TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Juha Nokelainen

ANALYSING THE EFFECTS OF GENERAL DATA PROTECTION REGULATION ARTICLE 17 ON BLOCKCHAIN TECHNOLOGY

Bachelor's thesis
European Union and International Law

Supervisor: Agnes Kasper, PhD

Tallinn 2019

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 8848 words from the introduction to the end of summary.

Juha Nokelainen ……
Student code: 166352HAJB
nokelainen.juha@gmail.com

Supervisor: Agnes Kasper, PhD: ……
The paper conforms to requirements in force

Chairman of the Defence Committee:
Permitted to the defence

……

TABLE OF CONTENTS

ABSTRACT

This research focuses on blockchain (BC) technology and its possible contradiction with European Union (EU) General Data Protection Regulation (GDPR) Article 17. Although the legislation is advanced compared to other similar legislations in the world it seems to ignore new technologies and innovations such as blockchain technology. The aim of this research is to analyse the current legislation, how it should be interpreted and scrutinise it from the perspective of blockchain technology. The research also covers European Union's principles and policies about technological development and their relation to EU legislation. The objective is to create a proper understanding about the current situation and analyse it from different viewpoints. Therefore the research questions concern how GDPR Article 17 affects on blockchain technology and should GDPR Article 17 be reviewed from the perspective of blockchain technology? In order to create clear and logical text that takes into account the necessary point of views, qualitative methods are used in this research. Traditional legal research will be needed to understand the subject. Legal interpretation and case analysis are also used in the research. Analysis of the legal acts is used to understand the necessary sections.

Keywords: Blockchain, Contradiction, Technological neutrality, GDPR, Decentralised

INTRODUCTION

During the last two decades, the world has witnessed the unforeseen technological revolution. The invention of computers and the internet has rapidly changed the world and its development. This development has created several new technologies that have the potential to change the way we use technology and perceive things. One of these technologies is blockchain technology. Blockchain technology can be used in order to execute several functions from storing data to creating new financial systems. At the same time, the legislators are trying to keep up with the development. The latest notable legislation in the European Union is General Data Protection Regulation (GDPR) that came in to force 25 May 2018 replacing the old Directive 95/46/FC.

GDPR aims to regulate cyberspace and contains several milestones concerning privacy and technological development. We haven't yet acknowledged the full impact of the Regulation. Article 17 of the GDPR declares the right to erasure or 'right to be forgotten'. The article gives individuals the right to ask for erasure of their personal data from the internet. At the same time blockchain technology is developing and the European Union is planning to further regulate the field. However, the GDPR contains sections that in principle contradict the very fundamental structure of the blockchain technology. This research aims to scrutinise whether GDPR and blockchain technology contradict and how GDPR should be interpreted especially if the EU is planning the two to co-exist. In addition, the research aims to analyse the possible outcome of the contradiction as well as the solutions. The problem seems to be that blockchain provides immutable and secure way of storing data. Once the information is stored in the blockchain it is extremely hard to alter or delete it. This feature is problematic considering the GDPR Article 17.

The research aims to elaborate on questions regarding the contradiction between blockchain technology and current European Union legislation. On one hand, how does General Data Protection Regulation Article 17 apply on blockchain technology? On the other, should GDPR Article 17 be reviewed from the perspective of blockchain technology and if yes, how? The methods for further scrutinising raised concerns include qualitative methods. Traditional legal

research will be needed to understand the subject. Legal interpretation and case analysis will also be used as well as analysis of legal acts.

The research begins by part one outlining what is blockchain technology covering also briefly the technical perspective. Different use-cases for blockchain technology are demonstrated. The examples cover both already existing and theoretical applications. The applications are also scrutinised from different viewpoints to understand the bigger picture. Hence the examples are not only from the private sector but also applications that United Nations and European Union are planning to utilise. After thorough overview chapter one ends to an analyse about the dangers of blockchain technology. The research concludes the situation and creates a distinction between technological and legislative threats.

Part two focuses on analysing the legislative position of blockchain technology. The chapter analyses whether blockchain technology falls under the scope of GDPR by using different kind of examples and cases. This part aims to scrutinise the legislation and the situation from several perspectives. In order to provide a proper understanding about the situation the research covers examples to demonstrate the complexity of the problems and the legislative stance that the European Union will eventually consider.

1. BLOCKCHAIN TECHNOLOGY

1.1 Functioning of the blockchain

The blockchain is described to be one of the greatest innovations in technology since the creation of the internet.[1] It is essentially a way to store structures of data into the distributed database that is a chain of so called blocks. Each block is connected to the previous block which creates a chain of blocks and the blocks are validated, currently in most of the cases, through a distributed computer network that has no central authority who would control the network. Therefore blockchain is usually maintained by a peer-to-peer network that validates the new blocks.[2] The idea is familiar from the centuries-old way of keeping paper records to make sure that people can not double spend their wealth. Instead of paper ledgers, which banks and other middlemen used, blockchain utilises distributed ledger technology (DLT) to verify the information.[3]

Public blockchain is run by independent people around the world who have decided to participate in maintaining the network by holding a copy of the transaction history and by validating new transactions.[4] These participants and their equipment are called nodes. The network of nodes maintains the blockchain network.[5] The fact that the nodes are spread all around the world in countries that are governed by countless legislations improves the network cencorship resistance. The network is therefore practically impossible to shut down. In private centralised networks the computational power of the network including the nodes are controlled by single authority.[6]

---

[1] Fenwick, M.; Kaal, W. A.; Vermeulen, E. P. (2017). Legal education in the blockchain revolution. *Vanderbilt Journal of Entertainment Technology Law* 20(2), p 363.
[2] Savu, I.; Carutasu, G.; Popa, C.; Cotet, C. (2017). Quality assurance framework for new property development: decentralized blockchain solution for the smart cities of the future. *Research and Science Today* 13(Supplement 2), p 199.
[3] Young, S. (2018). Changing governance models by applying blockchain computing. *Catholic University Journal of Law and Technology* 26(2), p 2.
[4] Botos, H. (2017). blockchain intelligence analysis. *Research and Science Today* 13(Supplement 1), p 43-44.
[5] Ibid.
[6] EU Blockchain Observatory and Forum (2018), BLOCKCHAIN AND THE GDPR, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf 5 March 2019. p 16.

Recorded data of the public blockchains is extremely hard to change later on and therefore the technology has good resistance for modification or altering after the block that has been added to the chain. On one hand, this creates a huge potential for blockchains to be used for example in different kind of records for sensitive information.[7] On the other, this immutability which at the same time can be extremely useful in a sense of authenticity of the information, brings us to one of the main questions of this research. How does the GDPR apply to a situation where personal information is practically impossible to alter or delete?

1.2. Applications of blockchain technology

Blockchain can be used for several purposes and the development is still in its early stages. The technology can be utilised both by a public (permissionless bc) and private (permissioned bc) sector.[8] The network can be centrally controlled or it can be decentralised. There are several different consensus mechanisms that are used to run the networks. The security and intended purpose usually determine what consensus mechanism provides the best outcome.[9] This part of the research aims to present different use-cases for the blockchain technology in order to understand the legal implications later in the research.

1.2.1. Cryptocurrencies

One of the first implementations of blockchain technology was introduced in 2008 by the unknown cryptographer who used an alias Satoshi Nakamoto.[10] This protocol introduced virtual currency called Bitcoin. It is described to be decentralised cryptocurrency that is electronically stored and created.[11] Bitcoin is a peer-to-peer network with no central authority or middlemen. Unlike Bitcoin, traditionally currencies are backed by a central bank or government. The fact, that the underlying technology behind cryptocurrencies is different than traditional currencies, can be seen

[7] Savu, I.; Carutasu, G.; Popa, C.; Cotet, C. (2017). Quality assurance framework for new property development: decentralized blockchain solution for the smart cities of the future. *Research and Science Today* 13(Supplement 2), p 199-200.
[8] Walch, A. (2017). The path of the blockchain lexicon (and the law). *Review of Banking and Financial Law* 36(2), p 720.
[9] Reyes, C. L. (2016). Moving beyond bitcoin to an endogenous theory of decentralized ledger technology regulation: An initial proposal. *Villanova Law Review* 61(1), p 196-199.
[10] Piazza, F. S. (2017). Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses. *Penn State Journal of Law and International Affairs* 5(2), p 265-266.
[11] Tu, K. V.; Meredith, M. W. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review* 90(1), p 275.

in many ways. On one hand it gives certain advantages for the users. On the other, consumer's legal certainty is not guaranteed when using cryptocurrencies.[12] A history has proven that people do not always have trust toward banks. This claim was proven between 2007-2009 during the financial crises.[13] Some people argue that Bitcoin was created against the corrupted banks and their ways to make profit.[14] Thus the core idea is, that there is no central authority controlling circulation or creation of bitcoins that people would have to rely on.[15] Bitcoin is part of the wider concept called cryptocurrencies. Since the creation of bitcoin over thousand cryptocurrency projects have been created.[16] In order to better explain the relation between blockchain and cryptocurrencies, one could think an internet as an example. Whereas blockchain is the internet, bitcoin is merely an e-mail platform that is built on top of the blockchain and is therefore only one use-case of a blockchain.[17]

Bitcoin is the biggest and most famous cryptocurrency and will be used as an example in this chapter. As noted, "Bitcoin is a cryptocurrency that is recorded on public blockchain ledger without any centralized authority".[18] Legal status of Bitcoin remains unclear and even the EU has not taken a proper stance on how it should be regulated.[19] Important factor seems to be, that when using traditional payment methods which require permission from a third party, bitcoin transactions do not require permission from middle men.[20] Anyone can create so-called wallet and in order to secure its user's validity and privacy, each wallet has a private key which is secret to other users. A unique private key can be used to authorise the desired transactions in the network. The wallet also contains a public key that other users can see. Public key could be described as an account number of the wallet.[21]

---

[12] Ibid., p 275.
[13] Ross, E. (2017). Nobody puts blockchain in corner: The disruptive role of blockchain technology in the financial services industry and current regulatory issues. *Catholic University Journal of Law and Technology* 25(2), p 355.
[14]Investopedia (2018), Why Governments Are Afraid of Bitcoin, Accessible: https://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp 10 March 2019.
[15] Adimi, G. (2018). How the new generation cryptocurrencies decoded the investment contract code: Analysis of us and eu laws. *Bocconi Legal Papers* 10(1), p 314.
[16]The Economist (2018), From one cryptocurrency to thousands, Accessible: https://www.economist.com/technology-quarterly/2018/09/01/from-one-cryptocurrency-to-thousands 7 March 2019.
[17] Jones, S. (2018). Data breaches, bitcoin, and blockchain technology: modern approach to the data-security crisis. *Texas Tech Law Review* 50(4), p 802.
[18] Iskander, M. (2017). Blockchain: The future of all data. *Intellectual Property and Technology Law Journal* 22(1), p 6.
[19] Shcherbak, S. (2014). How should bitcoin be regulated. *European Journal of Legal Studies* 7(1), p 42.
[20] Belcher, S. (2017). Tracing the invisible: Section 11's tracing requirement and blockchain. *Colorado Technology Law Journal* 16(1), p 162.
[21] Sonderegger, D. (2015). Regulatory and Economic Perplexity: Bitcoin Needs Just Bit of Regulation. *Washington University Journal of Law Policy* 47, p 181.

Before going into the use cases of cryptocurrencies, or in another word virtual currencies, it is necessary to scrutinise traditional forms of currencies. Different traditional currencies are also recognised as "fiat currencies".[22] Fiat comes from the language of Latin and the term refers to government-backed and issued currency which holds no intrinsic value unlike gold or silver, that are commodity-based.[23] People can buy and sell goods and services by money. Money works as a medium of exchange and governments control the issuance of the money and back the value by their repetition.[24] Fiat currencies have value, since people collectively believe so.[25] In countries where the government-backed currency is distrusted, bitcoin provides an alternative as a medium of exchange when the economy is unstable. This has already happened in Argentina where people have gained interest towards bitcoin.[26]

Virtual currencies are described as a new, intangible subsitute for traditional forms of money.[27] When a person wants to send bitcoins to another person they create a transaction. The transaction is validated through decentralised network which uses the computational power of independent parties of the network and the transaction is visible to everyone which creates unforeseen transparency in the economic world. Traditionally banks have verified the transactions and acted as middlemen. Blockchain eliminates the middlemen by using mathematical algorithms instead.[28]

In February 2019 news sites reported about US investment bank JP Morgan which had created a cryptocurrency in order to improve payment settlement process between its clients and businesses.[29] Bank's cryptocurrency, JPM Coin, is the first digital currency to be backed by a major US bank.[30] The bank has reportedly transferred money succesfully by using the blockchain network. The network will not be available for retail customers and it is intended for internal use

[22] Piazza, F. S. (2017). Bitcoin and the Blockchain as Possible Corporate Governance Tools: Strengths and Weaknesses. *Bocconi Legal Papers* 9, p 266.
[23] Ibid., p 266.
[24] Ibid., p 266.
[25] Ibid., p 266.
[26] Ibid., p 272.
[27] Ibid., p 267.
[28] Shcherbak, S. (2014). How should bitcoin be regulated. *European Journal of Legal Studies* 7(1), 41-83.
[29] BBC (2019), JP Morgan creates first US bank-backed crypto-currency, Accessible: https://www.bbc.com/news/business-47240760 7 March 2019.
[30] Ibid.

only. JP Morgan has initially started trials with private blockchain network in order to reduce risk and enable instant transfers.[31]

Although the idea of switching into digital currencies has drawn attention in the private sector, there are also examples from the public sector. Ukraine's central bank has initiated a trial to run its own national digital currency, the e-hryvnia. Cash payments are mainly used in Ukraine and the government has taken a stance to digitalise the payments. The project has been initiated in December 2018 and the results of the initiative will be used to analyse the next move of the nation.[32]

1.2.2. Initial Coin Offering

Perhaps one of the biggest accomplishments of a blockchain technology has been Initial Coin Offerings (ICO). ICO's have been created as a new way of raising capital from investors. This allows the developers to raise capital from investors all over the world without granting them voting rights or other rights that traditional fundraiser who contacted venture capitalists or held an Initial public offering (IPO) had to grant. Even though ICO investors are not legally protected, billions of dollars have been raised through ICO's.[33] Instead of equity shares that traditional IPO's provide for investors, ICO investors are given cryptocurrency coins or tokens. The investor buys one of the biggest cryptocurrencies such as bitcoin or ether and exchanges them to fundraisers tokens. The tokens would be used in a product that the company promises to deliver. From investors side, the idea is that the value of a token would later on increase and it could be sold with profit.[34]

1.2.3. Store of information

As described at the beginning of the part one of the research, blockchain is essentially a way to store information securely and efficiently. It provides a way to store information in a way that it can not be deleted or altered after adding it to the block of chains. The possibilities of the blockchain are countless and its full potential remains unexplored. This chapter aims to introduce

[31] Ibid.
[32] Cointelegraph (2019), Ukraine Completes Pilot Scheme for E-Hryvnia National Digital Currency, Accessible: https://cointelegraph.com/news/ukraine-completes-pilot-scheme-for-e-hryvnia-national-digital-currency 14 March 2019.
[33] Essaghoolian, N. (2019). Initial coin offerings: Emerging technology's fundraising innovation. *UCLA Law Review* 66(1), p 294.
[34] CNBC (2018), Tokenization: The world of ICOs, Accessible: https://www.cnbc.com/2018/07/13/initial-coin-offering-ico-what-are-they-how-do-they-work.html 10 March 2019.

use cases of blockchain technology as a store of information. It is important to note that these initiatives do not only come from the private companies or national level but also the European Union and United Nations have considered utilising blockchain technology for several purposes.

Since April 2018, a state of Nevada (US) has granted digital marriage certificates which are built by using smart contracts on the Ethereum blockchain.[35] Reportedly 950 marriage certificates in digital format have been issued.[36] Marriage certificates are only one example of a situation where trustworthy way to store data is needed. United Nations writes in its article about the situation where a massive earthquake destroyed entire cities in Haiti in 2010.[37] The problem occurred when authorities were searching for landowners that UN was unable to identify. In addition, there were many disputes about who was the actual landowner.[38] The article also concludes that these issues create problems when trying to recover from such destruction. It is noted that corruption plays a big role in many of the developing countries and as the land registry was stored physically, in paper files, the information was destroyed. According to the UN this could have been avoided by using blockchain based land registry where the information about ownership cannot be tampered with, the authenticity of the information can not be questioned, nor the information could have vanished in the first place.[39] Based on this example the UN has decided to create a land registry which is based on blockchain technology to Panchkula, located in India. The thought process behind the idea is to prevent such incidents that happened in Haiti.[40]

European Union has created Blockchain Observatory and Forum (EUBOF) to scrutinise the possibilities of blockchain technology. The report about Blockchain for government and public services that was released in December 2018 describes the possible use cases for blockchain in the European Union.[41] The report proposes a solution for blockchain based digital identities for EU

[35] Cointelegraph (2019), Nevada Issues Almost 1,000 Marriage Certificates on Ethereum, But Gov't Acceptance Varies, Accessible: https://cointelegraph.com/news/nevada-issues-almost-1-000-marriage-certificates-on-ethereum-but-govt-acceptance-varies 13 March 2019.
[36] Ibid.
[37] United Nations Development Programme (2018), Using blockchain to make land registry more reliable in India, Accessible: https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html 1 March 2019.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] European Union Blockchain Observatory & Forum (2018), Blockchain for government and public services, Accessible:https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf 10 March 2019, p 1-33.

citizens. The argument behind the idea is that "internet- has no built-in identity mechanism".[42] Nowadays banks and other trusted parties provide people a way to identify themselves on the internet and according to the report identifying has become increasingly important during the era of the internet.[43]

Food ministry of South Korea has expressed its interest in launching a pilot program to better trace origin of its citizen's consumed beef. The information of a delivery chain is supposed to be registered to a blockchain based database which makes it easier to trace the origin and supply chain.[44] Swiss food manufacturer Gustav Gerig AG has expressed similar plans for certifying tuna and its place of origin. Blockchain technology is supposed to improve transparency in the food market and in the delivery chain.[45] Blockchain technology has been considered as a new way to certify products, especially for companies with higher moral and ethical standards.[46]

Lastly, Internet Court in Hangzhou, China has reported its plans to use blockchain technology to fight against piracy. According to the article, Hangzhou is a domicile for many of the online bloggers or writers in China who suffer from the lack of ways to prove that they have written their work. By adding their work to the blockchain based data storage system they can enhance their possibilities to provide evidence for the court about their intellectual property rights.[47] The decision conforms the ruling of China's Supreme Court which has given a judgement that evidence can be authenticated with blockchain technology and it has binding effect.[48]

[42] Ibid., p 20.
[43] Ibid., p 20.
[44]Cointelegraph (2019), South Korea Science, Food Ministries to Use Blockchain for Tracing Beef Supply Chain, Accessible: https://cointelegraph.com/news/south-korea-science-food-ministries-to-use-blockchain-for-tracing-beef-supply-chain 7 March 2019.
[45]Cointelegraph (2019), Swiss Food Manufacturer Partners with ETH-based Blockchain Service to track Tuna Products, Accessible: https://cointelegraph.com/news/swiss-food-manufacturer-partners-with-eth-based-blockchain-service-to-track-tuna-products 10 March 2019.
[46] Fowler, M. D. (2018). Linking the public benefit to the corporation: Blockchain as solution for certification in an age of do-good business. *Vanderbilt Journal of Entertainment Technology Law* 20(3), p 913.
[47] Cointelegraph (2019), Chinese Internet Court Uses Blockchain to Protect Online Writer's Intellectual Property, Accessible: https://cointelegraph.com/news/chinese-internet-court-uses-blockchain-to-protect-online-writers-intellectual-property 6 March 2019.
[48] Cointelegraph (2019), China's Supreme Court Rules That Blockchain Can Legally Authenticate Evidence, Accessible: https://cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence 10 March 2019.

1.2.4. Store of value

One of the concerns in the traditional economy is inflation. Due to the mostly political or economic reasons, the Federal Reserve may decide to increase the money supply. After the increase of a money supply, each dollar is less valuable than before. This artificial inflation is expected to improve economy but in reality it can have far-reaching results because the natural economy is distorted.[49]. Bitcoin network is programmed in a way that maximum of 21 million coins can ever exist. However, not all the coins are yet created.[50] A process called mining creates bitcoins and it is argued to balance the supply and demand. This algorithm controlled steady increase would, in theory, improve bitcoin's inflation resistance as far as the popularity of bitcoin continues to increase.[51] Additionally, bitcoin is described to be a technological replacement for gold.[52] This characterisation could have been invented due to the nature and scarcity of bitcoins.

1.3. Dangers of blockchain technology

The blockchain is described to be the next big innovation among the Internet of Things (IoT) and Artificial Intelligence (AI) after the invention of the internet that revolutionises the world.[53] Although the technology has proven its functioning there are still uncovered aspects of the security of blockchain technology which concern the future of blockchain networks. In order to create proper understanding about the dangers of blockchain, there are two perspectives that need to be scrutinised.

Firstly, from the technological point of view, there have been concerns about situations, mainly on the smaller and weaker decentralised blockchain networks, where a group of miners could acquire the majority of the computational power of the network. This attack has been named to so-called '51% attack'. The attack is based on the idea that hacker or hackers take over the control of the network by owning more than 50% of the network's computational power. This, in theory, would

[49] Papp, J. (2014). A medium of exchange for an internet age: How to regulate bitcoin for the growth of e-commerce. *Pittsburgh Journal of Technology Law and Policy* 15(1), p 42.
[50] Cook, R. (2014). Bitcoins: Technological innovation or emerging threat. *John Marshall Journal of Information Technology and Privacy Law* 30(3), p 539.
[51] Papp, J. (2014). A medium of exchange for an internet age: How to regulate bitcoin for the growth of e-commerce. *Pittsburgh Journal of Technology Law and Policy* 15(1), p 42.
[52] Allen, H. J. (2017). $=euro=bitcoin. *Maryland Law Review* 76(4), p 904.
[53] Forbes (2018), Merging Internet Of Things And Blockchain In Preparation For The Future, Accessible: https://www.forbes.com/sites/darrynpollock/2018/12/13/merging-internet-of-things-and-blockchain-in-preparation-for-the-future/#3f29861c41fc 10 March 2019.

allow the hacker or hackers to create so-called double spends. This would not be possible in centralised networks where the single authority possesses the computational power of the network. Also the use of a 51% attack for bigger decentralised networks such as bitcoin is extremely expensive and therefore highly unlikely to occur.[54] In addition, when programming complicated networks such as blockchains a chance for human error is always present in programming which may lead to serious consequences.[55]

Furthermore, the experts of the field have continuously warned about the energy consumption of decentralised blockchains such as bitcoin. Blockchain network requires computational power from computers that are validating transactions and keeping up the network. These processes that solve complicated mathematical problems consume significant amounts of electricity. Some people have estimated that keeping up the bitcoin network requires as much energy as a city with a population of 150,000 or depending on the number of transactions, all the way up to a country with a population of 10 million.[56] It is however notable that due to technological development and rise of the renewable energy, the world has an enormous potential of replacing traditional, environmental hazardous forms of energy. For example, in just 90 minutes our planet receives the same amount of energy from the sun that is equivalent to the whole world's annual energy consumption.[57] In addition, there are many other sources of renewable energy.[58] Therefore it is reasonable to assume that energy consumption of blockchain networks may not be a significant problem in the future.

Lastly, due to technological development, quantum computing can raise concerns for the blockchain networks.[59] Quantum computing is able to solve even the hardest computational problems in reasonable time and the technology is well recognised among people from the field of technology.[60] The ability of classical computation in problem solving is not comparable with quantum computing.[61] Use of quantum computing would therefore allow hackers to allocate unforeseen computational power towards private keys of the blockchain network in order to solve the passwords of peoples' wallets. In theory, it would also be a lot easier to gain control of the

[54] Investopedia (2019), 51% Attack, Accessible: https://www.investopedia.com/terms/1/51-attack.asp 5 March 2019.
[55] Rimbelow, C. (1981). Liability for programming errors. *International Business Lawyer* 9(7 and 8), p 303-306.
[56] Gabison, G. (2016). Policy considerations for the blockchain technology public and private applications. *SMU Science and Technology Law Review* 19(3), p 342.
[57] Harari, Y. N., Purcell, J., & Watzman, H. (2015). *Sapiens: Ihmisen lyhyt historia*. p 377.
[58] Ibid., p 377-378.
[59] Choi, J. (2018). Quantum computation and its influence on cybersecurity. *Charleston Law Review* 12(3), p 393.
[60] Ibid., p 393-394.
[61] Ibid., p 393-394.

majority of the network's computational power and create a 51% attack.[62] The threats mentioned in this chapter are hypothetical but necessary to acknowledge in the 21st century.

The above-mentioned examples considered technological threats of blockchain technology. During the recent years, one the biggest applications of blockchain technology that has raised attention is bitcoin.[63] This is however only one application of blockchain technology. The European Commission is scrutinising existing laws and whether they include obstacles for the development of new technologies.[64] This has also been a topic for regulators around the world since there is no clear and comprehensive legislation about how to for example regulate bitcoin and its users.[65] Thus, one of the dangers of blockchain technology could be the legislation and blockchain applications' legal status.

According to some authors there is clearly a need for blockchain regulation and the regulations should aim to balance the rights of users and relevant risks by taking in to account the benefits of the specific applications.[66] It is argued that the legislation ought to solve the legal uncertainty that exists around the blockchain technology. In addition, legislation should include clarification of current legal statutes and their relation to specific applications such as bitcoin network, the possibilities of the authorities to oversee the compliance and creation of comprehensive legislation that enables users to legally and securely use the applictions.[67]

In the EU general understanding among the legislators is that bitcoin is legal.[68] Although there are no proper regulations concerning blockchain technology EU has made research about blockchain applications[69] It should be noted that different countries in the EU treat these applications in different ways.[70] European Union report about 'blockchain for government and public services' is

[62] Nature (2018), Quantum computers put blockchain security at risk, Accessible: https://www.nature.com/articles/d41586-018-07449-z 15 March 2019.
[63] Tu, K. V.; Meredith, M. W. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review* 90(1), p 273.
[64] EU Blockchain Observatory and Forum (2018), BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf 10 March 2019.
[65] Ibid., 274.
[66] Shcherbak, S. (2014). How should bitcoin be regulated. *European Journal of Legal Studies* 7(1), p 43.
[67] Ibid., p 82-83.
[68] Ibid., p 43.
[69] Ibid., p 43.
[70] Ibid., p 44.

one of the comprehensive analysis about blockchain technology in the European Union. According to the report the EU and its Member States should "set up the right infrastructure to make sure it is easy and fast for government agencies and institutions to build their own applications in a cost-effective and interoperable manner".[71] This kind of infrastructure would require certain kind of legal certainty and legislation. In the report 'virtual currency schemes' by European Central Bank (ECB) it is stated that cryptocurrencies "do indeed fall within central banks' responsibility as a result of characteristics shared with payment systems, which give rise to the need for at least examination of developments and the provision of an initial assessment."[72] Therefore when assessing the dangers of blockchain technology it is necessary to consider the legislative aspect as well. Some argue that blockchain technology, especially in a decentralised form, will be limited and complicated in several ways by the legislators.[73]

[71] EU Blockchain Observatory and Forum (2018), BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf 10 March 2019, p 6.
[72] European Central Bank (ECB), (2012) Virtual currency schemes, Accessible: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf 15 March 2019 p 47.
[73] Gudkov, A. (2018). Control over Blockchain Network. *Nova Law Review, 42*(3), p 356.

2. EUROPEAN UNION LEGISLATION

2.1. General Data Protection Regulation

As previously discussed, there are several legal concerns about blockchain technology and the EU has merely started serious considerations about the implications of emerging technologies. Discussions have consisted of cryptocurrency regulation and regulating blockchain technology in general. However, there are raising concerns about the individuals' privacy when utilising blockchain technology.[74] European Union General Data Protection Regulation entered into force in 2018. Commission of the Union assumes this new privacy regulation to be technologically neutral and according to the Commission, "the Regulation enables innovation to continue to thrive under the new rules".[75] In order to scrutinise the regulatory position of blockchain technology concerning privacy in the EU, including its previously mentioned use cases and features, it is necessary to understand what GDPR in fact is.

European Union General Data Protection Regulation came in to force 25th May 2018 and it is described as one of the greatest developments on EU's cyberspace and data protection field.[76] The regulation replaces the previous Directive 95/46/EC.[77] GDPR regulates individuals and their data. In addition, the regulation will affect to a public and private entities and businesses.[78] GDPR is expected to increase legal certainty as there are 28 different countries with divergent legal systems that are brought together under one regulation.[79] This is certainly soothing for the companies that have to operate in the EU and can more easily comply with the legislation. The effect for the companies, but also for private citizens in the EU is brightening.[80]

[74] Berberich, M.; Steiner, M. (2016). Blockchain technology and the gdpr how to reconcile privacy and distributed ledgers. *European Data Protection Law Review (EDPL)* 2(3), p 422.
[75] European Commission (2017), Questions and answers – Data protection reform package, Accessible: http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf 5 March 2019.
[76] Ganotra, S. (2018). Gdpr compliant or not. *Court Uncourt* 5(6), p 2.
[77] 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).
[78] Ganotra, S. (2018). Gdpr compliant or not. *Court Uncourt* 5(6), p 2.
[79] Albrecht, J. (2016). How the gdpr will change the world. *European Data Protection Law Review (EDPL)* 2(3), p 288.
[80] Ibid., p 288.

Around 250 million people in the EU use the internet everyday and they are sharing private information on different websites. The GDPR aims to improve peoples' privacy and their rights concerning their data.[81] EU citizens have the right to acquire clear information on who is processing their data, for what purpose is the data processed for and why it is processed.[82] Citizens can also request all the information organisations have about them. When companies need individual's consent for processing their data, they need to ask for approval and clearly explain how they will use that data.[83] Individual's consent has to be clearly given. In case of a data breach, where information is stolen or lost, the companies are obliged to report the incident immediately.[84]

Therefore from citizen's point of view, it's easy to assume that GDPR is good and welcomed reformation. However, from the perspective of technological development, there are details that may seem disturbing. Firstly, how much the lawmakers took into account new technologies when creating the legislation and what are the principles lawmakers should take into consideration according to EU policies? According to the Treaty of the Functioning of the European Union (TFEU) Article 173 "the Union and the Member States shall ensure that the conditions necessary for the competitiveness of the Union's industry exist".[85] This can be seen as a clear sign that EU understands the importance of supportive legislation of the industry and economics. Articles between 179 and 190 specify the importance of technological development and research.[86]

According to the considerations of GDPR, "In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used".[87] The principle of technological neutrality arose first time in 2002 when the EU was creating its legislation for electronic communications. It has since been adopted as one of the main principles concerning technology.[88] The idea is, that the principle applies

[81] Euroopan Komissio (2018), EU:n tietosuojauudistus: paremmat tietosuojaoikeudet Euroopan kansalaisille, Accessible: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-citizens_fi.pdf 3 March 2019.
[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01
[86] Ibid., p 128-132.
[87] GDPR (2016), supra nota 1, p 3.
[88] Hogan Lovells Global Media and Communications (2014), Technology neutrality in Internet, telecoms and data protection regulation, Accessible: http://www.hoganlovells.com/files/Uploads/Documents/8%20Technology%20neutrality%20in%20Internet.pdf 10 March 2019 p 19.

"regardless of which kind of existing or potentially new technology is involved".[89] According to the EU report, the principle "is essential to provide the necessary flexibility to deal with emerging technologies and their convergence in fields such as media, internet and mobile communications".[90] One could then conclude, that the principle is widely accepted in the EU and considered relevant.

So far this research has aimed to create a proper understanding of blockchain technology and its recognised benefits. As mentioned, blockchain is essentially a way to store data securely and deleting or altering the data from public blockchains afterwards is practically impossible. EU policy and principles about technological development as well as GDPR have also been introduced in order to understand the bigger picture. The next chapter will introduce Article 17 of GDPR and its possible significance to the development of both public and private blockchain networks.

2.1.1 Article 17

Perhaps one of the most interesting Articles of GDPR is Article 17 that provides right to erasure or in other words, right to be forgotten.[91] Natural persons can request data controllers or processors for their data to be deleted if "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed".[92] The application of the Article 17 has been demonstrated in the case *NT1 & NT2 v Google LLC* where the defendant NT2 requested Google to erase the search information about him being part of minor criminal activities earlier in his life. Google had refused to erase the search results on the ground of journalism exemption. By considering the decision of Court of Justice of the European Union (CJEU) in the case *Google Spain SL & another v Agencia Espanola de Proteccion de Datos (AEPD)* and other factors, the court ruled in favour of NT2 and obliged Google to erase the search results.[93] Above mentioned cases indicate in practice that private citizens of the EU have the right to ask their information to be deleted from the internet in case it is no longer relevant or necessary to store it. From the technological point of view obeying the court order was effortless for Google. However, if the information would have been stored on blockchain, deleting it would be considerably more

[89] European Commission (2006) The European Electronic Communications Regulation and Markets 11th Report – Frequently Asked Questions, Accessible: http://europa.eu/rapid/press-release_MEMO-06-84_en.pdf 22 April 2019 p 2.
[90] Ibid. p 2.
[91] GDPR (2016), supra nota 2, Article 17.
[92] GDPR (2016), supra nota 3, Article 17 1(a).
[93] EWHC 799, NT1 & NT2 v Google LLC [2018].

challenging.[94] As Google should be able to control its database it would utilise private centralised blockchain and own the computational power of the network. Thus, Google could in theory override its information or hide it from the public. However around 80% of the current blockchains are public.[95]

In principle, there are two considerations about personal data in public blockchains. According to the CJEU's decision in the case *Patrick Breyer v Germany* IP addresses can be considered as personal data even if they are dynamic.[96] The situation is much like with blockchain and public keys. Under the EU legislation public keys which are visible to everyone are concluded to be personal data.[97] Secondly, the transaction history of a blockchain can be considered as personal data.[98] In conclusion it can be said that Article 17 applies to blockchain technology at least in these two ways but is it possible to apply this Article to blockchain networks in practice?

As discussed in the beginning of the research, decentralised public blockchain networks do not have central authority and no certain person or entity controls them. If we take an example from bitcoin network where also EU citizens make transactions every day, they should be able to request their public keys to be erased from the blockchain. If there is no central authority controlling the network, who should be responsible for executing this request?

Another example was conducted by group of software engineers, who created a hypothetical example about a company working in the EU utilising private blockchain to store its data in a project.[99] The team was planning a way to automatically calculate the capacity of a commuter railroad and planned to use blockchain to store the data. The project aimed to estimate the delays in the railroad traffic especially when functioning with a high capacity. In addition, the train's influence on other trains on the same line was scrutinised. The team received data from multiple sources including sensors from rails and in the passenger space, ticketing system and from the process analysing the amount of people in the train. Everything seemed to be under control until ticket information was added to the blockchain. Ticket information is connected to privacy issues

[94] EU Blockchain Observatory and Forum (2018), BLOCKCHAIN AND THE GDPR, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf 5 March 2019. p 25.
[95] Ibid. p 16.
[96] C-582/17, *Patrick Breyer v Bundesrepublik Deutschland* [2016].
[97] Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), p 25.
[98] Ibid., p 24.
[99] eWEEK (2018), Software Engineers Discovering How GDPR Limits Use of Blockchain, Accessible: https://www.eweek.com/enterprise-apps/software-engineers-discovering-how-gdpr-limits-use-of-blockchain 7 March 2019.

since it contains sensitive information from the passengers such as credit card details. Since the system included personal details about the passengers it fell under the scope of GDPR. According to the experiment, the challenge arose since the information had to be stored in to a blockchain database which could not be altered afterwards and would therefore violate Article 17 right to be forgotten of the GDPR. The project was never put in to operation because of the privacy issues it faced but it illustrated the complexity of complying with the GDPR when utilising blockchain technology.[100]

In conclusion, Article 17 of the GDPR complicates the legal adoption of the blockchain technology and increases the cost of implementation and use of the blockchain technology in the EU. It seems to be possible to comply with the GDPR while utilising private blockchains.[101] What about the situation concerning transaction history in public decentralised blockchains that are not under the control of any particular group of people? The most famous example bitcoin stores all the transactions of its users to a public blockchain where everyone can scrutinise the transaction history.[102] The data in public blockchain is pseudoanonymous which means that it is identifiable with additional information.[103] There seems to be countless number of examples that demonstrate the difficulties when applying GDPR to blockchain technology. Could there be a situation where EU can not enforce its legislation and no one can be held responsible? How should the situation be interpreted?

2.2. Interpretation

In the previous chapters the research has aimed to scrutinise different perspectives to the issue between blockchain technology and EU principles, policies and legislation. By taking into account the precedents about personal data, it is clear that blockchain technology falls under the scope of GDPR. This chapter aims to understand different view points to the current situation. It should be noted that the situation is challenging especially for lawyers, who should be able to understand the

[100] Ibid.
[101] EU Blockchain Observatory and Forum (2018), BLOCKCHAIN AND THE GDPR, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf 5 March 2019 p 16.
[102] Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), p 19-20.
[103] Ibid., p 24.

bigger picture and identify "the legal, policy and strategic implications of blockchain technology".[104]

European Union has always been a supporter of new technologies and it considers itself as a pioneer in developing new technologies and deploying it.[105] In addition, EU has created principle about technological neutrality, that promotes new technologies to be taken into account when creating new legislation.[106] European Union invests billions of euros annually to support and develop new technologies.[107] The EU has for example created European Observatory for Blockchain technologies and funded several researches about the technology. In addition, several facets in the EU have recognised the benefits of blockchain technology.[108] From this perspective the stance of the Union towards blockchain technology ought to be positive. However, one of the most important basic rights in the EU, especially during the 21st century is individual's right to privacy which is established in the EU Charter of Fundamental Rights.[109] If the blockchain technology turns out to be as disruptive as it is described to be and it reforms along with the Internet of Things and AI, almost all the sectors including financial and political sectors,[110] EU should carefully scrutinise its objectives when balancing between the new technologies such as blockchain and individual's right to privacy.[111] However some argue that from the perspective of principle of technological neutrality blockchain does "not impair the ability of data messages to meet legal requirements".[112] This can be understood in a way that the technology is developing all the time and we may not have the same privacy issues with the blockchain technology in the future.

---

[104] Finck, M. (2018). Blockchains: Regulating the unknown. *German Law Journal* 19(4), p 666.
[105] European Parliament (2019), Fact Sheet Policy For Research And Technological Development, Accessible: http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.5.pdf 22 April 2019.
[106] Hogan Lovells Global Media and Communications (2014), Technology neutrality in Internet, telecoms and data protection regulation, Accessible: http://www.hoganlovells.com/files/Uploads/Documents/8%20Technology%20neutrality%20in%20Internet.pdf 10 March 2019.
[107] European Parliament (2019), Fact Sheet Policy For Research And Technological Development, Accessible: http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.5.pdf 22 April 2019.
[108] European Commission (2019) Policy on Blockchain Technologies, Accessible: https://ec.europa.eu/digital-single-market/en/blockchain-technologies 22 April 2019.
[109] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02
[110] Forbes (2018), Merging Internet Of Things And Blockchain In Preparation For The Future, Accessible: https://www.forbes.com/sites/darrynpollock/2018/12/13/merging-internet-of-things-and-blockchain-in-preparation-for-the-future/#3f29861c41fc 10 March 2019.
[111] EU Blockchain Observatory and Forum (2018), BLOCKCHAIN AND THE GDPR, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf 5 March 2019.
[112] de las Heras Ballell, T. (2018). Digital technology-based solutions for enhanced effectiveness of secured transactions law: The road to perfection. *Law and Contemporary Problems* 81(1), p 36.

One interesting perspective concerning the legal responsibility is that if the direction will head towards the adoption of blockchain technology and more specifically decentralised blockchains, who should then be kept responsible for the network? The GDPR specifies in Article 4 the meaning of data 'controller' as "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."[113] In addition the GDPR defines data 'processor' as "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[114] In order to apply these definitions to a decentralised blockchain networks it should be determined who can be considered as data processor or controller in blockchain network.

As mentioned previously in the research, decentralised blockchains are run by independent people from different legislations who provide computational power for the network.[115] These computers are called nodes.[116] One theory has been that these nodes who are responsible for keeping up the network would qualify as data controllers or processors[117] since each node has a copy of the transaction history of the network.[118] In practice this makes them all data processors since they they are updating the copy as they validate new transactions. [119] When considering the definitions of a processor or controller it is interesting to realise that GDPR uses singular form which could be related to an assumption that normally there is only one data processor or controller in a centralised database.[120] Data controllers could probably be identified in private blockchains but for public blockchains it becomes impossible to determine only one data controller.[121] In such situation, either all the nodes qualify as data controllers or none of them would. It is important to notice that nodes can not independently determine the rules or means for processing.[122]

[113] GDPR (2016), supra nota 4, Article 4 (7).
[114] GDPR (2016), supra nota 5, Article 4 (8).
[115] Shcherbak, S. (2014). How should bitcoin be regulated. *European Journal of Legal Studies* 7(1), p 41-83.
[116] Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), p 19-20.
[117] Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), p 26.
[118] Botos, H. (2017). blockchain intelligence analysis. *Research and Science Today* 13(Supplement 1), p 43-44.
[119] Ibid., p 43-44.
[120] Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), p 26.
[121] Ibid. p 26-27.
[122] Ibid. p 26.

GDPR Article 26(1) defines 'jointly controllers' which in group "jointly determine the purposes and means of processing".[123] However the understanding is that nodes cannot be jointly responsible of processing since they have not determined necessary requirements and aims for processing.[124] When considering the situation where each node would be determined as data controller it raises several concerns.[125] GDPR sets down requirements for data controller to qualify as such however, nodes do not fulfil the criteria.[126] Nodes for example can not see the information they are processing since it is hashed. In addition they can not makes changes to it.[127] Therefore it would not be accurate to call nodes as data processors. It would also be unrealistic to assume that they could afford to pay the fines that GDPR sets out.[128] This would make the enforcement of GDPR even more difficult. It is also important to consider the fact that people who hold private keys and add information about themselves to a blockchain could in some cases be considered both as data controller and processor.[129] These examples demonstrate the difficulties of determining the 'data processor', 'controller' and ultimately the people responsible for public blockchains.

As demonstrated in sub-section Article 17 of this research, CJEU has taken a strict stance on people's privacy in its decisions. By considering the EU's stance on privacy the direction will continue to be the same. The chapter also gave examples about application of Article 17 to blockchain technology and analysed the difficulties which arosed. Article 17 of GDPR clearly prevents the application of blockchain technology. Whether this is a good thing depends on the perspective. In addition, if the GDPR will indeed be applied to blockchains, the advancement of the technology will probably be significantly higher outside the EU and may lead to remarkable economic consequences for EU Member States.

Article 17 which sets the right to erasure or right to be forgotten can be enforced in some cases considering blockchain technology, especially in private blockchains. However enforcing the Article 17 on public blockchains becomes merely impossible. Therefore it is necessary to consider the possible, partial exemptions of blockchain technology from GDPR or some sections about it.

[123] GDPR (2016), supra nota 6, Article 26 (1).
[124] Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), p 26.
[125] Ibid., p 26.
[126] Ibid., p 26.
[127] Ibid., p 26.
[128] Ibid., p 27.
[129] Ibid., p 27.

Otherwise the direction may lead to a situation where EU legislation cannot be enforced. Some have argued that GDPR was created to a world where data is centrally controlled and does not take into account decentralised forms of processing or storing data.[130]

[130] Ibid., p 17.

CONCLUSION

The research paper concentrated on creating a proper understanding about what is blockchain technology, what are its applications, dangers and legislative position. The research paper aimed to analyse the effects of EU legislation and more specifically GDPR Article 17 on blockchain technology. The research discovered that it is important to make a distinction between public and private blockchains when determining the effects of the GDPR Article 17. Considering private blockchains the research discovered that Article 17 of GDPR, at its current state, makes it significantly harder for companies to adopt blockchain technology in to their businesses. It is important to highlight that GDPR Article 17 does not make it impossible for private blockchains to be GDPR compliant however the cost and practicality of the adoption may become an obstacle for companies.

Unlike private blockchains, public blockchains are created in a way that there is no central authority that would control the network nor held responsible for the functioning of the network. Independently acting and participating nodes of the network do not know each other and are located around the world. The study finds that in theory it is almost impossible for decentralised public blockchains to be compliant with GDPR Article 17 since the information cannot be deleted from the chain without the full consensus of the network participants. In practice the compliance is impossible.

Blockchain technology is developing and people around the world are working on the field. The blockchain technology has already proven its applicability, but there are also several dangers for the development and adoption. The research finds that the dangers should be categorised as technological and legislative. Technological threats for the technology include human errors in programming, quantum computing and 51% attacks to gain control of the network. Legislative threats for the development of blockchain technology include ignorance of the decision makers and legislation that would prevent the technology from developing. However, the attitude towards blockchain technology has been mostly positive in the EU and the regulators seem to have the strategy of waiting for the technology to develop before taking stance on the application of the

current legislation. The decision is strategically wise since regulating the technology without understanding it could prevent the important technological development in the EU.

When considering the future of the blockchain technology it is necessary to acknowledge three perspectives. Firstly, in order to guarantee the safety of the European Union and its proper functioning, sooner or later the regulations must be enforced. This would basically mean that blockchain technology would not be misused and the regulations would give the EU possibility to monitor the situation and eradicate the misuse. Secondly, it is fundamentally important to consider the citizen's point of view. On the 21st century privacy has increasingly important significance in the Union and securing the privacy of the citizens is essential. The privacy of the citizens' should be considered in all EU decisions. Thirdly, it is required to understand the technological point of view. As the technological development is accelerating and becoming increasingly important it is necessary to create a legislation that allows this sector to thrive. This may include compromises between these three perspectives but if the EU desires to be one of the leading inventors of new technology these considerations are necessary.

In order to accomplish above mentioned considerations and goals the EU should persuade talented people on the field to make research in the EU. It is necessary to maintain cooperation between legislators and the experts of the industry. In addition, the education from the field is fundamental for the development of blockchain technology. Currently there is no specific blockchain legislation on the EU level. The technology has proven its applicability but it is necessary to keep in mind that technology is created by people and someone is always misusing the possibilities and thus the regulation is required to provide legal certainty and framework to control the behaviour. As it is demonstrated in this research, there are unforeseen effects of the current legislation that have an impact on blockchain technology even this may not have been considered to occur when creating the legislation. Before further developing the legislation, it is necessary to scrutinise the effects of EU legislation on blockchain technology in order to prevent unintended consequences. As we know, the world is taking an example of the EU in many cases also when it comes to GDPR and by considering this, EU's stance on blockchain technology is becoming increasingly important.

LIST OF REFERENCES

Scientific books:

1. Harari, Y. N., Harari, Y. N., Purcell, J., & Watzman, H. (2015). *Sapiens: Ihmisen lyhyt historia. p. 377-378.*

Scientific articles:

2. Adimi, G. (2018). How the new generation cryptocurrencies decoded the investment contract code: Analysis of us and eu laws. *Bocconi Legal Papers* 10(1), 313-346.

3. Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review (EDPL), 2*(3), p 287-289.

4. Allen, H. J. (2017). $=euro=bitcoin. *Maryland Law Review* 76(4), 877-939.

5. Belcher, S. (2017). Tracing the invisible: Section 11's tracing requirement and blockchain. *Colorado Technology Law Journal* 16(1), 145-174.

6. Berberich, M.; Steiner, M. (2016). Blockchain technology and the gdpr how to reconcile privacy and distributed ledgers. *European Data Protection Law Review (EDPL)* 2(3), 422-426.

7. Botos, H. (2017). blockchain intelligence analysis. *Research and Science Today* 13(Supplement 1), p 43-44.

8. Choi, J. (2018). Quantum computation and its influence on cybersecurity. *Charleston Law Review* 12(3), 393-398.

9. Cook, R. (2014). Bitcoins: Technological innovation or emerging threat. *John Marshall Journal of Information Technology and Privacy Law* 30(3), p. 539.

10. de las Heras Ballell, T. (2018). Digital technology-based solutions for enhanced effectiveness of secured transactions law: The road to perfection. *Law and Contemporary Problems* 81(1), 21-44.

11. Essaghoolian, N. (2019). Initial coin offerings: Emerging technology's fundraising innovation. *UCLA Law Review* 66(1), 294-344.

12. Fenwick, M.; Kaal, W. A.; Vermeulen, E. P. (2017). Legal education in the blockchain revolution. *Vanderbilt Journal of Entertainment Technology Law* 20(2), 351-384.

13. Finck, M. (2018). Blockchains and data protection in the european union. *European Data Protection Law Review (EDPL)* 4(1), 17-35.

14. Finck, M. (2018). Blockchains: Regulating the unknown. *German Law Journal* 19(4), 665-692.

15. Fowler, M. D. (2018). Linking the public benefit to the corporation: Blockchain as solution for certification in an age of do-good business. *Vanderbilt Journal of Entertainment Technology Law* 20(3), 881-918.

16. Gabison, G. (2016). Policy considerations for the blockchain technology public and private applications. *SMU Science and Technology Law Review* 19(3), 327-350.

17. Ganotra, S. (2018). GDPR Compliant or Not. *Court Uncourt, 5*(6), 2-4.

18. Gudkov, A. (2018). Control over Blockchain Network. *Nova Law Review, 42*(3), 353-374.

19. Iskander, M. (2017). Blockchain: The future of all data. *Intellectual Property and Technology Law Journal* 22(1), 1-18.

20. Jones, S. (2018). Data breaches, bitcoin, and blockchain technology: modern approach to the data-security crisis. *Texas Tech Law Review* 50(4), 783-814.

21. Papp, J. (2014). medium of exchange for an internet age: How to regulate bitcoin for the growth of e-commerce. *Pittsburgh Journal of Technology Law and Policy* 15(1), 33-[i].

22. Piazza, F. S. (2017). Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses. *Penn State Journal of Law and International Affairs* 5(2), 262-301.

23. Reyes, C. L. (2016). Moving beyond bitcoin to an endogenous theory of decentralized ledger technology regulation: An initial proposal. *Villanova Law Review* 61(1), 191-234.

24. Rimbelow, C. (1981). Liability for programming errors. *International Business Lawyer* 9(7 and 8), p 303-306.

25. Ross, E. (2017). Nobody puts blockchain in corner: The disruptive role of blockchain technology in the financial services industry and current regulatory issues. *Catholic University Journal of Law and Technology* 25(2), 353-386.

26. Savu, I.; Carutasu, G.; Popa, C.; Cotet, C. (2017). Quality assurance framework for new property development: decentralized blockchain solution for the smart cities of the future. *Research and Science Today* 13(Supplement 2), 197-203.

27. Shcherbak, S. (2014). How should bitcoin be regulated. *European Journal of Legal Studies* 7(1), 41-83.

28. Sonderegger, D. (2015). Regulatory and Economic Perplexity: Bitcoin Needs Just Bit of Regulation. *Washington University Journal of Law Policy* 47, 175-216.

29. Tu, K. V.; Meredith, M. W. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review* 90(1), 271-348.

30. Walch, A. (2017). The path of the blockchain lexicon (and the law). *Review of Banking and Financial Law* 36(2), 713-766.

31. Young, S. (2018). Changing governance models by applying blockchain computing. *Catholic University Journal of Law and Technology* 26(2), 1-33.

EU and International legislation

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

33. European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01

34. 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)

Court decisions

35. CJEU, Case C-582/17, *Patrick Breyer v Bundesrepublik Deutschland* [2016]
36. EWHC, Case 799 (QB), *NT1 & NT2 v Google LLC* [2018]

Other sources

37. BBC (2019), JP Morgan creates first US bank-backed crypto-currency, Accessible: https://www.bbc.com/news/business-47240760 7 March 2019.

38. CNBC (2018), Tokenization: The world of ICOs, Accessible: https://www.cnbc.com/2018/07/13/initial-coin-offering-ico-what-are-they-how-do-they-work.html 10 March 2019.

39. Cointelegraph (2018), Blockchain's scaling problem, Explained, Accessible: https://cointelegraph.com/explained/blockchains-scaling-problem-explained 13 March 2019.

40. Cointelegraph (2019), Swiss Food Manufacturer Partners with ETH-based Blockchain Service to track Tuna Products, Accessible: https://cointelegraph.com/news/swiss-food-manufacturer-partners-with-eth-based-blockchain-service-to-track-tuna-products 10 March 2019.

41. Cointelegraph (2019), South Korea Science, Food Ministries to Use Blockchain for Tracing Beef Supply Chain, Accessible: https://cointelegraph.com/news/south-korea-science-food-ministries-to-use-blockchain-for-tracing-beef-supply-chain 7 March 2019.

42. Cointelegraph (2019), Chinese Internet Court Uses Blockchain to Protect Online Writer's Intellectual Property, Accessible: https://cointelegraph.com/news/chinese-internet-court-uses-blockchain-to-protect-online-writers-intellectual-property 6 March 2019.

43. Cointelegraph (2019), China's Supreme Court Rules That Blockchain Can Legally Authenticate Evidence, Accessible: https://cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence 10 March 2019.

44. Cointelegraph (2019), Ukraine Completes Pilot Scheme for E-Hryvnia National Digital Currency, Accessible: https://cointelegraph.com/news/ukraine-completes-pilot-scheme-for-e-hryvnia-national-digital-currency 14 March 2019.

45. Cointelegraph (2019), Nevada Issues Almost 1,000 Marriage Certificates on Ethereum, But Gov't Acceptance Varies, Accessible: https://cointelegraph.com/news/nevada-issues-almost-1-000-marriage-certificates-on-ethereum-but-govt-acceptance-varies 13 March 2019.

46. Euroopan Komissio (2018), EU:n tietosuojauudistus: paremmat tietosuojaoikeudet Euroopan kansalaisille, Accessible: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-citizens_fi.pdf 3 March 2019.

47. European Banking Authority (2019), Report on crypto-assets, Accessible: https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf 10 March 2019.

48. European Central Bank (2012), Virtual currency schemes, Accessible: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf 15 March 2019.

49. European Commission (2019) Policy on Blockchain Technologies, Accessible: https://ec.europa.eu/digital-single-market/en/blockchain-technologies 22 April 2019.

50. European Commission (2017), Questions and answers – Data protection reform package, Accessible: http://europa.eu/rapid/press-release_MEMO-17-1441_en.pdf 5 March 2019.

51. European Commission (2006), The European Electronic Communications Regulation and Markets 11th Report – Frequently Asked Questions, Accessible: http://europa.eu/rapid/press-release_MEMO-06-84_en.pdf 22 April 2019.

52. European Parliament (2019), Fact Sheet Policy For Research And Technological Development, Accessible: http://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.5.pdf 22 April 2019.

53. European Union Blockchain Observatory and Forum (2018), BLOCKCHAIN AND THE GDPR, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf 5 March 2019.

54. European Union Blockchain Observatory and Forum (2018), BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES, Accessible: https://www.eublockchainforum.eu/sites/default/files/reports/eu_observatory_blockchain_in_government_services_v1_2018-12-07.pdf 10 March 2019.

55. eWEEK (2018), Software Engineers Discovering How GDPR Limits Use of Blockchain, Accessible: https://www.eweek.com/enterprise-apps/software-engineers-discovering-how-gdpr-limits-use-of-blockchain 7 March 2019.

56. Forbes (2018), Merging Internet Of Things And Blockchain In Preparation For The Future, Accessible: https://www.forbes.com/sites/darrynpollock/2018/12/13/merging-

internet-of-things-and-blockchain-in-preparation-for-the-future/#3f29861c41fc 10 March 2019.

57. Hogan Lovells Global Media and Communications (2014), Technology neutrality in Internet, telecoms and data protection regulation, Accessible: http://www.hoganlovells.com/files/Uploads/Documents/8%20Technology%20neutrality%20in%20Internet.pdf 10 March 2019.

58. Investopedia (2018), Why Governments Are Afraid of Bitcoin, Accessible: https://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp 10 March 2019.

59. Investopedia (2019), 51% Attack, Accessible: https://www.investopedia.com/terms/1/51-attack.asp 5 March 2019.

60. Nature (2018), Quantum computers put blockchain security at risk, Accessible: https://www.nature.com/articles/d41586-018-07449-z 15 March 2019.

61. The Economist (2018), From one cryptocurrency to thousands, Accessible: https://www.economist.com/technology-quarterly/2018/09/01/from-one-cryptocurrency-to-thousands 7 March 2019.

62. United Nations Development Programme (2018), Using blockchain to make land registry more reliable in India, Accessible: https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html 1 March 2019.