right to be forgotten, the principle of data minimization and privacy by design. As the scope of responsibility of persons on a blockchain system has been explored, it is of essence to discuss how the substantive aspect of the GDPR applies to blockchain.

3.1.1. The Right to Be Forgotten and The Right to Rectification

One of the main concepts under the GDPR is the right to be forgotten. Article 17 of the Regulation gives a data subject the right to request erasure of their personal data on the basis of various grounds, (a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed (b) that the data subject withdraws consent on which the processing is based or where there is no other ground for processing; (c) that the data subject objects to the processing and that there are no overriding legitimate grounds for processing; (d) that data has been unlawfully processed; (e) that personal data has to be erased for compliance with national or supranational law to which the controller is subject[44]. It should be noted that the right to forgotten, formally referred to as the right to erasure is not an absolute right and shall be allowed to be exercised by the data subject if it is based on at least one of the grounds mentioned above in Article 17(1)[45]. All of the grounds for the right to be forgotten pose risks for the functionality of a public blockchain, as reported by the Open Data Institute, "the irreversibility and transparency of public blockchains mean they are probably unsuitable for personal data"[46].These risks shall be discussed further, yet it is necessary to introduce the right to rectification as the same risks materialize in regards to the functionality of blockchain when the right to rectification is invoked. Article 16 of the GDPR, provides to a data subject the right to rectify personal data of the data subject that is incorrect. Both the right to rectification and the right to be forgotten when

[44] *See* GDPR Article 17.
[45] Salmensuu C.(2018). The General Data Protection Regulation and the Blockchains (2018). *Liikejuridiikka*, 16.

[46] Open Data Institute. (2018). Applying Blockchain Technology In Global Data Infrastructure – The ODI. *Open Data Institute*, 16.

requested by a data subject requires change or erasure of data. Blockchain's reprised quality is that the essence of a DLT based system is not controlled by a central authority, is tamper free and consequently censorship free[47]. This quality of blockchain is expressed through the fact that public blockchain systems are immutable and resistant to erasure. Viewing blockchain through a GDPR compatible lens is not possible – prima facie it is not possible to implement a blockchain system that is GDPR compliant[48] – yet such a claim should need further analysis. Firstly, on the right to rectification in the context of blockchain, rectification entails the possibility for a user to register correct information on themselves, overriding the previously false information. Solely the act of rectification is possible, by registering the correct information on the blockchain including a message stating that the previously created entry was false[49]. The topic of uncertainty is how to abide by the need to erase erroneous information as prescribed by the GDPR, this in the same manner applies to how to erase information when a data subject requests to exercise their right to be forgotten. Two approaches may be taken to inspect whether there is a necessity to comply with a data subject's request to erasure as a data controller. One of the approaches is viewing the proportionality of the right to be forgotten towards data subject. A possible reasoning to not carry out a request to execute a person's right to be forgotten is when there are overriding legitimate grounds of processing as stated in Recital 47 of the GDPR[50]. The essence of the GDPR is to allow individuals to exercise their data protection rights and prevail over the data controller[51]. When taking proportionality into account, it would seem suitable to claim that the restriction on a data subject's right to erasure would be acceptable, as a request to erase information on a blockchain would render the whole blockchain not functional. Thus, the overriding legitimate ground of processing in this case would be the blockchain network's functionality[52]. Another option for the compatibility of the right to be forgotten with the blockchain would be to not override the right, but to ensure technological and organizational tools are created in a manner that would at least in part allow for the exercise of the right to be forgotten by a data subject. As previously stated a block in the blockchain consists of transactional information and the public key. Storing the transactional information which contains personal data off the blockchain, on a traditional database

[47] Nakomoto, *supra nota* 3.
[48] Finck, *supra nota* 17.
[49] Barsan I., (2019, July 1). Public Blockchains: The Privacy-Transparency Conundrum. *Revue Trimestrielle de Droit Financier (RTDF) N° 2 – 2019*, 49
[50] *See* GDPR Recital 47.
[51] Walters N. (2019). Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance.*17 Canadian Journal of Law and Technology 276*, 11.
[52] *Ibid.*

system, would allow to comply with the GDPR, while simultaneously not affecting the blockchain structure[53]. The second aspect of the block, the public key has no possibility for erasure, and thus a proportionality test must be taken to examination on a case by case basis whether there is an overriding legitimate ground of processing, by balancing the powers between the data subject and the data controller.

3.1.2. Data Minimization

Another aspect of the GDPR which poses similar quagmires as the concept of erasure on a blockchain, is the principle of data minimization. Article 5 of the GDPR prescribes that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"[54], known as the data minimization principle. The blockchain in structure is almost immutable and works on an "append only" principle[55], meaning information on the blockchain can only be added to the blockchain itself, yet not be overwritten or removed. This characteristic pertains risk to adhere by the concept of data minimization as a principle of a blockchain system. The same conundrum of adhering to the principle of data minimization is not limited to blockchain, but materializes in other novel technologies such as big data[56]. Yet, a more holistic approach may be taken in order to view a blockchain as aligned with the principle of data minimization. A data controller could assess what information would be necessary for a transaction on a blockchain to be successful and thus attempt to minimize the disclosed personal data of a data subject[57]. With regard to the limitation aspect of the data minimization principle, the assessment of what information would be necessary for a transaction to occur would not be sufficient, as the need for retention periods of the personal data should be established. The French data protection authority has stated in its analysis of blockchain that in reality the retention period of personal data on a blockchain is directly related to the duration of the life of the blockchain system itself[58]. Thus,

[53] *Ibid, 36.*
[54] *See* GDPR Article 5
[55] Walters, *supra nota 51*, 29.
[56] Zarsky T. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, 47(4).

[57] Ramsay, S. (2018). The General Data Protection Regulation vs. The Blockchain: A legal study on the compatibility between blockchain technology and the GDPR. *Stockholm University*, 53-58.

[58] CNIL. (2018) .Blockchain – Solutions for a responsible use of the blockchain in the context of personal data. CNIL 7-8.

even though in part it would be possible to attempt to integrate the principle of data minimization into a blockchain based solution, the appropriate level of efficiency of doing so would be limited and would not be able to properly cover the limitation aspect of the data minimization principle.

3.1.3. Privacy by Design and Privacy by Default

A core concept of the GDPR is data protection by design and by default, often referenced to as privacy by design and by default. This concept engulfs and touches upon the previously mentioned rights in this chapter that affect blockchain. Data protection by design and by default established in Article 25(2) of the GDPR establishes the need for a data controller to "implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" and requests for data controllers to "implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles". The concept of privacy by design does not create the obligation for a data controller to apply a specific measure. The principle of privacy by design promotes an implementation of a software that considers privacy whenever creating a new service, including for example data minimization. Once again, it seems that the basis of the structure of a blockchain does not make it possible to be compliant with the GDPR, yet another argument could be made. The notion of pseudonymization and anonymization is a part of a blockchain solution, as many blockchain technologies employ encryption to ensure privacy. Which allows it to at least in part attempt to enrich the privacy by design concept.

3.2. California Consumer Protection Act and Blockchain

The previous chapter had examined the main aspects of the interoperability between blockchain technologies and the GDPR, and to what extent blockchain based solutions should need to adhere to the GDPR regime. This chapter aims to similarly evaluate the arena of blockchain under the

CCPA. Yet, unlike the GDPR's overarching effect on blockchain, the compatibility and applicability between the CCPA and blockchain is at a different stage of progress in terms of research into the topic. The amount of research into the subject of the applicability of blockchain under the CCPA is miniscule, due to the recent nature of the enactment of the CCPA, being only applicable since the 1st of January of 2020. It has been established prior in the research that under the CCPA both the transactional data on a blockchain as well as the public key linking to the transaction on the blockchain would be viewed as personal information under the California Consumer Protection Act. Theoretically, information on a blockchain would constitute personal information under the CCPA, yet the act unlike the GDPR is narrow in scope. The act only applies to businesses that collect a California consumer's personal information and that satisfy one of the three following requirements:

a) The business has annual gross revenues in excess of twenty-five million dollars, or

b) The business alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, or

c) The business derives 50 percent or more of its annual revenues from selling consumers' personal information[59].

The requirements at first glance seem to target a very narrow set of businesses, and even though the CCPA's scope is narrower than that of the GDPR[60], it still affects manifold of businesses. The reason for it reaching a large amount of businesses is the second requirement to be deemed liable under the CCPA. The CCPA takes a broad stance on what could be deemed personal information[61]. The broad stance of what could be seen as personal information of a consumer in conjunction with no definite expansion on the concept of sharing under the second requirement to be subject to the CCPA could place a large amount of small blockchain based solutions under the scrutiny of the CCPA[62]. The nature of blockchain requires for each user ie. node to have a copy of all information on the blockchain as a part of the technology's integrity. If the nodes were to be

[59] *See* CCPA 1798.140(1).
[60] Erdem B. (2019). Towards a Transatlantic Concept of Data Privacy. *Fordham Intellectual Property, Media and Entertainment Law Journal* 30(1), 177.
[61] *Ibid.*

treated as devices under the CCPA, and since each node possesses a copy of the whole chain, this may be viewed as sharing between nodes. If the blockchain were to have personal information of 50,000 or more users, it could be seen to fall under the CCPA. In 5 years since its creation the Ethereum blockchain contains over 10 million blocks[63]. Etherum blockchain and many more contains personal information of 50,000 or more consumers, thus making blockchain based solutions applicable to CCPA regulation. Since the material scope of applicability of blockchain to the CCPA has been established, it is also vital to examine how certain aspects of the CCPA would affect the functioning of a blockchain technology.

3.2.1. The Right to Deletion

The CCPA grants a right to consumers similar in effect as the GDPR's right to be forgotten. The CCPA affords consumers the right to deletion, Section 1798.105 of the CCPA states, "A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer"[64]. Yet, unlike the GDPR, the CCPA grants a wider scope of exceptions to not permit a consumer to exercise their right to request deletion. Section 1798.105(d) of the CCPA lays out that:

A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

a) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

[63] Thomson, G. (2020). The Ethereum blockchain is now 10 million blocks long - Decrypt. Retrieved 10 May 2020, from https://decrypt.co/27555/the-ethereum-blockchain-is-now-10-million-blocks-long
[64] *See* CCPA 1798.105(d)

b) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

c) Debug to identify and repair errors that impair existing intended functionality.

d) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

When attempting to permit a user of a blockchain system to exercise their right to deletion, two aspects must be evaluated that may limit the possibility for a consumer to exercise their right to deletion. Firstly, in a decentralized system such is the case of a blockchain technology, who shall be regarded as being liable to carry out a request to deletion, when there is no centralized body acting as the business liable to carry out such request. Liability shall arise to be a legal challenge within the CCPA framework, this relates also to blockchain based companies who need to comply with the CCPA. When there is no centralized authority determining the means of personal information deletion, there would not then be a possibility for a consumer to request that their personal information is deleted. Secondly, the nature of a blockchain system renders it and data records on it immutable[65]. If the first hurdle of assigning a certain entity responsible for allowing a consumer to request that their personal information is deleted, the nature of a blockchain system would still pose hurdles to practically achieving the exercise of the right of a consumer to request that their personal information be deleted. The only possibility for a blockchain based business to not provide the option for a consumer to have the right to deletion could be point one of Section 1798.105(d) of the CCPA. It could be argued that in order for a consumer to be a participant of a blockchain technology, within the context of the ongoing business relationship with the consumer, the consumer would not be able to possess the right to deletion. The context would then be the irregularity of the blockchain system being decentralized. This theoretically could be an option for blockchain businesses to avoid a need to provide a consumer to have the right to deletion.

[65] Hofmann F. *et al*. (2017). The immutability concept of blockchains and benefits of early standardization. *IEEE*, 2.

4. EVALUATING THE EFFECT OF THE CCPA AND GDPR ON BC TECHNOLOGIES

The previous chapters outlined the major points of friction between blockchain technologies and the CCPA and the GDPR. This chapter aims at exploring the similarities and differences in the applicability of blockchain technologies to the CCPA and the GDPR, and ultimately aims to suggest possible outcomes that the CCPA and GDPR may have on the development of blockchain technologies.

4.1. Similarities in applicability of blockchain technologies to the CCPA and GDPR

The similarities in the applicability of blockchain technologies to the CCPA and GDPR lie firstly in the two privacy law's definition of personal information and secondly the right to be forgotten, known as the right to deletion under the CCPA granted to persons by the two documents compared. Both the CCPA and the GDPR take a broad stance as to what can be deemed as personal information[66]. The broad definitions of personal information allows for information that is typically stored on a blockchain system to fall under the definition of personal information. This indeed allows for a fruitful discussion on the applicability of blockchain technologies to the CCPA and GDPR.

[66]Chander. *supra nota 28.*

If the definitions of personal information in the CCPA and GDPR excluded information on a blockchain, there would not be a place for examining the effects of the GDPR and CCPA on blockchain, as technologies of such nature would not be burdened to evaluate compliance to the privacy laws. Since it has been established in previous chapters, blockchain technologies fall under scrutiny of the GDPR and CCPA, a blockchain based business would need to evaluate to what extent it would need to grant persons rights granted by the GDPR and CCPA. The overlapping of the CCPA and GDPR on the concept of data erasure [67]creates a similarity in extent of applicability. Both documents give persons the opportunity to request the erasure of the personal information that they have provided to a business[68]. This right similarly creates a clash with blockchain technologies, particularly due to the technical structure of a blockchain. Under both the CCPA and GDPR it is impossible for a blockchain business to adhere to the right to be forgotten except without workarounds such as partial off-chain implementations of a blockchain. Meaning that certain data, particularly personal data, that originally would fall under the general structure of a blockchain would be stored on a database that would be possible. This would give a user the opportunity to request deletion of data as in any other centralized system. Such a workaround would achieve the aim of allowing blockchain technologies to achieve the right to be forgotten under the GDPR and CCPA[69]. On the other hand, this would diminish the reliability and immutability aspect of blockchain, the core aspect of blockchain.

4.2. Differences in applicability of blockchain technologies to the CCPA and GDPR

From first glance, the CCPA and GDPR both seem to aim to catalyze access to privacy, particularly the right to privacy of individuals. Yet, where the GDPR could be compared to a doctorate research paper, the CCPA is closer to an assignment written the night before the deadline[70]. The difference in extensity and scope regarding data privacy between GDPR and CCPA causes for a strong

[67] Pernot-Leplay, Emmanuel, EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model? (2020). Colorado Technology Law Journal, Vol. 18, No. 1, 2020. Available at SSRN: https://ssrn.com/abstract=3542730, p. 118
[68] *Ibid.*
[69] Bayle A., Koscina M., Manset D., Perez-Kempner O. (2018). When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. *IEEE,* 791.
[70] Chander, *supra nota 27, 12.*

difference in the applicability of blockchain technologies to the GDPR and CCPA. The GDPR obliges a higher level of diligence and respect for a data subject's privacy on a blockchain technology compared to its US counterpart[71]. The GDPR unlike the CCPA covers all citizens, rather than focusing on a particular group. The CCPA on the other hand only applies protection to consumers residing in California.

The difference can be largely contributed to factors such as the US legal system, where legal precedent trumps legislation, unlike EU law. The CCPA would need time to establish basis for case law that would affect the interpretation of the CCPA. In outcome, the scope and the substantive elements are more extensive in the GDPR than the CCPA. This, applies also to the difference in extent of applicability of blockchain to the privacy legislations. The GDPR constrains more the flexibility in implementation of blockchain than the CCPA, as it prescribes more rights to the user of the blockchain. This makes it more difficult for blockchain solutions possessing users in the EU to remain legally compliant since the enactment of the GDPR than the CCPA.

Though the GDPR is more stringently applicable to blockchain than CCPA when analyzed at present, this may not remain the case. Californian authoritative bodies may set guidelines or establish case law that may affect the applicability of blockchain, as the CCPA is yet to be implemented on a wide scale.

[71] Hartzog W., Neil M. (2019, August 23). Privacy's Constitutional Moment and the Limits of Data Protection. 61 Boston College Law Review, 28.

CONCLUSION

The aim of this paper was to analyze whether the GDPR and CCPA are applicable to BC technologies, and if so, how the two privacy laws shall affect the development of BC based technologies and businesses. The paper aimed to firstly describe the technical basics of blockchain systems in order to evaluate how these technical characteristics may be affected or applied under the GDPR and CCPA. Secondly, the paper described the main characteristics of the GDPR and CCPA, particular attention was brought to aspects of the two privacy laws that may have an effect on blockchain technologies. It has been determined that both the GDPR and CCPA are attempts to consolidate a framework for the use and handling of personal data of individuals. When evaluating the compatibility of blockchain technologies to the GDPR and CCPA, it can be concluded that legislators drafting the two privacy laws have not to a sufficient extent considered to draft documents *de lege ferenda*. The definitions of personal data in both the GDPR and CCPA create the basis for all data related to an individual on a blockchain to fully fall within the ambit of the two discussed pieces of privacy legislation. This causes blockchain technologies to be forced to comply with the GDPR and CCPA. The GDPR requires blockchain systems to be implemented in a manner that adheres to rights granted by the GDPR such as the right to be forgotten, the right to rectification, and to apply principles of the GDPR such as data minimization, privacy by design and privacy by default. This creates burden upon persons attempting to implement blockchain technologies. The CCPA also creates a burden for the implementation of blockchain technologies, particularly by establishing the right to deletion.

When comparing the applicability of the GDPR and the CCPA to blockchain technologies, it can be concluded that the GDPR creates a higher level of strain upon the development of blockchain technologies compared to CCPA, with a more numerous list of rights granted to persons that could possibly affect the rate of development of blockchain technologies. Even though the GDPR and CCPA both attempt to establish a data protection regime that allows for persons to take control of

their data, they both fail to assess the true extent of technological progress. Innovative approaches to data handling such as blockchain are still in their early stages of research and implementation. Creating legal barriers as do the GDPR and CCPA only restricts the opportunity for blockchain technologies to flourish. The GDPR and CCPA both discourage innovators in the blockchain field to attempt pursuing novel implementations, by creating a sense of responsibility and fear of breaching laws and receiving fines. Furthermore, it is of disappointment that the drafters of the CCPA have not attempted to mitigate the unnecessary burden that the GDPR has created for innovative technologies but on the contrary, attempted to create a similar level of burden as the GDPR. Both European and American legislators will have to carefully examine the balance of proportionality between enforcing data protection principles and allowing for the experimentation in the emerging field of blockchain. Blockchain businesses may attempt at present to create technical measures to reduce the necessity to uphold data protection principles prescribed by the GDPR and CCPA, yet without a clear formulation of guidelines given to blockchain developers on how they should comply with privacy laws, the current state of applicability of blockchain technologies to the GDPR and CCPA will lead to a decline in progress in the field of blockchain. Changing the existing GDPR and CCPA to allow for emerging technologies to evolve would be, in the author's opinion, a disproportionally complicated task. To change the present models of data privacy, legislators should push to create a new model of understanding of data privacy, one where novel technological systems are encouraged, and one which makes the GDPR and CCPA obsolete and replaced by data protection standards that are forward looking. If change would not be possible in the current regulatory framework, there should be an attempt to create particular new guidelines in regard to particular technologies. Technologies that are early in progress should be analyzed from a technical and legal stand point in order to create specific guidelines easing uncertainty in compliance with regulations. A third option would be to lower the standard of enforceability of breach of the GDPR and CCPA towards emerging technology such as blockchain or artificial intelligence. Overall, there is a need to reassess how to ensure the compatibility between the respect for data protection and privacy laws worldwide and the possibility for unrestrictive technical implementation and experimentation.

LIST OF REFERENCES

Scientific books:

1. Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Cambridge, United Kingdom: Cambridge University Press.

2. Morabito, V. (2017). *Business Innovation Through Blockchain*. *s.l.*: Springer International Publishing AG

3. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Beijing, China: O'Reilly.

Scientific articles:

4. Bayle A., Koscina M., Manset D., Perez-Kempner O. (2018). When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. *IEEE,* 791.
5. Barsan I., (2019, July 1). Public Blockchains: The Privacy-Transparency Conundrum. *Revue Trimestrielle de Droit Financier (RTDF) N° 2 – 2019*, 49.
6. Bolognini, L., Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review*, 33(2), 171-181.

7. Chander A et al. (2019, August 7). Catalyzing Privacy Law. *Georgetown Law Faculty Publications and Other Works*.

8. CNIL, (2018). Blockchain – Solutions for a responsible use of the blockchain in the context of personal data. *CNIL*, 7-8.

9. Committee on International Trade (2020). Report on Blockchain: a forward-looking trade policy. *Committee on International Trade*.

10. Drake M. (2019). The California Consumer Privacy Act of 2018: Why It Matters to Clients in Arkansas. *The Arkansas Lawyer*, 54(1).

11. ENISA. (2019, January 28). Pseudonymisation techniques and best practices, Recommendations on shaping technology according to data protection and privacy provisions. *European Union Agency for Cybersecurity*.

12. Erdem B. (2019). Towards a Transatlantic Concept of Data Privacy. *Fordham Intellectual Property, Media and Entertainment Law Journal,* 30(1), 177.

13. Goddard, M. (2017) .The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal Of Market Research*, 59(6), 703-705.

14. Hartzog W., Neil M. (2019, August 23). Privacy's Constitutional Moment and the Limits of Data Protection. 61 *Boston College Law Review*, 28.

15. Hofmann F. et al. (2017). The immutability concept of blockchains and benefits of early standardization. *IEEE*, 2.

16. Kessler J. (2019). Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource". *Southern California Law Review*, 93(1), 108.

17. Evans J. (2018). Curb Your Enthusiasm: The Real Implications of Blockchain in the Legal Industry. *The Journal of Business, Entrepreneurship & Law*, 11(2), 276.

18. Open Data Institute. (2018). Applying Blockchain Technology In Global Data Infrastructure – The ODI. *Open Data Institute*, 16.

19. Davis L. (2020). The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation. *North Carolina Banking Institute*, (24)1.

20. Pilkington M. (2015). Blockchain Technology: Principles and Applications Research Handbook on Digital Transformations. *Research Handbook on Digital Transformations*, 6-7

21. Ramsay, S. (2018). The General Data Protection Regulation vs. The Blockchain: A legal study on the compatibility between blockchain technology and the GDPR. *Stockholm University*, 53-58.

22. Reid F., Harrigan M. (2011). An Analysis of Anonymity in the Bitcoin System. Cornell University, 2.

23. Salmensuu C .(2018). The General Data Protection Regulation and the Blockchains (2018). *Liikejuridiikka*, 16.

24. Truong, N. et al. (2019). Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things. *IEEE Transactions On Information Forensics And Security*, 14(10).

25. Walters N. (2019). Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance.*17 Canadian Journal of Law and Technology 276*, 11.

26. Wright A., De Filippi P. (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*, 2.

27. Zarsky T. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, 47(4).

EU and International legislation:

28. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Other Countries' Legislation:

29. "Privacy: personal information: businesses.". *Assembly Bill No. 1798.140/(o)(2) of June 28, 2018*. California State Legislature. (California Consumer Protection Regulation).

Court decisions:

30. ECJ. (2018). 19.10.2017, Patrick Breyer v Bundesrepublik Deutschland, Case C–582/14, EU:C:2016:779

Other sources:

31. Buterin, Vitalik.Ethereum Blog. (2015) Visions, Part 1: The Value of Blockchain Technology. Retrieved 8 April 2020, from https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

32. Gabriel, M. (2018). European countries join Blockchain Partnership - Shaping Europe's digital future - European Commission. Retrieved 8 April 2020, from https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

33.Gupta, V. (2017). A Brief History of Blockchain. Retrieved 10 May 2020, from https://hbr.org/2017/02/a-brief-history-of-blockchain

34. Litan, A. (2019). Blockchain's Big Bang: Web 3.0 - Avivah Litan. Retrieved 8 April 2020, from https://blogs.gartner.com/avivah-litan/2019/08/08/blockchains-big-bang-web-3-0/

35. Marini, A. et al. (2020) Future of Privacy Forum. Retrieved 8 April 2020, from https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

36. Merriam-Webster Dictionary, 'blockchain' Retrieved 8 April 2020, from https://www.merriam-webster.com/dictionary/blockchain

37. More Than 200 GDPR Fines Issued Totaling €144 Million, New Study by Privacy Affairs Finds. (2020). Retrieved 10 May 2020, from https://martechseries.com/mts-insights/staff-writers/200-gdpr-fines-issued-totaling-e144-million-new-study-privacy-affairs-finds/

38. Nakamoto, Satoshi. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 8 April 2020, from https://bitcoin.org/bitcoin.pdf.

39. Thomson, G. (2020). The Ethereum blockchain is now 10 million blocks long - Decrypt. Retrieved 10 May 2020, from https://decrypt.co/27555/the-ethereum-blockchain-is-now-10-million-blocks-long

Appendix 1. Non-exclusive license

Non-exclusive license for reproduction and for granting public access to the graduation thesis[1]

I _____Yusef Ward_____

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Applicability of Blockchain Technologies Under the General Data Protection Regulation and the California Consumer Protection Act,

supervised by ____Thomas Hoffmann_____ ,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*