DISSERTATIONES
IURIDICAE
UNIVERSITATIS
TARTUENSIS
81

ANNE VEERPALU

Regulatory challenges to the use of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence

TARTU ÜLIKOOL
1632
UNIVERSITAS TARTUENSIS

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
81

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS
81

ANNE VEERPALU

Regulatory challenges to the use of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence

UNIVERSITY OF TARTU
Press

School of Law, University of Tartu, Estonia

The dissertation has been accepted for the commencement of the degree of Doctor of Philosophy (PhD) in law by a resolution of the Council of the School of Law of 12 April 2021.

Supervisors: Assoc. Prof. Dr. Martin Ebers (University of Tartu)
Dr. Anna-Maria Osula (TalTech)
Assoc. Prof. Dr. Alexander Horst Norta (TalTech)

Opponent: Prof. Dr. Florian Möslein, LL.M (Philipps-University Marburg)

The commencement will take place at 11:00 a.m. on 7 June 2021 in Tartu via video bridge.

Publication of this dissertation is supported by the School of Law, University of Tartu

The research leading to this dissertation was conducted with support provided by:

- the IT Law Programme of the University of Tartu in the framework of the European Union Structural Funds programme 'Increasing Digital Literacy';
- the European Regional Development Fund in the framework of action 4.4.2 'Specialised scholarships in higher education in the growth fields of smart specialisation' of the measure 'Increasing the local socio-economic impact of the R&D system and smart specialisation for development of growth areas'; and
- the Dora Plus Programme funded by the European Regional Development Fund.

ISSN 1406-6394
ISBN 978-9949-03-597-7 (print)
ISBN 978-9949-03-598-4 (pdf)

University of Tartu Press
www.tyk.ee

TABLE OF CONTENTS

LIST OF ORIGINAL PUBLICATIONS

The dissertation is based on the following publications:

Article I Anne Veerpalu, 'Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of *De Voogd* and *Hedqvist*' (2018) Baltic Journal of Law & Politics 11/2, pp. 61–94.

Article II Anne Veerpalu, 'Shareholder ledger using distributed ledger technology: the Estonian perspective' (2019) Masaryk University Journal of Law and Technology 13/2, pp. 277–310.

Article III Anne Veerpalu, Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva, Alex Norta, 'The hybrid smart-contract agreement challenge to European electronic signature regulation' (2020) International Journal of Law and Information Technology 28/1, pp. 39–84.

Article IV Anne Veerpalu, 'Functional equivalence – an exploration through shortcomings to solutions' (2019) Baltic Journal of Law & Politics 12/2, pp. 135–163.

Additional articles published on a similar topic by the author:

Article V Anne Veerpalu, 'Computational Law & Blockchain Festival DISCUSS Symposium Reports: Tartu Node' (2018) Stanford Journal of Blockchain Law & Policy 1. (24 June 2018).

Article VI Anne Veerpalu, Eduardo da Cruz Rodrigues e Silva, 'Hitting the white ball: the technology neutrality principle and blockchain based application' (2019) Indian Journal of Law and Technology 15/2, pp. 300–320.

ANALYTICAL COMPENDIUM TO A CUMULATIVE DISSERTATION

This dissertation is about a revolutionary technology called distributed ledger technology (DLT) and the question of whether the current regulatory framework in Estonia and the EU treats it adequately. To this end, the dissertation uses the principle of technology neutrality and its sub-principle of functional equivalence to assess the regulatory framework. The dissertation focuses specifically on the following use cases of DLT:

1. Treatment of bitcoin in comparison with traditional (fiat) currency and the treatment of bitcoin exchange service providers.
2. Treatment of DLT-based shareholder ledger.
3. Treatment of DLT-based hybrid smart contract agreements concluded during Initial Coin Offering (ICO).

The use-case analyses show that DLT replaces some of the typical functions of intermediaries and this feature of it should be taken into consideration in regulation as otherwise the regulation could have a bias against the technology. The dissertation approaches existing regulation relevant in the DLT use cases from the point of view of technology neutrality and functional equivalence in order to identify possible biases and map possible solutions under different regulative strategies.

In its introduction, the following analytical compendium explains what distributed ledger technology is and where it is used; in Chapter 1, the research problem, research questions and the field of investigation is presented along with the methods and resources used. In Chapter 2, the principle of technology neutrality is introduced along with its sub-principles, Chapter 3 discusses alternative regulative strategies for DLT regulation and Chapter 4 applies the principles to the existing regulatory framework specific to the chosen DLT use cases. In the final chapter, conclusions are presented.

I INTRODUCTION

1.1 Pace of technological change

The pace of technological innovation and its adoption by users – especially during the era known as the digital revolution – is accelerating with immense speed,[1] but law-making still remains a lengthy process and the delays in its adaptation can have unpredictable consequences on the use cases of new technology. This phenomenon is known as the Pacing Problem and is often framed as "technology changes exponentially, […] legal systems change incrementally".[2] The Pacing Problem leads the regulation to have gaps and be unfit for innovative solutions.

Along with the Pacing Problem, regulators are also experiencing the Collingridge dilemma,[3] explained as the desire of the regulator to interfere early on with a new technology even though the consequences of its application are still unclear. This desire is motivated by the fear that, by the time these consequences are clear, "the technology is often so much part of the whole economic and social fabric that its control is extremely difficult".[4] However, introducing any new regulation when the technology has not fully developed could prove to be detrimental to the expansion of the technology[5] and create unnecessary hurdles to its use cases.

All of the above must be assessed in the context that, since the 1990s, the digital world has grown exponentially with various software languages, applications and platforms. According to the Commission's previous President, Juncker,[6] the

---

1 According to Larry Downes, the fast pace of technological change can be explained by three "laws" governing digital life: Moore's Law (which means that every 12 to 18 months "the processing power of computers doubles while price holds constant"), Metcalfe's Law ("the usefulness of a network is the square of the number of users connected to it") and the Laws of Disruption, which in general mean that the acceleration of the pace of development of technology and the spread of their outputs is difficult to manage for the regulator. Moore's Law was named after Gordon Moore, the founder of Intel, who in 1965 made this prediction in his article "Cramming More Components onto Integrated Circuits". Larry Downes, *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age* (Basic Books 2009), pp. 12–17. Metcalfe's Law was named after engineer and one of the founding fathers of the Internet Dr Robert Metcalfe, who was in charge of connecting MIT computers to ARPAnet and was later challenged by other scientists. Bob Briscoe, Andrew Odlyzko and Benjamin Tilly, 'Metcalfe's Law is Wrong'. (*IEEE Spectrum,* 01 July 2006) <https://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong> accessed 20 October 2020.

2 Downes (n. 1), p. 17.

3 David Collingridge, *The Social Control of Technology*, (St Martin's Press, New York 1980), p. 11.

4 ibid.

5 ibid.

6 Jean-Claude Juncker was the President of the European Commission from 2014–2019.

Digital Single Market is aimed at creating a "level playing field"[7] for all that is digital, either developed by an incumbent or an innovator. In order to make sure the playing field is level for all technologies and applications, regulators need to learn about and investigate the impact of existing regulation on the new technology to ensure that competition and innovation stand a fair chance against the technology the existing regulation was built for.

1.2 Distributed ledger technology (DLT)

1.2.1 Concepts

The above-described regulatory challenges arise especially with distributed ledger technologies (DLT),[8] which brings about a transformative or disruptive innovation[9] that influences many layers of society – economic, political and social – representing a shift from the current *status quo* to a society disrupted by innovative new constructs infused with new technical possibilities that cross state borders and infrastructural barriers. In other words, DLT is a combination of technologies that allow multiple parties (nodes) unknown to one another (peer-to-peer (P2P) networks[10]) to jointly maintain a resilient digital database (ledger) on the basis of a consensus algorithm. The resilience of the ledger is secured by the replication of the ledger's original copy in the computers of these multiple parties, the hashing process[11] and linked timestamping.[12] The resilience does not allow data recorded on the ledger to be amended or removed unless the change is allowed under the ledger's consensus policy. The combination of technologies bound to DLT aim to achieve transparency, high resilience and tamper-resistance.[13]

---

[7] Commission Communication: A Digital Single Market Strategy for Europe, COM 192 final (6 May 2015). <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final> accessed 20 October 2020.

[8] In the dissertation, for the sake of brevity these are referred to as DLT and used in the singular although they bind together a number of different technologies. No separation between different technologies that make up DLT or different versions of DLT are made by the author in this dissertation.

[9] Julija Kiršienė, Christopher Kelley, Deividas Kiršys, and Juras Žymančius, 'Rethinking the Implications of Transformative Economic Innovations: Mapping Challenges of Private Law', (2018) Baltic Journal of Law & Politics 12/2, p. 50, DOI: <https://doi.org/10.2478/bjlp-2019-0011> accessed 18 March 2020.

[10] Satoshi Nakamoto, 'Bitcoin: Peer-to-peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 12 April 2018.

[11] Hashing is a one-way cryptographic function that turns any text into an illegible string of numbers and letters that is unique and consequently, secures that the hashed text is untampered with. See Article I.

[12] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018), p. 2.

[13] ibid.

Although there are many types of ledger[14] with different characteristics, the primary advantage of most DLT-based ledgers is related to the security and authentication of data that is resistant to modification.[15] Instead of a single administrator, DLT-based ledgers are decentrally controlled by a distributed network of nodes.[16] Data is controlled under the network's governance rules and consensus mechanism. Furthermore, DLT data records are visible to all users and this means that changes in the recorded data are transparent. These features ensure certain functions, such as the possibility to track, trace and gain transparent oversight of all records on the DLT ledger. Consequently, DLT is a fusion of technologies that promote cooperation and trust among strangers without an intermediary such as a central authority or a bank.

1.2.2 Bitcoin and blockchain

DLT is often known by its most popular example, blockchain, which emerged in 2008 when an author named Satoshi Nakamoto published a white paper about an electronic cash system they called Bitcoin.[17] The idea of the new electronic cash system (with bitcoin as a unit) is based on an algorithm that creates a network of trust between strangers (nodes) and is operated without intermediaries in a transparent and secure way.

Blockchain – the core technology of Bitcoin system – is a specific type of ledger among other DLTs that collects transaction data into blocks that, as the name says, are recorded in a chain (a chronological list of blocks with hashes of previous blocks).[18] All of the nodes separately verify that every transaction meets the governance rules of the network protocol and then collectively decide whether a certain block will be added to the chain. All of these steps are executed by the nodes using their computational resources instead of manual checking and, consequently, there is a reward system to motivate the nodes to secure the system's sustainability. Blockchain is only one specific type of DLT; however, in order to be inclusive of all distributed ledger technologies, this dissertation will address DLT as a group of technologies.

---

[14] See Article I on the ledger types.

[15] European Parliament, 'Blockchain for supply chains and international trade. STUDY Panel for the Future of Science and Technology'. EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.544 – (May 2020, hereinafter: EU Blockchain Study), p. 4. doi: 10.2861/957600. <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf> accessed 11 October 2020.

[16] See Article I or Pierluigi Cuccuru, 'Beyond bitcoin: an early overview on smart contracts', (2017) International Journal of Law and Information Technology 25/3, p. 182 <https://doi.org/10.1093/ijlit/eax003> accessed 12 April 2018.

[17] Nakamoto (n. 10).

[18] EU Blockchain Study (n. 15), p. 4.

The main challenge of such electronic cash system lacking centralized intermediary oversight is the so-called 'double-spending' problem[19] – if there is no centralized controller, how can anyone make sure that funds are not spent twice? The Bitcoin system has been created in such a way that the entire network can make sure of the actual status of funds due to the existence of a transparent ledger, its protocol and the consensus mechanism[20] used to verify transactions.

1.2.3 Use cases of DLT

Blockchain technology-based Bitcoin quickly evolved into multiple versions of similar algorithm-based systems. These systems became a sort of new type of distributed infrastructure[21] that revealed a diverse set of new use cases which proved to be a substantial expansion from a simple electronic cash system. It was understood that DLT (and among it, also blockchain) is a disruptive technology allowing "data storage, digital asset transfers and transaction management, thus potentially replacing central processors and intermediaries with a decentralized computer architecture".[22]

After a slow global start, bitcoin and other cryptocurrencies have progressively expanded their use as a digital means of payment[23] and a target for investment.[24] A whole separate market has evolved around cryptocurrencies with "myriad users, trading companies, retailers, exchange platforms and financial service providers."[25] Although the financial sector remains one of DLT's focus points, the transformative or disruptive innovation rather lies in the innovative effect DLT can have on identity management, security management, data management and governance in general.[26]

This disruptive impact can also be identified in a number of applications developed in addition to financial sector applications, such as:

---

19 Cuccuru (n.16), p. 182.

20 ibid, p. 183.

21 EU Blockchain Study (n.15).

22 Cuccuru (n.16), p. 179.

23 *Skatteverket v David Hedqvist*, C-264/14, EU:C:2015:718 (hereinafter: *Hedqvist*).

24 Cuccuru (n.16), p. 181.

25 ibid.

26 ITU TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU Focus Group on Application of Distributed Ledger Technology (FG DLT). 'Technical Report FG DLT D 2.1. Distributed ledger technology use cases' (1 August 2019), pp. 21–22. <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf> accessed 20 October 2020.

- DLT-based smart contracts[27] allowing facilitation of international trade[28]
- ledgers to record land ownership[29]
- applications to collect taxes and allocate benefits[30]
- ledgers to record corporate events and share transactions[31]
- systems to prescribe and monitor the prescription of drugs[32]
- systems to monitor and track organ donations[33]
- applications to distribute and redistribute energy resources[34]
- applications to store and exchange data in supply chain management, healthcare, public services, intellectual property management, consumer ecommerce.[35]

As can be seen, DLT represents "general-purpose technologies"[36] with an abundance of possible applications. The estimate on the basis of positive scenarios is that intra-community trade will be using smart contracts in approximately 100 million transactions by 2030 that are worth up to approximately EUR 250 million, with total DLT expenditure reaching EUR 11 billion by 2030.[37]

---

27 Cuccuru (n.16), p. 186.

28 EU Blockchain Study (n.15), p. 65.

29 A test project by Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), ChromaWay, Landshypotek Bank, SBAB, Telia company and foresight company Kairos Future. Kairos Future. 'Report' (March 2017). <https://static1.squarespace.com/static/5e26f18cd5824c7138a9118b/t/5e3c35451c2cbb6170caa19e/1581004119677/Blockchain_Landregistry_Report_2017.pdf> accessed 20 October 2020.

30 Government Office For Science, 'Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser', (2016) p. 6. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> accessed by 19 October 2020.

31 Anne Lafarre and Christoph Van der Elst, 'Blockchain Technology for Corporate Governance and Shareholder Activism' European Corporate Governance Institute (ECGI) – Law Working Paper No. 390/2018, Tilburg Law School Research Paper No. 2018-7, (March 2018). <https://ssrn.com/abstract=3135209> or <http://dx.doi.org/10.2139/ssrn.3135209> accessed 20 October 2020.

32 ITU (n. 26), p. 53.

33 ibid.

34 ibid, p. 56.

35 EU Blockchain Study (n. 15).

36 ibid, p. 48.

37 PwC. 'PwC's Global Blockchain Survey 2018' (2018) <https://www.pwc.com/gx/en/industries/technology/blockchain/blockchain-in-business.html> and <https://www.pwccn.com/en/research-and-insights/publications/global-blockchain-survey-2018/global-blockchain-survey-2018-report.pdf> accessed 20 October 2020.

1.3 The research problem

The recently published Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for market infrastructures based on DLT (Pilot Regime)[38] clearly states that the "EU follows the principle of technological neutrality, but rules are still created based on market realities".[39] This means that the EU institutions are aware that the existing regulatory frameworks in most jurisdictions were built for centralized infrastructures[40] which leads "law and blockchain currently […] to stand in tension".[41] As stated by EBA and ESMA research and confirmed by the recent EU Digital Finance package (EU proposals for regulation of crypto-assets) the "provisions in existing EU legislation may inhibit the use of DLT".[42] Hence, investigations of such potential inhibitions is called for.

The problem itself is nothing new, as the development of the digital world led to the same problem – how to apply the regulations built for the offline world to the online world? Therefore, the problem is not specific to DLT, as the uptake of any new technology might lead to the same problem with existing regulation. If the problem is ignored, it might lead to a discrimination of the new technology. Consequently, DLT uptake raises the same problem, which must be addressed in line with the policy interest of the EU to develop and promote the uptake of transformative technologies, including blockchain and DLT.[43] The EU has taken steps towards this promotion both by the Digital Finance package and the development of the European Blockchain Services Infrastructure (EBSI), which is "a network of distributed nodes across Europe that will deliver cross-border public services".[44]

Therefore, upon the multiplicity of technologies that compete among one another, there is a need for regulation that can treat these competing technologies in a non-discriminatory way. Consequently, the main aim of this dissertation is to identify biases in regulation against the use of DLT and its outputs, processes and infrastructure. The biases are explored based on the existing regulatory

---

[38] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology, COM/2020/594 final (hereinafter: Pilot Regime).

[39] Pilot Regime (n. 38), p. 4.

[40] EU Blockchain Study (n. 15), p. 48.

[41] Michele Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 2019).

[42] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (Text with EEA relevance) SEC(2020) 306 final} – {SWD(2020) 380 final} – {SWD(2020) 381 final}, COM(2020) 593 final 2020/0265 (COD), (hereinafter: MiCA Proposal), pp. 1–4.

[43] Recital 1 of the MiCA Proposal (n. 42).

[44] EBSI platform. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI> accessed 17 December 2020.

frameworks in Estonia and the EU applied in the specific DLT use cases chosen by the author. The reasons for choosing these particular DLT use cases is elaborated in section 1.4 below. Along with this investigation, the author also explores the objectives of existing regulation to find the cause for these biases. By existing regulation, the author means the laws[45] of the Republic of Estonia and the European Union relevant in the context of the chosen use cases.

To identify biases, the author uses the technology neutrality principle and its sub-principle of functional equivalence as tools. The technology neutrality principle aims at securing neutrality in regulation towards any technology and the technology-considerate treatment of different technologies. The functional equivalence sub-principle is used to identify functional equivalence between the old and the new in order to grant equivalent treatment. However, as the principles are unclear as to their meaning and application, the research also includes an exploration of the said principles.

On the one hand, legal certainty and clarity are the "key catalysts" for the development of technology,[46] but on the other hand, the Pacing Problem and the Collingridge dilemma lead to the careful timing of the regulatory activity that should allow iterative adaptations as the technology matures.[47] This means that, although new regulation for DLT would have an invaluable 'trust-enhancing role'[48] and there is a plethora of regulative strategies that are considered to relieve the tension between DLT and law, such as: (1) the wait-and-see approach (innovators operating in 'quasi-lawless zones'); (2) application of existing legal frameworks; (3) regulatory cooperation (issuing guidance, regulatory sandboxes) and new regulation, incl. self-regulation and polycentric coregulation,[49] such alternative strategies should be carefully considered so as not to have an equally hindering effect as that of no DLT regulation. In response to the named challenges, this dissertation addresses some of these strategies with the aim of identifying a sustainable regulative strategy that secures a regulatory framework resistant to bias towards DLT. The research is especially relevant considering that, as stated in the proposal for Digital Finance package (a regulation on markets in crypto-assets) introduced at the end of September 2020 (MiCA Proposal)[50] and the proposal for the pilot regime for market infrastructures based on DLT (Pilot

---

45 On the basis of the Oxford Handbook of Law, Regulation and Technology, the existing regulation in this dissertation is meant as laws or as "authoritative rules backed by coercive force". Roger Brownsword, Eloise Scotford and Karen Yeung, *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017), p. 6.

46 EU Blockchain Study (n. 15), p. 11.

47 Finck (n. 41), p. 153.

48 Recital 1 of Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC 2014) OJ L 257/73. See also Finck (n. 41), pp. 152–153.

49 ibid, pp. 153–181.

50 MiCA Proposal (n. 42).

Regime),[51] the EU has a policy interest for the uptake of transformative technologies, such as DLT, in the financial sector, and for the adaptation of regulations to promote this uptake based on the evidence of hurdles.[52] Both proposals identify as one of their goals the generation of further evidence of these hurdles to assess "whether and how to amend existing financial services legislation to ensure it is technology neutral".[53] Furthermore, the MiCA Proposal reiterates that the proposal supports the EU's holistic approach to DLT and the aim to position Europe at the forefront of its innovation and uptake.[54] The dissertation supports these goals as the investigation of DLT use cases is also seeking evidence of these hurdles.

Lastly, this type of analysis is especially relevant during the adoption phase of a technology in society, meaning that, at the time, regulators are still considering multiple courses of action to react to the arrival of transformative innovation.

With the term regulator, the author means any branch of government – legislative, executive or judiciary – unless otherwise stated and, with the term "regulatory framework", the author refers to any modality of regulation that creates obligations on the subjects of DLT use cases.

1.4 Field of investigation and research questions

This dissertation does not treat the domain of DLT regulation as a specific or separate field of study but uses DLT as an example of a technology for which neutrality of regulation is crucial in order for it to compete with other technologies. The shortcomings of any regulatory framework in relation to any technology need to spark an action in the regulator to either address or choose to ignore these. It is not only by ignoring these shortcomings but also by choosing not to identify these shortcomings that leads regulators to be non-compliant with the principle of technology neutrality. However, in order to identify these shortcomings, regulators need to investigate both the technology and potential biases in regulation.

The DLT use cases the author explores in this dissertation range from operation of a bitcoin exchange, administration of shareholder ledger using DLT and use of smart contracts in Initial Coin Offerings (ICOs).[55] The use cases examined in this dissertation can broadly be divided into the following types:

---

[51] Pilot Regime (n. 38).

[52] ibid, Recital 1, and pp. 2–5.

[53] MiCA Proposal (n. 42), p. 146.

[54] ibid, p. 3.

[55] According to the European Securities and Markets Authority (ESMA), ICOs "effectively allow businesses to raise capital for their projects by issuing digital tokens in exchange for fiat currencies or other crypto-assets, e.g. Bitcoin or Ether. ICOs are typically promoted on the web and social media to potential investors using so-called 'white papers'." European Securities and Markets Authority, 'Advice Initial Coin Offerings and Crypto-Assets'

1. examination of the treatment of DLT outputs and the subjects operating with DLT outputs;
2. examination of the use of DLT in corporate ledgers;
3. examination of the use of DLT in contracts.

The chosen use cases allow the demonstration of different ways of apparent and non-apparent discrimination against DLT that may be difficult to detect. Consequently, the examples allow the identification of apparent and non-apparent biases of regulation against DLT in a wide selection of use cases. To address the research problems described above in the context provided in the introduction and based on the DLT use cases presented, the research questions addressed in this dissertation are divided into three main questions and three sub-questions based on each DLT use case as follows:

1. How to identify bias against DLT in regulation? (Chapter 2)
2. How to sustainably ensure DLT-neutrality in regulation? (Chapter 3)
3. Based on the chosen DLT use cases, is the existing regulation in compliance with the technology neutrality principle or is it based on a bias against DLT use? (Chapter 4)

    a) Whether the anti-money laundering regulation in Estonia and its application to bitcoin and its traders complies with the principle of technology neutrality (on the basis of *de Voogd*[56]) similarly to the EU VAT regulation and its application to bitcoin and its traders (on the basis of *Hedqvist*[57])?
    b) Whether, under the Estonian Commercial Code, a DLT-based shareholders ledger of an Estonian private limited company administered by a non-CSD could be regarded functionally equivalent to the CSD maintained ledger, and granted effects equivalence, with CSD administered shareholders ledger?

(9 January 2019), p.11. <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> accessed 21 July 2017. For the purposes of the discussion in this dissertation, there will be no separation made between ICOs, "Security Token Offering" (STO) or "Equity Token Offering" (ETO). "Security Token Offering" or "STO" is non-legal terminology and in the relevant community means an issue of tokens that "function as a traditional security asset. They represent a stake in the wealth created by a third party and take their value from that party's success or failure. Distinct from an equity token in that no ownership of the underlying venture is created." Eric Reed, 'Equity Tokens vs. Security Tokens: What's the Difference?' (Bitcoin Market Journal 13 February 2019) <https://www.bitcoin-marketjournal.com/equity-token/> accessed 23 July 2019

For an example of a whitepaper, please see here: <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 1 May 2019.

[56] Estonian Supreme Court Administrative Law Chamber (SCALC) judgment, 11th April 2016, case 3-3-1-75-15 (hereinafter: *de Voogd*).

[57] *Hedqvist.*

c) Under eIDAS, can DLT-based smart contract signature be regarded functionally equivalent to qualified electronic signature and granted effects equivalence with Public Key Infrastructure (PKI) model based signature?

Based on the DLT use cases examined and the regulative strategies identified by the EU Blockchain Study, this dissertation attempts to find an answer to the question how to ensure DLT-neutral regulation. In the context of regulatory approaches, the research explores principle-based regulation.[58]

1.5 Current status of research in the area

Regulatory approaches to technology have been the subject of academic discourse for decades, with DLT- or blockchain-specific legal research being a recent addition. Therefore, existing research can be divided into two separate topics: legal research on the technology neutrality principle and legal research primarily on DLT.

The legal research on the technology neutrality principle includes research on functional equivalence and functional approach as concepts of the same principle. This legal discourse has been developed since the 1990s with Bert-Jaap Koops[59] and Chris Reed[60] as the most noteworthy contributors. Koops' work entails a comprehensive overview of the principle of technology neutrality, addressing many of the misconceptions related thereto, with Reed addressing it more from the context of offline and online equivalence[61] or a cyberspace and futureproofing focus.[62] In this dissertation, the author builds on the work of both Koops and Reed to map the principles developed and presents the critique by Savin[63] on the diffi-

---

[58] Sofia Ranchordas and Mattis van 't Schip, 'Future-Proofing Legislation for the Digital Age' in S. Ranchordas and Y. Roznai (eds), *Time, Law, and Change* (Hart, 2020) (Forthcoming) <https://ssrn.com/abstract=3466161> or <http://dx.doi.org/10.2139/ssrn.3466161> accessed 22 October 2020.

[59] Bert-Jaap Koops, 'Should ICT Regulation Be Technology-Neutral?' in Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, (eds.), *STARTING POINTS FOR ICT REGULATION. DECONSTRUCTING PREVALENT POLICY ONE-LINERS,* IT & LAW SERIES, Vol. 9 (The Hague: T.M.C. Asser Press, 2006), pp. 77–108 <https://ssrn.com/abstract=918746> accessed 22 March 2020.

[60] Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement' (Autumn 2010) International Journal of Law and Information Technology 18/3, p. 249. <https://doi.org/10.1093/ijlit/eaq006> accessed 08 December 2019.

[61] ibid.

[62] Chris Reed, *Making Laws For Cyberspace* (Oxford University Press 2012).

[63] Andrej Savin, 'Rule Making in the Digital Economy: Overcoming Functional Equivalence As a Regulatory Principle in the EU' (*CBS LAW Research Paper* 19–10, 24 February 2019), Journal of Internet Law 22/8, p. 5 <https://ssrn.com/abstract=3340886> accessed 28 November 2019.

culties in the application of the principle in law-making and critique by Harvey[64] in the application thereof by courts. Furthermore, the importance of Kamecke and Körber,[65] in clarifying the focus of the principle towards allowing more self-regulation, cannot be overstated. Lastly, the principle has recently received its first address in the DLT context by Furrer and Müller,[66] who addressed the sub-principle of functional equivalence in the context of ICOs and DLT-based smart contracts.

However, the legal research related to DLT is in its early stages and mostly targets blockchain technology or cryptocurrencies. De Filippi and Wright[67] have substantially mapped this domain in a form that is detached from specific jurisdictions and regulative frameworks. Rather, their approach focuses on the possibilities of use and the potential impact of the technology on regulation in theory. They also address models of regulation and build on Lessig's[68] code is law by presenting code-based regulation as a development.

A rather comprehensive overview ranging from building regulative models on Lessig and addressing financial regulation and competition laws in the DLT context was presented in 2019 by Hacker *et al.*[69] The same year, Finck opened up many discussions focusing more on blockchain governance and concepts such as regulatable and regulatory technology (again building on Lessig's groundwork).[70] Finck also headed the EU Blockchain Study,[71] which aimed to identify the most crucial legal issues the EU needs to focus on and the regulative strategies at its disposal.[72]

The only research in this domain linking DLT and technology neutrality is the EU Blockchain Study that occasionally addresses in the report whether techno-

---

64 David John Harvey, *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Bloomsbury Publishing 2017), pp. 59–60.

65 Ulrich Kamecke and Torsten Korber, 'Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood. Technological Neutrality in the EC Regulatory Framework' (2008), p. 331. <http://www.unigoettingen.de/de/document/download/65b9d0d841b831596888f8fb208e838b.pdf/KameckeKoerber_ECLR08_29%285%29_330-339.pdf> accessed 30 April 2020.

66 Andreas Furrer and Luka Müller, '"Functional equivalence" of digital legal transactions A fundamental principle for assessing the legal validity of legal institutions and legal transactions under Swiss law,' Jusletter (18 June 2018), p. 15. <https://www.mme.ch/fileadmin/files/documents/MME_Compact/2018/180619_Funktionale_AEquivalenz.pdf> accessed 12 November 2020.

67 De Filippi and Wright (n. 12).

68 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

69 Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, "An Introduction" in Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, (eds.), *Regulating Blockchain Techno-Social and Legal Challenges*, 1st edition, (Oxford University Press, 2019), p. 2.

70 Finck (n. 41).

71 EU Blockchain Study (n. 15), p. 48,

72 ibid.

logy neutrality was established in either the text of the regulation or the implementation thereof. On the other hand, the study does not address the innate biases of regulation based on the technology neutrality principle. Nevertheless, the report rather sporadically mentions neutrality and often discusses it as a goal rather than as a measurement tool.

As mentioned, Furrer and Müller explored a functional equivalence sub-principle for DLT use cases, but quite briefly and in a limited context of ICOs and smart contracts. None of the earlier work addresses the biases in existing regulation based on the technology neutrality principle, specifically in relation to DLT nor conducted any functional analysis of the author's chosen use cases. Consequently, this research complements earlier research on both DLT and the principle of technology neutrality.

1.6 Methods and resources

To address the research problems and questions, the dissertation focuses on the following two tools: (i) the principle of technology neutrality and (ii) its sub-principle of functional equivalence (both presented in Chapter 2) and applies these principles to the existing regulation applicable in the specific DLT use cases (explored in Chapter 4).

The other legal research methods used for the purposes of research are a mix of legal research methodology and proactive methodology based on the IT law approaches presented by Peter Seipel.[73] First of all, the *qualitative systematic analysis method* is used to map the scope and content of the principles of technology neutrality and the sub-principle of functional equivalence on the basis of regulation, case law, legal theory and other secondary sources.

Secondly, in this dissertation, the author uses *legal doctrine or legal dogmatics* as a methodology (doctrinal legal research) and employs the said method in researching positive law in order to identify existing regulation that applies to the DLT use cases. The doctrinal legal research combines descriptive (external perspective),[74] hermeneutical and normative (internal perspective) research, meaning that the author is not only describing the positive law, but also interpreting and evaluating the text of the law.

The author does not use *comparative methodology* in the traditional sense but merely utilizes comparisons as a methodology in a limited scope. The methodology of comparisons is employed to present DLT-specific regulation enacted in different jurisdictions.

---

[73] Peter Seipel, IT Law in the Framework of Legal Informatics, p. 46 (2004). <https://www.scandinavianlaw.se/pdf/47-2.pdf> accessed 25 October 2020.

[74] As explained by Sanne Taekema the "external perspective fits descriptive research which an internal perspective fits normative research". Sanne Taekema, 'Relative Autonomy. A Characterisation of the Discipline of Law' in Bart van Klink and Sanne Taekema, *Law and Method. Interdisciplinary Research into Law* (2011), p. 41.

Thirdly, as DLT is a new and emerging technology, this dissertation also explores a *proactive methodology* using the IT law-specific *problem cluster approach* and the *special theory approach. The problem cluster approach* is problem-oriented or delves into the legal aspects of a particular technology use case.[75] As part of the approach, different legal instruments are analysed in order to identify the relevant legal norms applicable to a use case. Seipel considers this a functional approach functional that is targeted towards "locating *lacunae* and deficiencies in existing legal regulation" from the point of view of a problem or a specific use case. The specific DLT use cases formulate the problem cluster.

Lastly, *the special theory approach* – the themes that fall under this approach require "analyses of the interaction of rules and tools [...] and it does not content itself with simple presentations of valid law (*lex lata*)".[76] The author conducts functional analysis of legal norms and applies functional equivalence sub-principle as *a special theory approach* to identify the functions the existing regulation requires and the functions DLT performs in comparison. This means that in the research, the author not only explores existing regulation, but also explores the technology and its wider context to identify whether the technology is functionally equivalent to the objectives of the functions required by existing regulation. The *special theory approach* allows the for identification of infrastructural biases in regulation that are built around a certain system or 'tool', as used by Seipel, which the regulator knows and can relate to.

Through the application and expansion of the *special theory approach*, the author analyses the interaction between rules and tools, using the functional setup of a particular technology and the legislative aims of the regulator to identify functional equivalence.

As to the resources used to conduct the research, the key resources employed in the *qualitative systematic analysis method* are the Framework Directive,[77] the General Data Protection Regulation (GDPR),[78] eIDAS and the writings of legal scientists and academics. The DLT use cases guide the dissertation as to the areas of *dogmatic legal research* in the clusters based on the DLT use case. The specific regulation under examination expands from public law to private law. The first DLT use case explores the VAT (VAT Directive[79]) and anti-money laundering regulation (the Money Laundering and Terrorist Financing Prevention

---

75 Seipel (n. 73), p. 46.

76 ibid.

77 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ L 108, 24.4.2002, pp. 33–50.

78 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 the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) (Text with EEA relevance) OJ L 119, 4.5.2016, pp. 1–88.

79 Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax OJ L 347, 11.12.2006, p. 1–118 (VAT Directive).

Act[80] of Estonia, and of AML Directives),[81] the shareholder ledger use case explores corporate law and public ledger regulation (predominantly the Commercial Code[82] of Estonia) and the protocol-based contract use case explores both contract law and electronic signatures regulation (eIDAS,[83] Law of Obligations Act[84] and General Part of the Civil Code[85] of Estonia). The author uses the regulation of primarily Estonian – and EU laws as well as comparative regulation from other jurisdictions. The other jurisdictions are chosen because, in these jurisdictions DLT-specific regulation has been proposed or adopted. Such jurisdictions include France, Italy, Malta and also certain States in the US.

1.7 Structure

As explained in the previous subsection, the main research problem is addressed by exploring different DLT use cases and not at a specific field of law.

Therefore, this dissertation does not explore a specific substantive law, but instead explores existing regulation as applied to the DLT use cases chosen

---

[80] Money Laundering and Terrorist Financing Prevention Act of Estonia [*rahapesu ja terrorismi rahastamise tõkestamise seadus]* – RT I 2008, 3, 21; RT I 2008, 3, 21 (hereinafter: MLPA I). Money Laundering and Terrorist Financing Prevention Act of Estonia [*rahapesu ja terrorismi rahastamise tõkestamise seadus]* – RT I 06.07.2016, 13 (hereinafter: MLPA II). Money Laundering and Terrorist Financing Prevention Act of Estonia [*rahapesu ja terrorismi rahastamise tõkestamise seadus]* – RT I, 17.11.2017, 2 (hereinafter: MLPA III). All translations of these legal acts are based on the unofficial translations published in the Estonian State Gazette (*Riigi Teataja*). These translations do not have any legal force.

[81] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) OJ L 309, 25.11.2005, p. 15–36 (hereinafter: AMLD). Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) (hereinafter: the 4th AML Directive or AMLD), OJ L 141, 5.6.2015, pp. 73–117. On 30 May 2018 the 4th AMLD was amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) (hereinafter: the 5th AML Directive or AMLD) PE/72/2017/REV/1, OJ L 156, 19.6.2018, pp. 43–74.

[82] Commercial Code [*äriseadustik]* – RT I 1995, 26, 355; RT I, 10.07.2020, 35.

[83] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).

[84] Law of Obligations Act, [*võlaõigusseadus]* – RT I 2001, 81, 487; RT I, 20.02.2019, 8.

[85] General Part of the Civil Code Act [*tsiviilseadustiku üldosa seadus]* – RT I 2002, 35, 216; RT I, 06.12.2018, 3.

through the prism of the two principles. Therefore, the structure of the research is built as follows:

DLT use cases (*problem cluster approach*)	**existing regulation** (*legal dogmatics*)

These elements are put through a compliance check under the principle of technology neutrality as follows:

principle of technology neutrality
(qualitative systematic analysis method – to explore its scope)
sub-principle of functional equivalence
(special theory approach)

DLT use cases *(problem cluster approach*)	**existing regulation** (*legal dogmatics*)

The compliance check of existing regulation with the technology neutrality principle is not conducted in isolation from the objectives of the specific regulation as the objectives of the regulation not only reveal why the regulator decided to include certain formal requirements but also what functions any new solution could potentially fulfil without meeting the formal requirements. This approach challenges the regulation's bias towards a certain existing solution (technical or organizational) and allows to analyse whether, in a specific use case, the DLT solution is able to achieve objectives functionally equivalently without necessarily meeting all the procedural or formal requirements set in the existing regulation. The described approach allows the author to assess whether the existing regulation is technology-neutral or has an innate bias for a technical – or organizational solution that existed during the drafting of the regulation.

Each article the compendium is based on, other than Article VI, formulates a problem cluster. In the problem cluster, the technical- or organizational solution of the DLT use case is presented and the applicable existing regulation is explored in order to conduct the functional analysis. In order to conduct the functional analysis in each DLT use case first the requirements of the existing regulation are identified e.g., formalities, certificates, licenses, registrations, limitations, restrictions and thereafter, the objectives of these requirements are explored - such as transparency, legal certainty, identification, immutability, etc. Only after such analysis is it possible to assess whether the DLT employed in the specific use case is able to achieve the same objectives through the use of its functions. In

response to the research questions, the argument of this dissertation is developed in the four journal articles listed below along with the current compendium.

- Article I. "Decentralised technology and technology neutrality in legal rules: an analysis of *De Voogd* and *Hedqvist*"[86] investigates the means of payment use case and explores "whether the principle of technology neutrality can be applied to the centralised-decentralised scale in a manner similar to its application to the offline-online scale"[87]. The article discusses two court cases – one from the Estonian Supreme Court (*de Voogd*) and the other from the CJEU (*Hedqvist*) – comparing the two approaches of applying existing regulation to bitcoin and the activity of trading with bitcoin in comparison with the application of existing regulation to fiat currencies or traders in this. Based on this comparison, the author examines whether the regulatory framework and the interpretation of it was technology neutral. The article concludes that based on *de Voogd* there was a bias against alternative means of payment under Estonian law which is contrary to the principle of technology neutrality.
- Article II. "Shareholder ledger using distributed ledger technology: the Estonian perspective"[88], which analyses the compliance of the regulation that addresses the maintenance of a shareholder ledger with the principle of technology neutrality using Estonian law as an example. In addition, the article analyses whether existing regulatory framework grants effects equivalence to a functionally equivalent DLT-based ledger with a CSD maintained ledger. The article concludes that the regulation has a bias towards CSD maintained ledgers and, irrelevant of the functions the DLT-based ledger performs the result and effect under the regulation depends on the ledger administrator and not the functions and processes the ledger maintenance includes.
- Article III. "Hybrid smart contract challenge to European electronic signature regulation" (co-authored with Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva and Alex Norta)[89] explores, based on Estonian and EU law, whether regulation eIDAS allows the qualification of the DLT-based hybrid smart contract used in Initial Coin Offerings (ICO), based on the qualification of the electronic signature appended to it, as a contract in an electronic form. In

---

[86] Anne Veerpalu, 'Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De Voogd and Hedqvist' (2018) Baltic Journal of Law & Politics, 11/2, pp. 61–94. <https://doi.org/10.2478/bjlp-2018-0011> accessed 15 July 2019.

[87] ibid, p. 1.

[88] Anne Veerpalu, 'Shareholder ledger using distributed ledger technology: the Estonian perspective' (2019) Masaryk University Journal of Law and Technology, 13/2, pp. 277−310. <10.5817/MUJLT2019-2-6> accessed 15 July 2019.

[89] Anne Veerpalu, Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva, Alex Norta, 'The hybrid smart-contract agreement challenge to European electronic signature regulation' (2020) International Journal of Law and Information Technology 28/1, pp. 39–84. <https://doi.org/10.1093/ijlit/eaaa005> accessed 31 May 2020.

the article, the smart contract is referred to as the hybrid smart contract because the contract is not only code but composed of multiple components that include also written text. The focus point of the research is the compliance of eIDAS regulation with the principle of technology neutrality in the context of DLT-based smart contracts. Furthermore, the article uses the sub-principle of functional equivalence to assess whether the electronic signature on the hybrid smart contracts can be qualified as functionally equivalent to the qualified electronic signatures under eIDAS and concludes that eIDAS regulation includes a bias towards Public Key Infrastructure based model and centralized trust service providers.

- Article IV. "Functional equivalence – an exploration through shortcomings to solutions"[90] discusses the sub-principle of functional equivalence as a source for the development of a technology-neutral regulation model in order to respond to and resolve the bias against the application of the distributed technologies discussed in the preceding articles. The article explores the use of the sub-principle of functional equivalence in different jurisdictions and in case law. The article explores a principle-based approach to regulation on the basis of the "privacy by design" regulation model used in the GDPR.

[90] Anne Veerpalu, 'Functional Equivalence: An Exploration Through Shortcomings to Solutions' (2019) Baltic Journal of Law & Politics 12/2, pp. 134–162. doi: <https://doi.org/10.2478/bjlp-2019-0015> accessed 07 June 2020

II THE PRINCIPLE OF TECHNOLOGY NEUTRALITY

In this chapter, the author presents the meaning and relevance of the principle of technology neutrality in the DLT context in order to address the research question: how to identify bias against DLT in regulation? Furthermore, the author elaborates on the difficulties of understanding and complying with the principle and identifies the ways in which the principle is misused.

2.1 The aim of the principle

The principle strives for anti-discrimination and equality of treatment of technologies along the lines of gender-neutrality and ethnic origin neutrality principles. In the EU law context, the principle is at times defined through the freedoms of the individual, e.g., a definition of technology neutrality provided in summary of Regulation (EU) No 283/2014 on trans-European networks in the area of telecommunications infrastructure:

> "the freedom of individuals and organisations to choose the most appropriate and suitable technology for their needs. Products, services or regulatory frameworks taking into account the principle of technology neutrality neither impose nor discriminate in favour of the use of a particular type of technology."[91]

The principle originated from the aim of securing offline-online equivalence. Considering that offline and online equivalence is no longer the primary focus, it can be stated that the principle aims to secure a sort of blindness to the differences between technology and flexibility in law not to hinder the further development of technology. According to Koops, technology-independence is not the same as neutrality independence as independence requires the regulation to "abstract completely away from technology"[92] and does not regard technology as part of the solution at all. Although, regulation that is technologically indifferent or independent can still be neutral in case regulation does not prefer the technology-void solution over the technology-inclusive solution.[93] Technology-neutral regulation, on the other hand, does not favour any technology over another.[94]

The main aim of the principle is therefore that "the rules should neither require nor assume a particular technology".[95] Neither should regulation be built so that

---

[91] Summary of Regulation (EU) No 283/2014 – guidelines for trans-European networks in the area of telecommunications infrastructure titled Supporting telecommunications networks and digital service infrastructures across Europe <https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32014R0283> accessed 1 March 2021.

[92] Koops (n. 59), p. 5.

[93] Reed (n. 62), p. 193.

[94] Koops (n. 59), p. 5.

[95] Reed (n. 62), p. 191.

only one technology can easily comply with it and that different technologies must adapt themselves to conform with the requirements set in regulation. Neutrality requires that each type of technology must be treated in an equivalent way so that the effect of the regulation across technologies is equivalent and does not favour a specific technology.[96] Given this aim, rather than focusing on the characteristics or functions as requirements, regulation should focus on the aim of these functions.[97]

Kamecke and Körber find that the principle prohibits the regulator from maintaining or creating regulation that aims to replace the market selection between technologies with selection by a regulator.[98] This means the principle dictates that "the market rather than the state should decide the success or failure of technologies".[99]

2.2 The relevance of the principle to DLT

When the online world emerged, many regulators identified a potential risk of discrimination against the online domain as regulation had been created only for the offline domain. The named discrimination was mitigated by the introduction of the principle of technology neutrality, which aimed to neutralize any preference of the regulator towards the offline domain.

Furthermore, as stated by Chris Reed, "the key factor in persuading legislators that technology neutrality should be adopted more widely was the advent of the Internet for general public use".[100] The threat of the mistreatment of the Internet was regarded sufficiently important to include the principle as a guiding goal in recitals, green papers, model laws, directives and regulation. Nevertheless, the principle, although primarily regarded as the "starting point for ICT regulation",[101] has along with the digital revolution outgrown its initial use case.

Therefore, the principle's overarching attempt to guide the regulator away from influencing how any technology in any sector, application and use case should work or be used [102] is absolutely relevant for DLT. Consequently, the principle is relevant for any technology, but especially relevant for technologies that are deconstructing the key structures of society, trade and communication. DLT is affecting key infrastructures of digital society similarly as the online domain deconstructed the offline infrastructures.

---

96 ibid, p. 192.

97 ibid, p. 192.

98 Kamecke and Körber (n. 65), p. 331.

99 ibid, p. 331.

100 Chris Reed, 'Taking Sides on Technology Neutrality', (September 2007) SCRIPTed 263 4/3, p. 264. <http://heinonline.org/HOL/P?h=hein.journals/scripted4&i=281> accessed 20 November 2018.

101 Koops (n. 59), p. 26.

102 ibid.

2.3 The subjects of the principle

Technology neutrality is sometimes confused with platform neutrality and net neutrality. As technology regulation is not based on well-developed legal theories, technology neutrality, platform neutrality and net neutrality are some of the key concepts in technology regulation. The principle needs to be distinguished from these other neutralities, as the subjects and content of the principle are very different. Platform neutrality applies to platforms (e.g., Amazon and Google) and means that online platforms with a wide audience should not use their platform only to offer, rank or create preference for their own goods and services.[103] Net neutrality applies to Internet service providers (ISPs).[104] ISPs that are predominantly operated by telecom companies are able to block Voice over Internet Protocol (VoIP), specifically services like Skype , Zoom, etc.[105] Therefore, net neutrality addresses the concern of discrimination against content providers. As ISPs have the technical capability to discriminate against content, meaning to prefer certain content and block other content, net neutrality prohibits discrimination based on content that travels through these controlling infrastructure intermediaries. Furthermore, net neutrality prohibits the preferential treatment of the services of these ISPs or any specific applications for the purpose of minimising competition, transparency and consumer choice.

Both of these neutrality concepts target either public – or private stakeholders who control certain infrastructure. In contrast, the principle of technology neutrality is targeted at the regulator who controls the regulation of multiple infrastructures, services, processes and outputs and the principle aims to restrict the regulator from discriminating against any technology. The principle is not only relevant to legislature in law-making, but also the executive branch and the judiciary are obligated to adhere to the principle when implementing and interpreting existing regulation.[106]

---

[103] Jan Krämera and Daniel Schnurr 'Is there a need for platform neutrality regulation in the EU?' (2018) Telecommunications Policy, 42/7, pp. 514–529. <https://doi.org/10.1016/j.telpol.2018.06.004> accessed 9 May 2020.

[104] Winston J. Maxwell and Marc Bourreau, 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' (January 2015) Computer and Telecommunications Law Review 21/ 1, pp. 1–4. <https://ssrn.com/abstract=2529680> or <http://dx.doi.org/10.2139/ssrn.2529680> accessed 28 September 2020.

[105] Almost 10 years ago in a speech delivered by Vice President of the European Commission Neelie Kroes at the European Commission and European Parliament Summit on 'The Open Internet and Net Neutrality in Europe' in Brussels, 11 November 2010. (Transcript) <https://ec.europa.eu/digital-single-market/en/news/net-neutrality-%E2%80%93-way-forward> accessed 9 May 2020.

[106] Koops (n. 59).

2.4 The origins of the principle

In July 1997, the principle was included in the Framework for Global Electronic Commerce by US President Bill Clinton and Vice President Al Gore,[107] the Bonn Ministerial Conference.[108] In 1998, ICT regulations were formulated by the UK and Dutch governments,[109] in which either technology independence or neutrality were discussed, and similar statements were included in the G8 Okinawa Charter on Global Information Society in 2000,[110] the Green Paper on Consumer Protection in 2001[111] and the World Summit on the Information Society (WSIS) in 2002.[112] Furthermore, the principle has been also represented in EU law in several directives and regulations, however, foundations of the principle can also be identified in the Treaty of European Union (TFEU),[113] in Article 2 by recognition of the values of equality and non-discrimination and in Article 3 that stipulates the aim of the Union to establish an internal market that promotes "scientific and technological advance". Without a doubt, the establishment of Digital Single

---

[107] "Rules should be technology-neutral (i.e. the rules should neither require nor assume a particular technology) and forward-looking (i.e. the rules should not hinder the use or development of technologies in the future)". William J. Clinton, Al Jr. Gore, 'Framework for Global Electronic Commerce', (White House 1 July 1997) <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html> accessed 12 November 2018.

[108] "Ministers stress that the general legal frameworks should be applied on-line as they are off-line. In view of the speed at which new technologies are developing, they will strive to frame regulations which are technology-neutral, whilst bearing in mind the need to avoid unnecessary regulation". European Commission. Directorate-General for the Information Society and Media. 'Declarations. Global information networks: Realising the potential.' (European ministerial Conference. Bonn, 6 to 8 July 1997). <https://op.europa.eu/en/publication-detail/-/publication/0d76a85c-e66a-41af-91c2-28cd29a85094> accessed 29 April 2020.

[109] Koops (n. 59), p. 1.

[110] "We should ensure that IT-related rules and practices are responsive to revolutionary changes in economic transactions, while taking into account the principles of effective public-private sector partnership, transparency and technological neutrality." Okinawa Charter on Global Information Society. <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> accessed 29 April 2020.

[111] "A comprehensive, technology-neutral, EU framework directive to harmonize national fairness rules for business-consumer commercial practices". 'Opinion of the Economic and Social Committee on the "Green Paper on European Union Consumer Protection' (COM(2001) 531 final) OJ C 125, 27.5.2002, p. 1–5.

[112] "The rule of law, accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-centered Information Society." World Summit on the Information Society. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Document WSIS-03/GENEVA/DOC/4, (12 December 2003). <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> accessed 29 April 2020.

[113] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390.

Market (DSM) is also a goal in line with the principle as DSM should be based on the freedom of establishment and freedom to provide services across the single market of the EU. As stated by European Commission in 2015, DSM is a market "where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence".[114] Therefore, under Articles 49–55 (freedom of establishment) and 56–62 (freedom to provide services) of the TFEU, self-employed persons and professionals or legal persons who are legally operating in one Member State should not be restricted or discriminated against for using a particular technology, form or means in another Member State. More specifically, the principle is represented in the following secondary law of the EU as provided below.

The e-Commerce Directive[115] of 2000 states in Article 9 that Member States must

> "ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

The referred Article aims for non-discrimination of electronic form of contracts and instructs the Member States not to deprive this different form legal effectiveness and validity. The new proposal for Digital Services Act[116] that amends the e-Commerce Directive specifically names the principle of technology neutrality in Recital 5 by stating that it aims to set up "requirements that are technology neutral" so that innovation would "not be hampered but instead be stimulated".

The principle was included from 2002 also in Recital 18 of the Framework Directive,[117] which stipulates that "regulation … neither imposes nor discriminates in favour of the use of a particular type of technology...". Article 8 (1) and (2) require Member States to ensure "that there is no distortion or restriction of competition in the electronic communications sector" and that "in carrying out the regulatory tasks specified in this Directive and the Specific Directives, in

---

[114] Communication from the Commission, A Digital Single Market Strategy for Europe, COM (2015) 192 final, p 3.

[115] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, pp. 1–16.

[116] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

[117] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). Official Journal of the European Union, L 108, 24.4.2002, pp. 33–50.

particular those designed to ensure effective competition, national regulatory authorities take utmost account of the desirability of making regulations technologically neutral."

The said Framework Directive promotes the principle also through the reiteration of the goals of non-discrimination principle in Article 8 (3) (c) "The national regulatory authorities shall contribute to the development of the internal market by inter alia ensuring that, in similar circumstances, there is no discrimination in the treatment of undertakings providing electronic communications networks and services" and the goal of transparency in Article 4 (d) "promoting the provision of clear information, in particular requiring transparency of tariffs and conditions for using publicly available electronic communications services.

The said principle was included in Recitals 34, 35, 38, 40, 68 and Article 7b of the Better Regulation Directive[118] in relation to spectrum management and is also included in the service neutrality principle. This brought about a new wave of liberalisation for the technology of mobile operators.[119]

Recital 51 of the NIS Directive[120] from 2013 included the principle stating that "measures … should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner." This means that the wording of the principle often does not use the term technology neutrality, but merely conveys the idea of it.

In Article 6 (7) (e) of Regulation (EU) No 283/2014 of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure[121] it is stipulated that in

> "Actions contributing to projects of common interest in the field of broadband networks shall meet all the following criteria in order to be eligible for funding:
> …
> (e) use the technology which is deemed most suitable to address the needs of the geographic area in question, taking into account geographic, social and economic factors based on objective criteria and in keeping with technological neutrality;"

---

[118] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Better Regulation Directive, Text with EEA relevance). OJ L 337, 18.12.2009, p. 37–69.

[119] Maxwell and Bourreau (n. 104), pp. 1–4.

[120] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union, L 194, 19.7.2016, pp. 1–30.

[121] Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC Text with EEA relevance OJ L 86, 21.3.2014, p. 14–26.

Furthermore, in Section 4(4) of the same Regulation's Annex titled Projects of Common Interest it is stipulated that:

> "Actions taken for the provision of local wireless connectivity shall be eligible to receive funding if they:
> …
> (4) respect the principles of technological neutrality at the level of the backhaul, the efficient use of public funding and the ability to adapt projects to the best technological offers;"

The General Data Protection Regulation (GDPR)[122] from 2016 stated that "in order to prevent creating a serious risk of circumvention" Recital 15 urges the protection of natural persons be technologically neutral, stating that it "should not depend on the techniques used". Recital 28 of GDPR talks about the specific technique of pseudonymisation, but also clarifies that "the explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection." Furthermore, in Recital 71 of GDPR, the idea of the choice of measures by the obligated subjects is stated, indicating that the subject needs to follow "appropriate mathematical or statistical procedures" and "implement technical and organisational measures" that are "appropriate". The 'appropriateness' of these measures is measured against the objectives these measures aim to achieve – that of minimisation of data, risk of errors and possible discrimination based on data.

Also, public-sector specific European Interoperability Framework (EIF) developed by European Commission and published in 2017 as a guideline should be also mentioned here, as it includes 12 principles to govern interoperability between different stakeholders and public sector and technology neutrality is one of these principles. The Framework stipulates clearly:

> "When establishing European public services, public administrations should focus on functional needs and defer decisions on technology as long as possible in order to minimise technological dependencies, to avoid imposing specific technical implementations or products on their constituents and to be able to adapt to the rapidly evolving technological environment."[123]

In the EIF and its implementation strategy, the principle is included in several recommendations for public administrations stating goals such as:

---

[122] 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 the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation or hereinafter: GDPR) (Text with EEA relevance) OJ L 119, 4.5.2016, pp. 1–88.

[123] European Commission. 'New European Interoperability Framework Promoting seamless services and data flows for European public administrations' (2017), p. 14. <doi:10.2799/78681> or <https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf> accessed 24 November 2020.

(i) "Do not impose any technological solutions on citizens, businesses and other administrations that are technology-specific or disproportionate to their real needs"
(ii) "Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evaluation of European public services without unjustified restrictions, if legally possible."
(iii) "Actively participate in standardisation work relevant to your needs to ensure your requirements are met."

The author argues that considering the stated aim and subjects of the principle, the principle of technology neutrality can be defined also using the principles of equality of treatment, non-discrimination and transparency that are elementary to public procurement processes. The aim of these named principles in the public procurement procedure is to secure that the state in purchasing goods and services is not favouring a particular technology neither as an object for purchase or in the procedure of procurement. The said principles are included in many recitals and articles of Directive 2014/24/EU[124] in relation to public contracts, tenders and rules of procedure. These clauses promote the idea that contracts by the regulator should be awarded on the basis of objective criteria and should not prefer a technology or a tenderer. The aim of technology neutrality principle is best explained in Recital 74 of the said Directive that states:

> "The technical specifications drawn up by public purchasers need to allow public procurement to be open to competition as well as to achieve objectives of sustainability. To that end, it should be possible to submit tenders that reflect the diversity of technical solutions standards and technical specifications in the marketplace, including those drawn up on the basis of performance criteria linked to the life cycle and the sustainability of the production process of the works, supplies and services.
>
> Consequently, technical specifications should be drafted in such a way as to avoid artificially narrowing down competition through requirements that favour a specific economic operator by mirroring key characteristics of the supplies, services or works habitually offered by that economic operator. Drawing up the technical specifications in terms of functional and performance requirements generally allows that objective to be achieved in the best way possible. Functional and performance-related requirements are also appropriate means to favour innovation in public procurement and should be used as widely as possible."

As said the principle stems from the offline-online treatment equivalence, consequently, the principle is recognizable also through medium- or form equiv-

[124] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance OJ L 94, 28.3.2014, p. 65–242.

alence of offline and online contexts regulated by the Software Directive[125] and Infosoc Directive[126] extending regulation to any form. More specifically Recital 5 of the InfoSoc Directive states that:

> "Technological development has multiplied and diversified the vectors for creation, production and exploitation. While no new concepts for the protection of intellectual property are needed, the current law on copyright and related rights should be adapted and supplemented to respond adequately to economic realities such as new forms of exploitation."

The principle is not specifically stated but present in Article 4 of the Infosoc Directive that treats the rights of the authors in relation to distribution equivalently irrelevant of the form stating that "Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit *any form* of distribution to the public by sale or otherwise." The same extension is included in the Article 4 of the Software Directive granting "the exclusive rights of the rightholder within the meaning of Article 2 (c) shall include the right to do or to authorise *any form* of distribution to the public". Furthermore, according to Recital 7 of the same Directive, "the term 'computer program' shall include programs in any form, including those which are incorporated into hardware. This term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage."[127]

Also in the new MiCA Proposal introduced in late 2020 it was stated that its goal is to ensure "that the EU financial services regulatory framework is innovation-friendly and does not pose obstacles to the application of new technologies",[128] while identifying the specific object of said regulation as "removing regulatory obstacles to the issuance, trading and post-trading of crypto-assets that qualify as financial instruments, while respecting the principle of technological

[125] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ 2009 L 111 (hereinafter: Software Directive), p. 16.

[126] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society
OJ L 167, 22.6.2001, p. 10–19

[127] To clarify this point further as stated in Recital 11 of the Software Directive "In accordance with this principle of copyright, to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive. In accordance with the legislation and case-law of the Member States and the international copyright conventions, the expression of those ideas and principles is to be protected by copyright." This means that the form must be interpreted in this case as any objective expression.

[128] MiCA Proposal (n.42), p.1.

neutrality".[129] More specifically, recital 6 of the MiCA Proposal reiterates that "Union legislation on financial services should not favour one particular technology." Lastly, the same Recital also clearly aims for preferring or presuming the use of DLT by stating that, "crypto-assets that qualify as 'financial instruments' as defined in Article 4(1) point (15) of Directive 2014/65/EU should therefore remain regulated under the general existing Union legislation, including Directive 2014/65/EU, regardless of the technology used for their issuance or their transfer."

Furthermore, in addition to MiCA Proposal also the Pilot Regime as part of the Digital Finance Package in the EU is straight-forward about the fact that "the EU follows the principle of technological neutrality, but rules are still created based on market realities."[130] This means that some of the existing regulation "sometimes restricts and even prevents the use of DLT".[131] Furthermore, Recital 1 of the Pilot Regime states that the regulation is aimed at contributing to a future-ready economy and regulation that is fit for the digital age.

In summary, the overview of the origins herein shows that the principle has been historically used in regulation aimed for information and communication technology (ICT) sector – Framework Directive, Better Regulation Directive, NIS Directive – however, the idea of equal treatment of online-offline or physical-digital is later conveyed also by more fundamental digital commerce regulation such as eCommerce, InfoSoc and Software Directive. Furthermore, the idea, aim and content of the principle is unmistakably recognizable in public procurement regulation through the use of the principles of equality of treatment, non-discrimination and transparency. These are all the same values that are recognized also part of the technology neutrality principle and therefore, the use of these principles in public procurement can be used to understand the expectations the technology neutrality principle creates for the regulators in relation to regulation. The placing of the principle among the values that need to be respected in establishing guidelines for the public sector in creating interoperability shows that whereever public sector is making decisions that could influence the use of technology – neutrality should be respected. Lastly, the clear use of the principle as a goal and value in GDPR and the references to it as the aim of the EU in introducing MiCA Proposal and Pilot Regime for the finance sector clearly indicate that digital society has expanded the use and value of the principle in a way that it can no longer be considered as a principle for the ICT sector. As technology has infiltrated also other sectors, such dissemination has brought the principle to all these other sectors that are transformed by technology and consequently, also the principle should be recognized more widely.

[129] MiCA Proposal (n. 42), p. 145 and 146.

[130] Pilot Regime (n. 38), p. 4.

[131] Pilot Regime (n. 38), p. 4.

2.5 The meaning of the principle

As discussed in Article I,[132] the principle of technology neutrality consists of different categories of equivalence:

> **Functional equivalence** aims to ensure that the regulator should not discriminate between different technology or domains (e.g., offline and online domains) in case these domains or technologies are able to perform equivalent functions or even merely reach similar objectives with the performance of different functions. It is the position of Van der Haar[133] that the utility aspect should also be part of the functional equivalence, who has explained the principle through denominated consumer certainty rational, or the "natural person's perspective", that if the services or goods are considered by the consumer as interchangeable, these services should enjoy equivalence of outcome and not be treated differently. In the DLT context, this means that, if cryptocurrencies are used by the consumer as fiat currency, these should be regarded as interchangeable and the effects equivalence of the regulation should be enjoyed. The author proposes that part of the functional equivalence is also the utility of the technology, meaning that if technology is used equivalently while not having similar functions, this should persuade the regulator to treat the technologies equivalently or, in other words, grant these technologies effects equivalence.
>
> **Effects equivalence**[134] aims for the regulation to have a substantively equivalent effect across technologies, even if the regulation addressing different domains or technologies is specifically and exclusively created for a single domain or technology (according to Reed this is referred to as "implementation neutrality"[135]). The effects equivalence is therefore related to the consequences of regulation. It is at times also referred to as equivalence of outcome, e.g., the effect of a signature in offline and online domains has equivalent consequences as to its binding force or validity.

In other words, if the technology performs equivalent functions and has equivalent utility, it should also enjoy the effects equivalence under regulation. The author elaborates on these concepts in the following section.

---

[132] Veerpalu (n. 86), p. 78.

[133] I. M. Van der Haar, 'The principle technological neutrality: connecting EC network and content regulation' (2008), <https://pure.uvt.nl/ws/portalfiles/portal/1063437/3240352.pdf> accessed 3 March 2019.

[134] The effects equivalence is consistent with CJEU case law on the issue, namely that "the requirement of strict interpretation does not mean that the terms used to specify the exemptions referred to in Article 135(1) must be construed in such a way as to deprive the exemptions of their effect (see, inter alia, judgments in *Don Bosco Onroerend Goed*, C-461/08, EU:C:2009:722, paragraph 25; *DTZ Zadelhoff*, C-259/11, EU:C:2012:423, paragraph 21; and *J.J. Komen en Zonen Beheer Heerhugowaard*, C-326/11, EU:C:2012:461, paragraph 20)." Quoted in *Hedqvist*, para. 35.

[135] Reed (n. 100), p. 264.

2.5.1 Functional equivalence

Some authors argue that functional equivalence is a generally accepted principle of law-making[136] and can be regarded as one of the main regulation methods in information technology in the EU.[137] Although, often confused as one and the same, technology neutrality and functional equivalence are not with the same scope. This is due to functional equivalence being rather a starting point of the technology neutrality principle. [138] This means that these principles partly overlap but do not carry the same weight or scope. According to some scholars the principles can be separated because functional equivalence is the guiding principle as to equality in treatment as a principle of law which should apply to any new behaviour, and the principle of technology neutrality should be the basis for "the choice between the available substantive rules which could be used to implement those legal principles".[139] Such distinction is especially relevant in case of convergence of markets and disruption of one sector by the stakeholders of another sector (e.g., ecommerce startups disrupting financial sector.)

The aim of the equivalence is to secure legal recognition for the functionally equivalent electronic form outputs – electronic transactions and registries, signatures and data – as for paper-format outputs in order to ensure that the difference in the medium of the transaction, registry, signature or data did not affect the legal effect in a negative way.[140] However, the functions the electronic signature must meet in order to have equal weight and validity are very different from those applied to paper-based signatures.

The difficult part here is the identification of what can be considered functionally equivalent. For this purpose, using the example of electronic form, "an examination of the function fulfilled by traditional form requirements ('writing', 'signature', 'original', 'dispatch' and 'receipt') and a determination as to how the same function could be transposed, reproduced or imitated in a dematerialised environment"[141] is needed. Using the UNCITRAL example in developing the Model Law on Electronic Signatures[142] (MLES), the determination of these features followed these steps (also referred to as functional analysis):

- an analysis of the requirements applied to paper-based signatures;
- identification of the purposes and objectives of these requirements; and
- an analysis of the functions of the novel system.

---

136 Reed (n. 60), p. 248.

137 Savin (n. 63), p. 5.

138 Koops (n. 59).

139 Reed (n. 60), p. 249.

140 Harvey (n. 64).

141 ibid, p. 60.

142 UNCITRAL Model Law on Electronic Signatures, (5 July 2001). <https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures> accessed 02 May 2020.

Only after such functional analysis is it possible to determine whether effects equivalence (such as binding force and validity) can be granted to the novel system.[143]

Furthermore, functional equivalence can be also recognized in the functional method used in comparative legal theory that is used to understand regulation in other jurisdictions. The method is used to compare the unknown with the known by decomposing the unknown into functions and institutions that perform these functions. This comparative functional method brings us back to the concept of functional equivalence that as already discussed suggests that "similar functional needs [of society] can be fulfilled by different institutions . . . .".[144] As explained by Ralf Michaels:

> "The functional method asks us to understand legal institutions not as doctrinal constructs but as societal responses to problems – not as isolated instances but in their relation to the whole legal system, and beyond, to the whole of society."[145]

The functional method in comparative law bears a lot of similarities to functional equivalence – the comparisons undertaken inspect the functions and purposes of the functions of the foreign system aiming to identify the functionally equivalent purpose of function instead of comparing merely legal institutions and architecture. The functional method of comparativists starts off by asking the question "what social problem a certain legal institution seeks to resolve"[146] without basing the investigation on concepts known to the person conducting the comparison on the basis of the legal system they know but instead investigate the solution on "purely functional terms."[147] Thereon, the comparativist would investigate the foreign system to identify the corresponding legal institution that also resolves the same social problem identified. By setting aside the perceptions of the known legal concepts, purposes or functions and legal institutions the comparative theorist can understand what makes law work in the foreign legal system and not only how it differs from the existing known legal system. Such method allows the

---

[143] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998. <http://www.uncitral.org/pdf/english/texts/electcom/V1504118_Ebook.pdf> accessed 28 November 2019.

[144] Reyes, Carla, Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal (April 18, 2016). *Villanova Law Review*, Vol. 61, No. 1, 2016, p. 224. Stetson University College of Law Research Paper no. 2016-8, <https://ssrn.com/abstract=2766705> accessed 8 March 2021.

[145] Ralf Michaels, The Functional Method of Comparative Law, in THE OXFORD HANDBOOK OF COMPARATIVE LAW 339, 357 (Mathias Reimann & Reinhard Zimmermann eds., 2006) quoted in Reyes, Carla, Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal (April 18, 2016). *Villanova Law Review*, Vol. 61, No. 1, 2016, p. 224. Stetson University College of Law Research Paper no. 2016-8, <https://ssrn.com/abstract=2766705> accessed 8 March 2021.

[146] Reyes (n. 145), p. 225.

[147] ibid.

comparative theorists to acknowledge and accept "reasonable substitutes" to the known legal reality. Similar logic is applied also under the functional equivalence principle.

2.5.2 Effects equivalence

While functional equivalence is identified on the basis of the functions, outputs and utility of the new technology in comparison to the pre-existing ones, effects equivalence has to do with the existing regulation and the treatment of these under the regulation. Simply worded, effects equivalence is the treatment the innovator may demand from the regulator in case functional equivalence is already established under functional analysis. This is supported by the statement that, "if the effects of a technology are regulated rather than the technology itself, the regulation will usually establish functional equivalence between [these] technologies".[148] This means that effects equivalence deals only with the consequences of using the new technology and its outputs or processes. The effects equivalence question often deals with treatment – are these goods treated equivalently to the way functionally equivalent goods are treated?

Using DLT as an example, as discussed in Article III, in the case that DLT-based smart contracts are qualified as functionally equivalent to electronic contracts, the treatment as to the validity of the contract needs to be equivalent. The effects might differ due to differences in functions, but in order to be in line with the principle of technology neutrality, all the differences in treatment must be non-discriminatory, transparent and neutral in their effect.

Finally, if regulation makes the use of the innovative solution more onerous or potentially less effective than the pre-existing technology, no effects equivalence has been granted by regulation and there is discrimination against the innovative solution. The same aspects are discussed in Article I – if cryptocurrencies and fiat currencies are identified as functionally equivalent (like bitcoin and legal tender in *Hedqvist),* effects equivalence must be granted in the tax treatment of these outputs. Furthermore, if the compliance requirements under anti-money laundering regulation for these outputs prove to be more onerous for cryptocurrencies than for fiat currencies, no effects equivalence is granted and, in order to be in line with the technology neutrality principle, the regulator must justify such difference in treatment on the basis of neutral, transparent and non-discriminatory reasons.

[148] Koops (n. 59), p. 7.

2.6 Sustainability

According to Reed, sustainability of regulation is one of the most cited values of the technology neutrality principle.[149] The principle aims for the regulation to be flexible enough so as not to hinder technological innovation and to guarantee a certain level of legal certainty not requiring constant change and uncertainty.

Sustainability requires the regulator to draft regulation in such a way that it is flexible enough to not impede on any future development or application of technology. Sustainability should ensure that regulation allows innovation without needing over-burdensome regulatory amendments or constant revision to facilitate fast-paced technological change.

In line with the sustainability aim, the Digital Finance Strategy[150] communicated by the EU Commission also stated as that one of its aims is to "ensure that the Union's financial services legislation is fit for the digital age and contributes to a future-ready economy that works for the people, including by enabling the use of innovative technologies", which is also repeated in Recital 1 of the MiCA Proposal. However, this does not mean that the regulation can merely remain the same whatever the change in technology. EU regulators are often motivated to subject the innovative solution to the existing regulation due to fear of the impact on the market, consumers, the environment or their own potential control over it.[151] The obvious question market incumbents have in such a case is: the disruptors are disrupting the market the incumbents have built (and dominate), so how is it possible for the innovator to operate on the same market without being subjected to the same regulation? Consequently, the incumbents lobby to apply existing regulation to the disruptors business model no matter the differences in the technology, business or infrastructural model used. This is not what sustainability means. Sustainability, while still ensuring technology neutrality, means that the regulator must investigate new technology and ensure neutrality of regulation either through implementation or adaptation of its interpretation even if the regulation remains the same.

Additionally, it is not easy for regulators to let existing regulation expire and be repealed simply due to innovation. This is understandable, as the regulators have put a lot of effort into building the regulation and, thereafter, building the relevant case law. Not to mention the fact that the creation of a new regulatory framework is not an easy task for any regulator, especially considering that regulation is often needed for a domain, technology or infrastructure that the regulator does not understand or the effects of which have not been realized to a substantial level.

Instead, in accordance with the subsidiarity principle, the sustainability value of the neutrality principle requires that the higher the specific legal act is in the

---

[149] Reed (n. 62), p. 196.

[150] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for EU COM(2020)591.

[151] Savin (n. 63).

hierarchy of legal acts, the more sustainable and abstract its legal norms must be. Such legal norms are accompanied by the less sustainable and gap-filling guidelines, standards, etc. in the lower level.[152] On the basis of the sustainability value, Koops claims that the regulatory framework should promote certain substantive principles (such as fundamental values[153] and rights) that are important from the point of view of the regulator "rather than put all effort into creating specific regulations for specific problems."[154] At the same time, it must be considered that the more abstract the regulation is, the less certain the regulation subjects are of the outcome of its application in a specific use case. At the same time, the more abstract the regulation is, the more sustainable it becomes. Sustainability is also sometimes referred to as "future-proofing of regulation" and "statutory longevity".[155] The neutral wording of regulation aims to achieve this so-called future-proof, sustainable or, in other words, foresight regulation. However, foresight regulation often tends to be vague and therefore creates legal uncertainty, as the subject of the regulation is unable to predict the effect of the regulation on a new set of facts and consequently, the regulation becomes non-transparent. An example of this is the long-standing confusion related to the term 'stored on electronic device' in the context of electronic money under the e-Money Directive.[156] Does 'stored on electronic device' include a smart card or an electronic wallet on the user's computer, a loyalty card or a mobile application, etc? Is the term 'device' in this context future-proof?[157] Therefore, according to some scholars, foresight regulation is not possible at all,[158] as technology advances so quickly and so unpredictably that applying existing regulation will always bring unforeseeable consequences, such as limiting the use and depriving the innovative solution of its benefits. Additionally, according to Bennett Moses,[159] language is unable to achieve technology neutrality as, in order to draft

---

[152] Koops (n. 59).

[153] The same was indicated by the Commission communication of 2016 as one of the principles to develop the legal framework for online platforms (European Commission, 'Online Platforms, and the Digital Single Market', (Communication, 25.5.2016 COM(2016) 288 final), p. 5. <https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF> accessed 22 July 2019.

[154] Koops (n. 59), p. 25.

[155] Brad A. Greenberg, 'Rethinking Technology Neutrality', (2016) Minnesota Law Review 100, p. 1495.

[156] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance) OJ L 267, 10.10.2009, p. 7–17.

[157] Reed (n. 100), p. 281.

[158] Daniel J. Gervais, 'Towards a new core international copyright norm: the reverse three-step test', (2005) Marquette International Property Law Review 9. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=499924> accessed 27 November 2019.

[159] Lyria Bennett Moses, 'Understanding legal responses to technological change: the example of in vitro fertilization', (2005) Minnesota Journal of Law, Science and Technology,

regulation with legal certainty, language uses existing terminology tied to the present technological reality.

2.7 The principle of technology neutrality in Estonian law

The principle of technology neutrality is included also in the national laws of EU Member States and has been similarly included in the national laws of Estonia. The predominant source for the principle in Estonian law is the Estonian Electronic Communications Act (ECA).[160] The principle is already described in § 1 of the ECA through the purpose of the act that is stated as

> "to create the necessary conditions for the development of electronic communications to promote the development of electronic communications networks and electronic communications services without giving preference to specific technologies and to ensure the protection of the interests of users of electronic communications services by promoting free competition and the purposeful and just planning, allocation and use of radio frequencies and numbering."

The principle can also be recognized in the wording of § 6 section 2 of ECA that stresses that the specific purpose of regulating the management of radio frequencies is the need to "ensure the purposeful, objective, transparent and proportionate management, and the effective and efficient use of radio frequencies" also in order to create possibilities "for the development of new technologies". Furthermore, without specifically mentioning of the principle, the aim of the principle is stated in § 28 section 2 of ECA stating that "the Minister of Economic Affairs and Communications and the Consumer Protection and Technical Regulatory Authority shall manage the numbering resources on the basis of objective, transparent, non-discriminatory and proportionate criteria, taking account of the need to achieve harmonised, efficient and effective use of numbering."

§ 40 section 1 of ECA states as "the purpose of the sector-specific regulation of markets of communications services (hereinafter market) is to ensure the pluralism of communications service providers, their equal and non-discriminatory treatment by encouraging competition, and the quality and availability to end-users of the provided services" and in section 3 of the same paragraph "the sector-specific regulation of markets must be technologically neutral". In the opinion of the author separating technology-neutrality into a different section of the legal norm while the meaning of the principle is already explained in section 1 shows that the meaning of the principle was empty to the regulator and the term

6/2. <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1337&context=mjlst> accessed 28 November 2018.

[160] Electronic Communications Act [*elektroonilise side seadus]* – RT I 2004, 87, 593; RT I, 20.05.2020, 34.

"technologically neutral" is used to meet the expectation to use this term, while understanding the meaning of this term is uncertain.

Additionally, § 134 section 4 of ECA stipulates the objectives of state organisation of the electronic communications sector by explaining the principle of technology neutrality with specific components without again naming the principle. The section reiterates that the state organisation of electronic communications sector must be pursued on the basis of objective, transparent, non-discriminatory and proportionate regulatory principles, among other things, the following:

- "the promotion of foreseeability of regulation by ensuring uniform regulatory approach also after regulatory amendments;
- the ensuring of equal and non-discriminatory treatment of communications undertakings;
- the promotion of infrastructure-based competition;
- the promotion of investment in communications networks and other units of electronic communications infrastructure, the supporting of innovation and the protection of investments."

The author finds this § 134 section 4 of ECA as the clearest description in Estonian law of the components and aims of the technology neutrality principle.

In addition to ECA, the principle is recognizable (though not mentioned) also in §§ 14, 17, 21 and 29 of the Personal Data Protection Act[161] that states a general obligation of the controller of personal data to implement legal and technological measures which enable to fulfill the obligations of the act. The Personal Data Protection Act does not mention the technology neutrality goal or principle specifically nor mention any of its components stated in ECA.

Lastly, the author concludes that the principle is through its components represented also in other legal acts in Estonia that limit or guide the regulator, such as § 22 section 1 of the Product Conformity Act[162] under which the "conformity assessment bodies perform their functions in a competent, transparent, impartial, independent, non-discriminating and proportionate manner and follow the requirements established for the conformity assessment of specific products" or Public Procurement Act[163] that aims "to ensure the transparent, practical and economic use of the contracting authority's or the contracting entity's funds, equal treatment of persons, and effective use of competition in public procurement".[164]

---

[161] Personal Data Protection Act [*isikuandmete kaitse seadus]* – RT I, 04.01.2019, 11.

[162] Product Conformity Act [*toote nõuetele vastavuse seadus*) – RT I 2010, 31, 157; RT I, 30.06.2020, 23.

[163] Public Procurement Act [*riigihangete seadus]* – RT I, 01.07.2017, 1; RT I, 08.07.2020, 8.

[164] § 2 (1) of Public Procurement Act.

By far the most case law on the content of the principle has been generated on the basis of public procurement disputes.[165] Through reference to Public Procurement Act § 88 section 7, Articles 42(2), 18 (1) and Recital 74 of 2014/24/EU Directive the principle and its sub-principle of functional equivalence are at lengths discussed in Estonian Supreme Court case 3-20-718, nevertheless, still unmentioned by their titles.[166]

2.8 CJEU case law

Most CJEU cases that mention technology neutrality or functional equivalence are dealing with electronic communication,[167] broadcasting[168] or broadcasters.[169] Nevertheless, the principle is present, though not mentioned, also in other types of disputes as discussed below. In *European Commission, European Parliament v Council of the European Union*, [170] technology neutrality was discussed in the context of the meaning of the "broadcasting organisation" to include broadcasters "regardless of whether, in the context of new digital technologies, the reference to broadcasts transmitted by wire or over the air". The principle was applied on the basis of the Framework Directive for example in *Belgacom SA v Belgium*[171] to fees charged for radio frequencies from the mobile telephone operators where the court stated the fees must be "objectively justified, transparent, non-discriminatory and proportionate in relation to their intended purpose and take into account the objectives of" the technology neutrality principle. In *Comunidad Autónoma del País Vasco, Itelazpi SA*[172] the court supported the European

---

[165] See Supreme Court Administrative Law Chamber (hereinafter SCALC) judgment, 5th November 2020, case 3-20-718/28; SCALC judgment, 4th November 2020, case 3-20-924/24; SCALC judgment, 6th March 2014, case 3-3-1-13-12, SCALC judgment 12th October 2011, case 3-3-1-31-11, SLALC judgment, 27th October 2010, case 3-3-1-66-10, etc.

[166] 3-20-718, p. 15 and 17.

[167] *Belgacom SA and Others v État belge*, CJEU Case C-375/11 (Judgment of the Court (Fourth Chamber) of 21 March 2013).

[168] *Comunidad Autónoma del País Vasco, Itelazpi SA (C-66/16 P), Comunidad Autónoma de Cataluña, Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI) (C-67/16 P), Navarra de Servicios y Tecnologías SA (C-68/16 P), Cellnex Telecom SA, formerly Abertis Telecom SA, Retevisión I SA (C69/16 P) v European Commission, SES Astra SA* Joined CJEU Cases C-66/16 P to C-69/16 P and Cases C-70/16 P and C-81/16 P, (Judgment of the Court (Fourth Chamber) of 20 December 2017).

[169] *European Commission, European Parliament v Council of the European Union*, CJEU C-114/12 (Judgment of the Court (Grand Chamber) of 4 September 2014). Technology neutrality was discussed in the context of the meaning of the "broadcasting organisation" to include broadcasters "regardless of whether, in the context of new digital technologies, the reference to broadcasts transmitted by wire or over the air". CJEU C-114/12, Para 87.

[170] ibid.

[171] *Belgacom SA and Others v État belge*, CJEU Case C-375/11.

[172] *Comunidad Autónoma del País Vasco, Itelazpi SA,* CJEU Case C-66/16 P.

Commission in the conclusion that granting state aid to digital terrestrial television operators in order to switch over from analogue television to digital is not in accordance with the principle of technology neutrality, insofar as the state aid excludes other technology provider such as satellite service providers.

As stated in section 2.5 above the author finds that the principle can also be explained through the use of the principles of transparency, equal treatment and non-discrimination used in public procurement. This is especially so concerning "technical specifications, in the light of the risks of discrimination related either to the choice of specifications or their formulation".[173] Furthermore, "complying with those requirements is all the more important when […] the technical specifications listed in the procurement documents are formulated in a particularly detailed manner. Indeed, the more detailed the technical specifications, the higher the risk of favouring the products of a given manufacturer will be."[174] Furthermore, according to CJEU it is required that "the level of detail of the technical specifications complies with the principle of proportionality".[175] These cases assist to understand what non-favouring of certain technology means and how to interpret these principles.

The examples of CJEU case law show that functional equivalence is often raised in the case of how goods and services of different forms, such as physical versus digital, are compared. Given that the principle was developed for the equal treatment of these two media, the principle is of the utmost relevance in relation to digital goods[176] and the Digital Single Market (DSM). In *eDate Advertising,*[177] the court treated paper-based – and online media equivalently, specifically identifying the equivalence of publication and the distribution of a newspaper (paper-based medium) and a publication online "by means of the Internet" (online medium). The dispute was related to eCommerce directive and the court reinforced that the free movement of services applies equally to electronic commerce services and non-electronic services. Furthermore, the court also reiterated that the right to initiate proceedings against such service providers should also not be subject to stricter rules than those for non-electronic commerce services.

However, the equivalent treatment of these categories is not relevant only from the point of view of the simple treatment of the category but also from the

---

[173] *Commission v Netherlands*, CJEU Case C-368/10, paragraph 62.

[174] *Roche Lietuva' UAB v Kauno Dainavos poliklinika VšĮ,* CJEU Case C-413/17*,* para 37.

[175] ibid*,* para 41.

[176] Janja Hojnik defines digital goods as "a broad and rapidly expanding term in view of the variety of 'goods' actually covered, referring to all goods that are stored, delivered and used in its electronic format, such as smartphone applications, digital music and books, computer design files for 3D printed products, for instance houses, medical devices and food". Janja Hojnik, "Technology neutral EU law: digital goods within the traditional good/services distinction", *International Journal of Law and Information Technology*, (2017) 25:63-84 (92) and :71. <DOI: 10.1093/ijlit/eaw009> accessed 29 April 2020.

[177] *eDate Advertising GmbH and Others v X and Société MGN Limited* CJEU Joined Cases C-509/09 and C-161/10.

point of view of taxation. On the basis of the principle of fiscal neutrality that "precludes similar goods or supplies of services, which compete with one another, from being treated differently for VAT purposes"[178] discussed in *Commission v Germany,*[179] functionally equivalent goods also need to be taxed similarly for the purposes of competition and equal treatment.

However, although the technology neutrality principle dictates that digital goods, though distinctly different from physical goods, should be treated equally, not all directives and consequently, also case law of the CJEU on these different media is that consistent with this idea. While, regarding software as reinforced in the *UsedSoft* case[180], the Software Directive treated downloaded software equally with software on a material medium (e.g., CD-ROM or DVD) [181] under the Software Directive, e-books – as the digital version of printed books – were at times treated differently. The rulings of *Commission v Luxembourg and France*,[182] *Allposters*,[183] *Darmstadt*,[184] *VOB v Stichting Leenrecht*[185] and recently *Tom Kabinet*[186] show that the court is inconsistent as to whether different media of a book should be treated equally or differently. In the *Tom Kabinet* case,[187] the court regarded it inappropriate to apply the *UsedSoft* logic to e-books, as these are not software, nor are they functionally equivalent to physical books. The court regarded the Software Directive as *lex specialis* from InfoSoc Directive and reasoned that, although the aim of the Software Directive was to treat "tangible and intangible copies of computer programs"[188] equivalently, it was not the aim of the InfoSoc Directive.

In order to treat e-books differently, the CJEU qualified these goods as functionally different and identified a limitation to the principle of technology neutrality. For example, the court stated in the *UsedSoft* case:

---

[178] *Adam* CJEU Case C-267/99, para 36. *Commission of the European Communities v Federal Republic of Germany*, CJEU Case C 109/02, para 11.

[179] *Commission of the European Communities v Federal Republic of Germany*, CJEU Case C 109/02, para 20.

[180] ibid, para 47.

[181] *UsedSoft GmbH v Oracle International Corp,* CJEU Case C 128-2 (hereinafter: *UsedSoft*).

[182] *European Commission v French Republic*, CJEU Cases C-479/13 and *European Commission v Grand Duchy of Luxembourg*, CJEU Case C-502/13.

[183] *Art & Allposters International BV v Stichting Pictoright* Request for a preliminary ruling from the Hoge Raad der Nederlanden, CJEU Case C-419/13.

[184] *Technische Universität Darmstadt v Eugen Ulmer KG,* CJEU Case C-117/13.

[185] Advocate General's Opinion of 16 June 2016 in *Vereniging Openbare Bibliotheken v Stichting Leenrecht* Request for a preliminary ruling from the Rechtbank Den Haag, CJEU Case C-174/15.

[186] *Nederlands Uitgeversverbond, Groep Algemene Uitgevers v Tom Kabinet Internet BV, Tom Kabinet Holding BV, Tom Kabinet Uitgeverij BV*, CJEU case C-263/18 (hereinafter: *Tom Kabinet*).

[187] *Tom Kabinet*.

[188] *Tom Kabinet*.

> "the sale of a computer program on a material medium and the sale of a computer program by downloading from the internet are similar, since the online transmission method is the functional equivalent of the supply of a material medium. Accordingly, interpreting Article 4(2) of Directive 2009/24 in the light of the principle of equal treatment justifies the two methods of transmission being treated in a similar manner."[189]

Hence, the CJEU separated the content layer and the transport layer of the technology and established that there is no difference in the product itself (the content layer) even though its transport layer is different. However, in the *Tom Kabinet* case, the court stated:

> "the supply of a book on a material medium and the supply of an e-book cannot, however, be considered equivalent from an economic and functional point of view. As [...] dematerialised digital copies, unlike books on a material medium, do not deteriorate with use, and used copies are therefore perfect substitutes for new copies. [190]

As can be seen, the court analyses the goods functionally and separates the transport layer from the content layer (e.g., the difference of supply), and the different utility aspect of the e-book is that it does not deteriorate with use and used copies are perfect substitutes for new copies. Those characteristics can also be regarded as functions of the e-book's delivery process and, therefore, this process comes with a different bundle of rights for the e-book itself under Article 3 of the InfoSoc Directive that are not the same as the rights attached to printed books.

Interestingly, also in the *UsedSoft* case, downloadable software has different delivery processes, but the Software Directive does not separate these bundles of rights in an equivalent way. Consequently, the core difference of online – and offline media – the fact that digital medium does not deteriorate with use as it does not have a materialised component – is a cause to treat the delivery process and hence, the good itself differently and, consequently, the relationship of use might change from distribution to mere communication to the public. Therefore, such differences in treatment might limit the principle of technology neutrality due to difference in functions that justifies difference in treatment.

The court also pointed to the reason for the justification of such difference: "a parallel second-hand market would be likely to affect the interests of the copyright holders in obtaining an appropriate reward for their works much more than the market for second-hand tangible objects". [191] This point is more related to the economic point of view than the functional, as there are plenty of material goods which actually increase in value over time or with use (furniture, art, vintage goods, etc.) and also these are later sold on the second-hand market along with

[189] ibid, para. 57.

[190] ibid, para. 59.

[191] ibid.

the originals to the detriment of the copyright holders attempting to sell originals of the same. The issue is that these two cases are based on the application of two different directives. Under the InfoSoc Directive, there appears to be a limitation to the principle of technology neutrality due to the economic interests of the copyright owner and that limitation devalues the scope of rights of the user for the benefit of the copyright holder. In a way, this means that because technology has advanced to a level that allows the publisher of the book to control access to the electronic version of the book indefinitely than as stated by the court, the assets and features of the new technology have consequently altered the rights attached to the digital good. This in turn has changed the relationship of use of this digital good for the benefit of the copyright holder. This is a direct consequence of technology use as due to technology there is no deterioration of the e-book upon use. Legally, therefore, the court argues that no sale is taking place, as all the copyright holder is doing is communicating the e-book to the public and consequently, no exhaustion of distribution right takes place.

The *Tom Kabinet* case ruling, and the respective InfoSoc Directive interpretation show, that, upon advancing technology, the scope of rights that was limited due to constraints in the physical world can be expanded or changed. This means that the choice to expand these scopes is directly related to technological possibilities and capabilities. This is an additional limitation of the technology neutrality principle: when technology advances and the contextual changes take place, the rights and liberties of individuals might also expand or change. This aspect does not carry the preference of a regulator for one technology over another, but merely grants the electronic version of the category – such as e-books – a higher level of exclusive control by the copyright holder.

DLT in essence also has capabilities to advance the control of the copyright holder (mostly directly the author) and there are a number of solutions built on DLT, such as Scenarex's product book chain,[192] that allow authors to forego publishers and sell, resell and lend their e-books without involving the technology heavy solution of a third party publisher. This allows the author themselves to earn directly from the distribution and decide whether the smart contract governing the sale, resale and lending should allow for the expansion of absolute right like in *Tom Kabinet's* case or instead allow for ownership and resale option for the buyer of the e-book while granting the author the right to earn through the execution of the smart contract on all following resales of the respective e-book. Another example of a DLT-based publishing solution is Publica's[193] product Book ICO, which allows funds for writing the book to be raised and, consequently, copies of the book to be sold prior to it being written.

[192] Scenarex website. <https://www.scenarex.ca/en/bookchain/> accessed 16 November 2020.

[193] Publica website. <https://publica.com/> accessed 16 November 2020.

2.9 Critique

In addition to the pessimism around the sustainability goal of the principle as described in the section 2.6 above, there are other reasons why the principle is difficult to apply and follow in practice. Reed has stated that, even though the principle is not clearly understood by regulators, the validity and priority of the principle is rarely questioned.[194]

The critique of the principle presented herein is not only related to its limitations but also to the difficulties in its application and the guidance the regulator is able to obtain from the principle. This critique can be divided into several categories, such as (i) contextual changes and convergence of technologies; (ii) failure to understand the technology; and (iii) undesired consequences such as vagueness, as further discussed below.

2.9.1 Contextual changes and convergence of technology

Due to the advancement of technology, the context of the market and society changes constantly and, at times, leads existing regulation to become unfit in the changed context. This was also discussed in the work of Kamecke and Körber as presented above – the aim of the principle is to curb regulators from extending existing regulation to the changed context. Chris Reed presents the example of a publisher in the online domain in comparison to the offline domain as an example of this type of contextual changes.[195] The publisher in offline media has systematic control over content ("media under editorial control"[196]), but in the online domain, control by a hosting service provider is less systematic due to the mere abundance of content posted by users. Hence, the regulation differentiates the treatment of these publishers and introduces different regulation for these domains.[197] The same challenge arose in case of telecommunications services and OTT services[198] where the market changed dramatically as technologies converged from simply traditional telecommunications services into vastly different services. This type of convergence challenges the regulator to treat the outcome of utility-

---

194 Reed (n. 100), p. 264.

195 Reed (n. 100), p. 264.

196 Savin (n. 63).

197 Article 14 of e-Commerce Directive.

198 Andrej Savin uses a simplified definition for these services by characterizing them as "media companies that distribute content and services (VoIP, instant messaging, streaming, etc.) through the Internet rather than other proprietary channels." Andrej Savin. 'EU Regulatory Models for Platforms on the Content and Carrier Layers: Convergence and Changing Policy Patterns' (November 14, 2018). The Nordic Journal of Commercial law, 1/2018, Copenhagen Business School, CBS LAW Research Paper No. 19-08, p. 22. <https://ssrn.com/abstract=3284434> accessed 14 November 2020.

198 Reed, (n. 100), p. 278.

wide equivalent services (such as telephone services and VoiP) differently[199] and makes it difficult to understand how new regulation should be developed in order for it to be technology neutral.[200]

This is especially relevant in relation to social media and search engines, such as Google, Facebook and Twitter, which have become the "primary distributors of news content"[201] and through this control of news content delivery they also control the majority of all digital advertising budgets.[202] However, the extension of the "media under editorial control" regulation to social media and platforms on the basis of the functional equivalence sub-principle is uncalled for precisely because of the contextual differences.[203] Instead, these OTT service providers are subject to a "significantly simpler and less onerous regime"[204] known as internet society services (ISSs) regulation. Due to this, the incumbents of the market might not appreciate neutrality and merely identify the difference in the treatment of these service providers.[205]

Furthermore, as suggested by Savin, the EU's platform regulation is also the result of technological convergence bringing about different organizations (the platforms) on the markets for obtaining information, data, goods and services.[206] This means that the shift in the context, the roles of participants, the services these participants provide and the infrastructure they use in order to provide these could result in existing regulation being unfit to address the new market and an adaptation is called for. This in turn means that while the technology neutrality principle guides regulators to refrain from extending the existing regulation, it is not as clear as to the content of the new regulation so that the effects equivalence (equivalent effect across different technologies) could prevail. The hosting service providers in online media have a certain degree of immunity against defamation claims and consequently, their treatment is different.[207] However, even considering that the difference is caused by the process, setup, infra-structure, speed of change and control over changes of the specific service, it is difficult under the principle to establish how exactly the difference should be reflected in regulation for effects equivalence to prevail. Therefore, given the operating differences between service providers, technology neutrality remains

---

[199] Savin (n. 198).

[200] Reed, (n. 100), p. 278.

[201] Center for Media Transition. *The Impact of Digital Platforms on News and Journalistic Content* (2018). <https://www.accc.gov.au/system/files/ACCC%20commissioned%20report%20%20The%20impact%20of%20digital%20platforms%20on%20news%20and%20journalistic%20content%2C%20Centre%20for%20Media%20Transition%20%282%29.pdf> accessed 22 November 2020.

[202] ibid.

[203] Savin (n. 63).

[204] Savin (n. 198), p. 22.

[205] Savin, (n. 198), p. 22.

[206] Savin, (n. 198), p. 24.

[207] Reed (n. 100), p. 267.

ambiguous on how to grant equivalence of treatment considering these differences, and the intention of the regulator to introduce regulation at all should be examined in order to identify the ways to achieve equivalent effect. The outcome of such difficulty is examined in Article III and in section 4.3 of this dissertation (eIDAS use case), which shows that the regulation was aimed to be neutral regarding handwritten signatures and electronic signatures. Still, the contextual change in reality is considerably different and even while the regulation attempts to be technology-neutral, it still is closely linked to the existing understanding of the use of a particular technology.

2.9.2 Failure to understand technology

Reed argues that the aim of the principle is unattainable because the legislators fail to understand the technology.[208] In the wording of the regulation, the regulators fail to convey the technological part properly, either omitting something or over-regulating. Reed brings an example under the Database Directive[209] of 1996: the intention of the Commission expressed in the explanatory memorandum aimed at protecting "databases both of content originating from third parties and content originating from the maker of the database".[210] Unfortunately in the wording of the directive, the making was defined as the "obtaining, verification or presentation of the contents" and this tilted the protection of databases to only cover that which the maker of the database itself has obtained, verified or presented, instead of that of third parties. Consequently, database-making was a misunderstood process.

Similarly in Estonian law, point 10 of § 3 of the MLPA defines the virtual currency wallet service as "a service in the framework of which keys are generated for customers or customers' encrypted keys are kept that can be used for the purpose of keeping, storing and transferring virtual currencies".[211] The definition was transposed from the 5th AMLD proposal that read "'virtual currencies' means a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically" and wallet service as "wallet providers offering custodial services of credentials necessary to access virtual currencies".[212] As the 5th AMLD includes regulation about the credentials necessary to access the virtual currencies, it is important under the directive not how the credentials are maintained (encrypted or not encrypted), but rather that these credentials should grant access to the

---

[208] Reed (n. 100), p. 279.

[209] Directive 96/9 on the legal protection of databases OJ L77, 27 March 1996, p. 20.

[210] Reed (n. 100), p. 279.

[211] In Estonian: "*virtuaalvääringu rahakotiteenus on teenus, mille raames luuakse klientidele või hoitakse klientide krüpteeritud võtmeid, mida saab kasutada virtuaalvääringute hoidmise, talletamise ja ülekandmise eesmärgil*".

[212] Article 1 (1) and (2) of 5th AMLD.

wallet. The author concludes that the Estonian law-makers meant to say "encryption keys" (credentials used in controlling access to content) or even "encryption and decryption keys" but by mistake said "encrypted keys" (meaning that the keys themselves are encrypted for safekeeping these) in the definition of the respective service. Based on the Cybernetica AS overview of DLT mandated by the Estonian Information System Authority,[213] the word 'encrypted' is used in the context of 'encrypted' documents, messages or data and the word 'encryption' in the context of scheme, regime or operation or as a process. The algorithm and the keys are used for encryption and not encrypted themselves. As described in Article III,[214] the public key cannot be encrypted at all as it is a wallet address and otherwise the parties trading with each other would not be able to use these wallets. Plus, the custodial wallet provider does not generate any private keys for users and therefore, there is no need to encrypt any keys.

2.9.3 Undesired consequences

One undesirable consequence of the principle of technology neutrality is the vagueness of the regulation. Although the subsidiarity principle guides the regulator to develop regulation that is abstract in higher-level regulation, if regulation aims to be technology-neutral, the outcome only reveals itself through case law unless the guidelines or lower-level regulation that somewhat clarifies the meaning behind the vagueness are issued. In aiming to be vague for the sake of neutrality, legal clarity and certainty suffer as the regulation is unclear. Reed brings the example of the phrase 'stored on electronic device' in the then valid e-Money Directive, which is also present in the valid version, and believes that the vague construct leaves a lot of unanswered questions that have caused long-lasting debates with the UK FSA.[215]

2.10 Limitations

In order to frame the principle specifically in the digital society context leaving biotechnology, environment protection, military and similar applications aside, and specifically aiming to identify limitations to the scope of the principle of technology neutrality, it is possible to use the regulation of the Framework

---

[213] Cybernetica. 'Krüptograafiliste algoritmide elutsükkel. Uuring' [*Life cycle of cryptographic algorithms. Study*] (Riigi Infosüsteemi Ameti tellimusel, 2017). <https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf> accessed 21 October 2020.

[214] Veerpalu, Jürgen, Silva and Norta, (n. 89), pp. 39–84.

[215] Reed (n. 100), p. 280. Read further on the example at Chris Reed, 'The Law of Unintended Consequences – embedded business models in IT regulation' (2007) The Journal of Information and Technology Law 1, part 3.1 <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/> accessed 22 November 2020.

Directive in relation to significant market power as a source on the circumstances any curbing of any technology's use could be justified.

Also considering that the principle is based on the general principles of non-discrimination and equal treatment, the limitations of it are at the borders of differences that can be identified in the new technical solution. This means that in case the functions analysis reveals differences between the comparison objects that also effect the possibility to obtain the purpose and objective of the requirements set in regulation, the difference of treatment could be justified. However, the key question there is – whether the difference is substantive enough to justify difference of treatment and whether the difference in treatment is proportional to the difference in substance.

Furthermore, limitations to the principle can be identified under Article 3 (2) and (4) of the eCommerce Directive, under which the Member States may restrict the freedom to provide information society services from another Member State if the measures taken will be necessary for

> "public policy, in particular the prevention, investigation, detection and prosecution of criminal which the service provider has to comply in respect of: offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons, the protection of public health, public security, including the safeguarding of national security and defence, the protection of consumers, including investors"

which all could potentially be used as the basis for limiting the obligation to comply with the technology neutrality principle. Similar list is included and provides a justification to restrict data controllers or processors in Article 23 of the GDPR.

In the context of the NIS Directive, the limitations to the technology-neutrality are stipulated in Commission Implementing Regulation (EU)[216] laying down rules for application of the NIS Directive as regards to the further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

However, the author suggests that regulators should use the Services Directive[217] and the criteria for granting authorisations as an example for assessing the legality of limitations on the use of technology. Given this analogy, these limitations and differences of treatment must be:[218]

---

[216] Commission Implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

[217] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, pp. 36–68.

[218] Article 10, Service Directive.

(a) non-discriminatory;
(b) justified by an overriding reason relating to the public interest;
(c) proportionate to that public interest objective;
(d) clear and unambiguous;
(e) objective;
(f) made public in advance;
(g) transparent and accessible.

As it appears, specific legal instruments regulating in each specific sector or service may also include limitations for the technology neutrality principle that can justify a regulator's non-compliance with the principle as long as the choice is not arbitrary or unreasoned.

2.11 Conclusion

The current chapter provided an overview of the principle of technology neutrality. The principle is relevant to DLT, as regulation has been drafted for centralized structures and the impact of the regulation on distributed infrastructures must therefore be analysed to identify biases in regulation against DLT. The reason for the presentation of the principle is to understand the meaning of technology neutrality and functional equivalence and to guide the application of the principle in the DLT use cases discussed in Chapter 4.

In this chapter, the author presented a comprehensive overview of the aim, meaning, origins and subjects of the principle. In summary, the principle is expressed by the goal that "the rules should neither require nor assume a particular technology", and the principle is aimed rather to curb the regulator more than anyone else. This means that the regulator should refrain from preferring or favouring technologies, outputs of technologies, processes thereof or infrastructures based thereon. The principle is regarded as the starting point of information and communication technology (ICT) regulation but is considered relevant in all fields of law, applying equally to all branches of government – legislative, executive and judiciary.

The overview of the origins of the principle presented shows that the principle has been historically used in regulation aimed for ICT sector, –however, the principle has grown and expanded across sectors involving digital component.. Furthermore, the idea, aim and content of the principle is recognizable in public procurement regulation through the use of the principles of equality of treatment, non-discrimination and transparency. These are all the same values that are recognized also part of the technology neutrality principle and therefore, these principles in public procurement can be used to understand the expectations the technology neutrality principle creates for the regulators in relation to regulation. The placing of the principle among the values that need to be respected in establishing guidelines for the public sector for creating interoperability shows that where-ever public sector is making decisions that could influence the use of

technology – neutrality should be respected. Lastly, as technology has infiltrated also other sectors, the principle can no longer be considered as a principle only for the ICT sector, but this expansion has brought the principle to all sectors with digital processes or outputs and the principle should be recognized as a general principle of law.

In Estonian law, the principle is not worded in any other legal instruments than the ECA and even in ECA the term carries no definition. Nevertheless, the principles components can be found clearly stated in other norms of ECA and Public Procurement Act that also has the most relevant disputes ruled on in Supreme Court.

Consequently, as stated in this chapter, the main aim of neutrality is to secure competition among technologies that have the same characteristics, functions or utility or reach the same objective. In order to answer the question of how to identify bias in regulation on the basis of the technology neutrality principle, the author identified the components of the principle: (i) functional equivalence and (ii) effects equivalence. Both of these components should be used in analysing existing regulation in order to identify non-compliance with said principle. Initially, the functional equivalence sub-principle requires a functional analysis to be conducted. For the purposes of the analysis, the technology and its functions need to be studied along with the objective of the regulation and its requirements in the context of the aim and meaning of the technology neutrality principle. The effects equivalence requires that the equivalence of the effects of regulation is granted as soon as the equivalence of functions is established.

The court cases discussed show that courts struggle to understand the technology neutrality principle and that there is inconsistent practice in applying the principle. The principle is also relevant in the context of the treatment of digital goods versus material goods and, therefore, the court cases of *UsedSoft* and *Tom Kabinet* were discussed in the chapter in order to exemplify the fact that technology (such as the technical transfer layer) can also be the cause for difference of treatment. As can be seen in these cases, there are multiple layers in technological solutions, and the process of examination of these might reveal different functions and utility. Technological advances may change the context and develop reality in such a way that granting equivalent treatment to virtual expressions of previously physical objects seems like a constraint that was anchored in physical-world limitations. Hence, the offline-online equivalence of treatment, if followed to the letter, actually limits technological advances and use cases. Such difference of treatment is not necessarily contrary to the technology neutrality principle, as the principle requires regulators to consider the technology and its capabilities when regulating in order to ensure that the effect of their regulation is as non-favouring as possible. However, the principle does not require the limitation of the use of the technology for development of the rights of the parties and the object's trading options and liquidity. This is especially relevant to DLT and crypto-assets, even on the basis of the MiCA Proposal, which addresses the newly developed *sui generis* categories of different crypto-assets that are further developed versions of their off-chain concepts of means of payment, means of

exchange, entry-form securities, etc. Nevertheless, the layers might not necessarily justify equal or different treatment but may assist in understanding the interest the regulator wishes to protect and, consequently, reveal a reason why the regulator might wish to treat media differently despite the equivalence of utility and content layer.

The following chapter addresses how to ensure DLT-neutral regulation considering the regulative strategies suggested by previous research for DLT regulation. As mentioned in Chapter 1, this dissertation does not treat DLT regulation as a different field of study; however, recent regulative initiatives – the MiCA Proposal and the Pilot Regime – show that EU institutions are preparing to regulate DLT, and the regulative strategies presented in the following chapter are the alternatives that have been identified as relevant for consideration. The next chapter will build upon the research of earlier scholars and assess these regulative strategies on the basis of the sustainability and neutrality aims of said principle, bringing examples of the DLT-specific regulative initiatives identified by the author in the articles forming the compendium.

III REGULATIVE STRATEGIES

The following chapter aims to find an answer to the research question: how to sustainably ensure DLT neutrality? This research question is addressed on a foundational level, meaning that the question not only concerns which regulative strategy to use in a fragmented and isolated context of one specific DLT use case, but the wider perspective of the impact of the technology is considered. As previously mentioned, DLT is not an isolated technology that can be used in one sector but has applications across society and markets and expands into unexpected use cases constantly. Therefore, the choice of regulative strategy should consider the technology's wider context and the contextual changes introduced thereby.

Furthermore, DLT-based networks are globally accessible and not limited to a specific territory or jurisdiction. This means that any national or even multi-level regulatory activity at EU level should be conscious of the reach and accessibility of DLT as any regulation with limited territorial scope fragments the legal certainty of operating a global network and creates obstacles for users and innovators. Therefore, legal scholars carry the burden of sharing and investigating the regulative strategies adopted in different jurisdictions to identify potential regulative strategies that could limit the negative effect of fragmentation of national regulation.

The discussion in this chapter is followed by use case analyses based on specific existing regulation to exemplify the limitations existing regulation may create to DLT use. Nevertheless, in designing regulative strategies in response to the disruption brought about by DLT, the regulators should not only view the specific use cases but also the wider context and try to address the entire existing regulatory framework using a sustainable regulative strategy and models to ensure neutral treatment across the sectors in which DLT is used. Therefore, in the current chapter, the question of how to ensure DLT neutrality in regulation is addressed by displaying a selection of strategies that regulators should consider while aiming to regulate DLT use. The chapter addresses these regulative strategies based on sustainability and neutrality aims.

In 2018, the European Blockchain Observatory and Forum and the European Commission requested a study on the legal and regulatory aspects of blockchain-inspired technologies (Study),[219] which was completed in March 2020. The European Commission's aim was to look at the technology and understand its "developments and also its potential impact on society and economy with a view of setting the right conditions for the advent of an open, secure, trustworthy, transparent, and EU law-compliant data – and transactional environment."[220] The

[219] European Commission. Call for tender page. Tender press release 12 December 2018. <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects> accessed 06 November 2020

[220] ibid.

Study's outcome can potentially be used to pave the approach for DLT to be regulated in the EU. In September 2020, the EU introduced its first initiative to DLT-specific regulation – a proposal on markets in crypto-assets (MiCA Proposal) and a proposal on a pilot regime for market infrastructures based on DLT (Pilot Regime) among a package of instruments that is also analysed in this chapter as to its regulative strategy.

The EU Blockchain Study and, separately, Michele Finck, who also led the completion of the Study, have identified various strategies for DLT regulation to relieve the tension between law and technology. The selection presented in this dissertation is not a comprehensive overview of all possible options presented in the Study as the author considers some of these as temporary solutions (e.g., sandbox) or add-ons to other alternatives (e.g., wait-and-see). The overview of alternative regulative strategies is based on the categories presented in the EU Blockchain Study: (1) the wait-and-see approach (innovators operating in 'quasi-lawless zones'); (2) application of existing legal frameworks; (3) adapting existing regulation (ranging from introducing supranational regime to self-regulation and polycentric coregulation).[221] However, the author presents regulative models as part of these strategies that were not discussed in the EU Blockchain Study as models used to address technology regulation. The author does not discuss sandbox regime and considers this as part of the three main strategies that is used side-by-side with these as the aim of the sandbox regime is to learn about the new technology use cases during the wait-and-see phase in order to develop a strategy to either apply existing regulation or adapt it. All of the above strategies can be fluid phases in the sense that they are adopted temporarily while paving the road to the next phase.

For example, the MiCA Proposal introduced by the EU in late 2020 can be considered as a termination of the wait-and-see regulative strategy and the start of the strategy of adapting existing regulation by introducing a supranational regime – "a bespoke regime for crypto-assets".[222] Furthermore, the Pilot Regime is a revolutionary experimentational supranational regime that partly continues the wait-and-see regime as it is temporary regulation, nevertheless, it is also an adaptation of the existing regulation strategy as well. Both of these instruments are discussed further in this chapter as to their approach and impact.

Of the alternatives presented, Finck considers polycentric coregulation, that she calls the 28th regime in the EU, as the most agile and able to both overcome the Pacing Problem and achieve the goal of sustainability. However, in the EU Blockchain Study no such clear preference for a regulative strategy is issued. Furthermore, as seen by the Digital Finance Package, the EU chose the supranational regulation as the preferred strategy with the Pilot Regime being a fluid and customized regulation full of iterations and adaptations.

---

[221] Finck (n. 41), pp. 153–181.

[222] Pilot Regime (n. 38), p. 2.

Consequently, in coherence with the topic of the dissertation, the aim of the EU to pave the way for new regulation is important to address from the point of view of technology neutrality principle. The EU Blockchain Study suggested three different regulative strategies for DLT as presented above and the current chapter builds upon these strategies with technology regulation specific models. Each of these models are then assessed based on sustainability goal and technology neutrality principle as benchmarks. Although the EU Blockchain Study occasionally addressed neutrality concerns, the biases of existing regulation were not discussed and the sustainability goal of regulative strategies received little attention.

As mentioned in Chapter 1, this dissertation does not treat DLT regulation as a different field of study; however, as EU institutions are preparing to regulate DLT, these regulative strategies are presented as solutions to regulate the DLT context.

3.1 Effects equivalence as a cause for action

In section 2.5 above, the author identified the components of the principle of technology neutrality – functional equivalence and effects equivalence. The author further presented in section 2.6 above that the sustainability goal is a key element of the principle. Given this context, it is important to stress that, although, effects equivalence requires functionally equivalent technology to be granted equivalent treatment under existing regulation, this does not necessarily mean that existing regulation needs to be amended. Rather, given the sustainability goal of the principle, if it is possible to achieve technology-neutrality also through implementation neutrality meaning the interpreting of existing regulation in a functional-teleological way. Such strategy should be chosen in case no adaptation of the existing regulation is pursued to be in line with the sustainability goal.

If, on the basis of a compliance check with the principle of technology neutrality, the regulator establishes that existing regulation fails to comply with said principle, the regulator needs to provide solutions for how to comply with the principle either through a measure of guidance, the executive branch (central bank, ministry, government office, etc.) or guidance in the form of a court ruling or request such guidance from the market itself through market-led instructions for transparency and compliance.

This means that effects equivalence is a cause for action, while the first action that needs to be taken is the assessment of whether effects equivalence can be granted. This leads us to consider the downside of the wait-and-see strategy in the effects equivalence context. The following subsections will address the different regulative strategies that aim to secure DLT neutrality in a sustainable manner.

In the following sections, the different regulative models that fall in the three regulative strategies of (i) wait-and-see, (ii) application of existing regulation and (iii) adaptation of existing regulation discussed in the EU Blockchain Study are presented along with their assessment under technology neutrality and sustainability goal.

3.1.1 Wait-and-see strategy

Until the MiCA Proposal, the European Commission also employed the wait-and-see strategy for "'actively monitoring' blockchain technology without taking concrete regulatory steps".[223] The identified advantage of the wait-and-see approach is the promise that observing and assessing the changed circumstances will lead to better regulatory decisions and, hence, better regulation. However, the regulative strategy 'wait-and-see' actually presupposes that all of the existing regulation continues to apply, and this is often missed.[224] In this context, it is the view of the author that the wait-and-see strategy is largely the same as the 'application of existing regulation' strategy and has the same concerns and difficulties. Still, as wait-and-see requires regulators to 'see' meaning in order to actually observe, assess and learn about the new technology for the purpose of understanding the effect thereof, it would be correct to conclude that the strategy is not merely about 'waiting-and-seeing', but actually about learning and assessing.

Nevertheless, the disadvantage of the strategy is that it creates uncertainty among innovators and, as can be seen in the *de Voogd* use case below, also uncertainty and confusion in the regulator, the public and users of the technology. Furthermore, the biases in regulation against any new technology remain intact and the non-apparent risk is that not granting effects equivalence to functionally equivalent technologies as the regulator is waiting-and-seeing is equally non-compliant with the technology neutrality principle and therefore, should not be accepted as a DLT-neutral strategy. The author concludes that this regulative strategy cannot be regarded as sustainable due to its failure to grant technology neutrality.

3.1.2 Applying existing regulation strategy

As wait-and-see regulative strategy cannot be regarded as a separate or a sustainable regulative strategy, the other two alternative regulative strategies (applying existing regulation and adapting the existing regulation) must be explored. The author acknowledges that given the different roles of the regulator (legislative, executive and judicial branch), the judicial and executive branch have only one alternative of these two strategies – application of the existing regulation – as only one branch of the regulator (the legislative) is primarily involved in the adapting of the existing regulation. Nevertheless, the author regards the regulator representing all these branches and upon the regulator identifying a change on the market due to a transformative technology, it has the possibility to assess the change and decide how to proceed – the legislative branch may decide to remain passive and consequently, allow the judicial branch to apply the existing regulation without any analysis or guidance issued by either executive or legislative

[223] EU Blockchain Study (n. 15), p. 105.

[224] EU Blockchain Study (n. 15), p. 105.

branch or it may conduct exploration studies and publish analysis on the changes the new technology brings about on the market or it may issue interpretations of the existing regulation to guide the market participants or it may decide to adapt the existing regulation to react to the changed circumstances and pre-empt legal uncertainty given the changes. Consequently, the regulative strategies discussed herein treat the regulator as one decision-making actor with three different branches and not three different actors which all could have different strategies.

In this section, the regulative models of functional-teleological interpretation and waiver model are discussed along with the concerns of this strategy addressed as introduction.

3.1.2.1 Concerns in relation to DLT

As discussed in Chapter 2, regulators often use the functional equivalence sub-principle to justify the extension of existing regulation to new technology[225] without much consideration for the new technology. As Harvey points out, the principle of functional equivalence is often used to invoke liability of parties that are the easiest to identify and bring claims against.[226] Similar liability expansion discussions and research can be identified also in relation to DLT. Vast amount of publications on the distribution of liability on blockchain and distributed ledger-technology networks use the same logic of ease of identification and bringing claims.[227] This liability expansion often presumes similar construction and preconditions than those that served as the building blocks for existing regulation. The circumstances and construction of DLT is very different from centrally con-

[225] Savin (n. 63), p. 5.

[226] Harvey (n. 64).

[227] Aleksei Gudkov, 'Control on Blockchain Network' (2018) Nova Law Review 42, p. 353. See also, Laila Metjahic, 'Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations' (2018) Cardozo Law Review 39, p. 1533, Christopher Koopman, Matthew Mitchell and Adam Thierer, 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change', (2015) Journal of Business Entrepreneurship and Law 8, p. 529; Laila Metjahic, 'Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations' (2018) Cardozo Law Review 39, p. 1533; Mark Fenwick, Joseph McCahery, and Erik Vermeulen, 'The End of 'Corporate' Governance: Hello 'Platform' Governance' (2019) European Business Organization Law Review 20, pp. 171–187; Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity (2017) Law, Innovation and Technology 9, p. 269; Jeremy M. Sklaroff, 'Smart Contracts and the Cost of Inflexibility' (2018) University of Pennsylvania Law Review 166, p. 263; Patrick Berarducci, 'Collaborative Approaches to Blockchain Regulation: The Brooklyn Project Example' (2019) Cleveland State Law Review 69, p. 23, Ori Oren, 'ICO's, DAO'S, and the SEC: A Partnership Solution' (2018) Columbia Business Law Review 617 and Usha Rodrigues, 'Law and the Blockchain' (2019) Iowa Law Review 104, p. 679.

trolled and governed infrastructure. Only a few scholars[228] have in these discussions examined the different layers of the technological setup of DLT networks and consequently, introduced also correlated liability layers that are categorized as endogenous liability (liability in relation with other nodes aimed at securing the sustainability of the network) and exogenous liability (related to third parties outside the network). [229] This type of examination of layers serves as an example of a functional analysis of a new technology and its different layers that would allow the application of the functional equivalence principle and develop new regulation, if necessary.

The application of the functional equivalence principle in cryptoeconomics is nothing new, as ever since the arrival of bitcoin in 2008 and subsequently other cryptocurrencies, regulators have aimed to apply the anti-money laundering and counter-terrorism financing (AML/CTF) regulation to these DLT outputs without much consideration for the differences in the technology.[230] As the *de Voogd* case discussed in Chapter 4 indicates, regulators have subjected cryptocurrency exchange service providers to existing AML/CTF regulation, subjecting these outputs to more burdensome compliance requirements than even fiat currency exchanges, without any regard to the technological specifics.

Furthermore, since 2016, regulators have been faced with the innovative fundraising concept of Initial Coin Offering (ICOs), with the aim to subject these to existing regulation and only in some jurisdictions develop customized regulations for ICOs. Since the arrival of ICOs, various regulators have subjected the issuance of tokens[231] during an ICO to securities laws and regarded ICOs functionally equivalent to initial public offering (IPO).[232] The referred qualifications

---

[228] Dirk A. Zetzsche, Ross Buckley and Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) University of Illinois Law Review 1361.

[229] ibid.

[230] FATF, 'FATF Report: Virtual Currencies Key Definitions and Potential AML/CFT Risks' (June 2014). <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 01 December 2019.

[231] ESMA definition of a token: "digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose or use" and "tokenisation is a method that converts rights to an asset into a digital token. It is effectively a means to represent ownership of assets on DLT. Virtually anything can be tokenised, ranging from physical goods to traditional financial instruments." ESMA uses the term "token" interchangeably with "crypto-assets" and defines these "as a type of private asset that depends primarily on cryptography and Distributed Ledger Technology as part of their perceived or inherent value." ESMA (n. 55), pp. 7–8.

[232] The most renowned qualification of the regulator to this end was the US Securities and Exchange Commission (SEC) qualification of the DAO tokens as securities, as stated in the respective report: "The SEC's Report of Investigation found that tokens offered and sold by a "virtual" organization known as "The DAO" were securities and therefore subject to the federal securities laws." SEC, 'SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities'. (US Securities and Exchange Commission Press Release, 25 July 2017) <https://www.sec.gov/news/press-release/2017-131> accessed 01 December 2019. A similar conclusion, although based on different argumentation, is also used by the regulators

have led to ICO organizers being fined on the basis of existing regulation.[233] The issue which needs examination in the DLT context is whether ICO and IPO are functionally equivalent and, if so, whether existing rules need to be amended considering the new realm, its functions and characteristics and the qualities of the technology used, etc. In summary, the DLT context creates a number of challenges for the application of existing regulation and, consequently, the application of existing regulation should follow interpretational guidelines that also consider the DLT context and the related challenges, as discussed above.

3.1.2.2 Functional-teleological interpretation

In order to resolve these concerns raised in relation to DLT, in the opinion of Koops, the functional-teleological method of interpretation is the guiding principle of interpretation of the existing regulation[234] applied to any new technology. Koops stresses that existing regulation should be interpreted based on substantive values and interests the regulators intended the regulation to obtain, which means the regulators – including the executive branch and judiciary – must interpret even technology-specific and less abstract regulation in a "functional, teleological way."[235]

In the wider context, this means that the regulation applying to any new technology cannot only be made up of technical specifications, but must include the objective of the influence the regulation wishes to achieve, e.g., the list of aims in the GDPR in Recital 71 – minimisation of data, risk error and discrimination of individuals, etc. Therefore, it is the task of the interpreter of the existing regulation to seek to understand the objective of the functions that are set as requirements under existing regulation and consequently interpret existing regulation in a way that does not value the functions but the objective of the regulator's influence. Such interpretation was used by the CJEU in *Hedqvist*, where the court stated that strict interpretation of the VAT regulation does not mean that the

---

of the European Union Member States. For a shorter overview see: Philipp Maume, Mathias Fromberger, 'Initial Coin Offerings: Are Tokens Securities under EU Law?' University of Oxford, Faculty of Law [blog], (7 September 2018). <https://www.law.ox.ac.uk/business-law-blog/blog/2018/09/initial-coin-offerings-are-tokens-securities-under-eu-law> accessed 01 December 2019. For a longer overview see: Philipp Maume, Mathias Fromberger, 'Regulation of Initial Coin Offerings: Reconciling US and EU Securities Laws' (June 15, 2018). Chicago Journal of International Law, 19.2, pp. 548–585. <https://ssrn.com/abstract=3200037> or <http://dx.doi.org/10.2139/ssrn.3200037> accessed 01 December 2019.

[233] For example, SEC fined Block.one 24 MUSD for organizing an ICO that SEC considered breached securities law. See more here: U.S. Securities and Exchange Commission, 'SEC Orders Blockchain Company to Pay $24 Million Penalty for Unregistered ICO'. (Press Release 30 September 2019). <https://www.sec.gov/news/press-release/2019-202> accessed 01 December 2019.

[234] Koops, (n. 59)

[235] ibid, p. 25.

functionally equivalent bitcoin should not enjoy the effects equivalence of the VAT exemptions.[236]

It is the view of the author that, in the DLT context, this requires not only an understanding of the principle, existing regulation and DLT, but also the wider context of the technology, which primarily means the modalities of the architecture (infrastructure), consent mechanism, network governance rules, protocol as a self-regulation and a market on the basis of which the use cases operate. Such an approach is in line with Lawrence Lessig's theory on the four modalities of regulation.[237] According to Lessig's theory, the influence the regulator wished to achieve with the regulation should be assessed considering all of the different modalities of regulation at its disposal in the wider context of regulation – the market, the social norms (e.g., consensus mechanism and governance rules), the architecture (e.g., the protocol) and also existing regulation.

This regulative strategy is better achieved through the issuing guidance on interpretation by the regulator. As the EU Blockchain Study revealed, "oftentimes there is legislation in place in relation to a specific legal issue that has been identified but there seems to be a lack of awareness regarding its existence".[238] Usually such guidance is issued by an executive branch: the European Securities and Markets Authority (ESMA)[239] and the European Banking Authority (EBA)[240] have on multiple occasions resorted to issuing guidance or reports explaining DLT or regulation applying to DLT. However, probably the largest impact by a regulator has been from FINMA[241] in Switzerland, which has interactively contributed to the understanding of the technology, addressed legal uncertainty and disseminated knowledge of the technology-coherent interpretation of existing regulation, creating compliance and good practice.[242] Many financial regulators have issued warnings that operate like guidelines in relation to tokens and whether they qualify as securities under national regulation.[243] Also, the European Data

---

[236] *Hedqvist*, para. 35.

[237] Lessig (n. 68), p. 88.

[238] EU Blockchain Study (n.15), p. 107.

[239] ESMA (n. 55), p.11.

[240] EBA, 'Report with advice for the European Commission' (9 January 2019), p. 7. <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed: 09 December 2019.

[241] FINMA has issued several guidelines on blockchain and ICOs that have received a lot of attention also outside Switzerland and have been the basis of guidance by other national authorities. FINMA website. <https://www.finma.ch/en/documentation/finma-guidance/> accessed 4 April 2020.

[242] EU Blockchain Study (n. 15), pp. 106–108.

[243] The United States SEC, 'Investor Bulletin: Initial Coin Offerings' (July 2017) <https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings> accessed 24 October 2019.

Protection Board is planning to issue a guideline on the application of the GDPR to DLT.[244]

The lack of guidelines can create legal uncertainty that may cause individuals to be subjected to lengthy court proceedings and result in the suspension of all market activity in the related field. Such a situation can be identified in the *de Voogd* case, as discussed in Article I and Chapter 4 below. Guidelines allow regulators to quickly resolve legal uncertainty; however, it is certainly a burden on regulators to be quick in the development of these while the technology is still advancing and use cases are expanding.

Nevertheless, the author concludes that at times, mere interpretation is not sufficient and guidelines such as soft law are a temporary solution due to courts overturning these or the measures proving to be ineffective for ensuring compliance.[245] The adaptation of existing regulation might be a long-term goal, but a sufficient transitory alternative in the view of the author is the 'waiver solution' suggested by Furrer and Müller and discussed in the following section.

3.1.2.3 Waiver solution

On the basis of the articles by Harvey and Savin as well as the *de Voogd* case discussed in Article I and in Chapter 4 below, it appears to the author that the regulator and the courts are more light-handedly willing to secure the extension of the burden to comply than the equivalence of *outcome* (such as the validity or applicability of exemptions). Consequently, the regulator, including the judiciary is focused on expanding the compliance and liability burden to the disruptors entering the market dominated by incumbents. However, where the expansion of the equivalence of outcome is concerned, regulators are less generous with equivalence. Outcomes such as the validity of a smart contract as a contract in an electronic form or application of tax deductions or exemptions for cryptocurrencies are less light-handedly available. In such a scenario, incumbents receive a competitive advantage in comparison with disruptors, and the disruptors are inequivalently discriminated against.

Andreas Furrer and Luka Müller have consequently focused on the equivalence of outcome.[246] In the opinion of the author, Furrer and Müller have based their approach partly on the same idea of functional and teleological interpretation that is also promoted by Koops and the legislative design through abstraction of means as suggested by Hildebrandt and Tielemans (discussed in the following sub-section). In the authors view this is the meeting point of these different theories these different authors have presented. It appears to the author that in order to focus on the equivalence of outcome, the functional – and

---

[244] EDPB Workshop Program 2019/2020, <https://edpb.europa.eu/our-work-tools/our-documents/workprogram/edpb-work-program-20192020_en> accessed 24 October 2019.

[245] EU Blockchain Study (n. 15), p. 107.

[246] Furrer and Müller (n. 66), p. 15.

teleological interpretation of existing regulation must allow for the requirements of the existing regulation to be complied with by using technical measures built-in the DLT solutions and not by designing or building additional solutions that fit the requirement's box merely because the new technology meets the objectives of these requirements differently.

Furrer and Müller use examples of the functional equivalence principle from transport law and apply these to DLT use cases. According to them, the functional equivalence principle is applicable in the context of ICOs and DLT-based smart contracts since, in relation to these new phenomena, existing regulation is consulted for guidance and the regulator has the task of assessing whether and how to apply e.g., securities law and contract law. Furrer and Müller's understanding of the principle of functional equivalence is in line with the UNCITRAL model described in this chapter below, without requiring adaptation of existing regulation. For DLT-based smart contracts in particular, they present the following steps for the application of existing regulation on the basis of the functional equivalence sub-principle:

> "(i) The aim of the substantive and formal requirements set in the law for the validity of a transaction or existence of a legal institution must be analysed.
> (ii) The functioning of the digital system claiming to achieve the same aims must be analysed.
> (iii) If the aims can be achieved using the digital system, the substantive and formal requirements can be waived for the digital system's functions as there is no need for the substantive and formal requirements because the aims of these requirements are achieved through the functioning of the system."[247]

The UNCITRAL idea is the same as stated in Recital 74 of 2014/24/EU Directive as follows:

> "Where reference is made to a European standard or, in the absence thereof, to a national standard, tenders based on equivalent arrangements should be considered by contracting authorities. It should be the responsibility of the economic operator to prove equivalence with the requested label. To prove equivalence, it should be possible to require tenderers to provide third-party verified evidence. However, other appropriate means of proof such as a technical dossier of the manufacturer should also be allowed where the economic operator concerned has no access to such certificates or test reports, or no possibility of obtaining them within the relevant time limits, provided that the economic operator concerned thereby proves that the works, supplies or services meet the requirements or criteria set out in the technical specifications, the award criteria or the contract performance conditions."

This means that in case the supplies or services meet certain requirements or criteria set out in technical specifications of regulation, it should be allowed for

[247] Veerpalu, (n. 89), p. 154.

the obliged party to prove equivalence with third-party verified evidence or "other appropriate means of proof such as a technical dossier of the manufacturer".

The interpretation of the principle by Furrer and Müller is different from the UNCITRAL model (discussed in the following section) only in the sense that there is no need to amend existing regulation for the new realm, technology or infrastructure, but rather, if the functions required by the regulation to consider the transaction valid or the legal institution active can be achieved by the design created or organizational measures taken, there is no need for changes and the new digital system (e.g., programme) should be regarded as compliant with existing regulation.[248] Their definition of the principle is therefore as follows:

> "Insofar as ... law attaches the validity of legal transactions or the existence of a legal institution to substantive or formal requirements, these requirements shall be deemed to be fulfilled if a digital system can functionally replace the legal protection concerns behind these requirements on an equivalent basis".[249]

As with the solution provided by Hildebrandt and Tielemans (discussed below in this chapter), the burden of this solution rests on the role played by compliance supervisors and courts who need to be the ones to determine the equivalence of the functions of the innovative system and the function of the requirements stipulated in regulation. However, as described by Harvey above, the courts have difficulty in applying the functional equivalence principle and would most likely require the assistance of experts who validate or certify the innovative system. This is no different from the analysis of biological evidence for a DNA match, which involves scientific testing and a list of experts. The author concludes that this means there needs to be a shift of responsibilities and the rearrangement of roles from the legal professionals assessing compliance to the software or organizational experts assessing this type of compliance. Nevertheless, this means that the supervisory authority or judiciary still need to grasp the objectives of the regulation as if the respective authority or judiciary is unable to understand the objective of the requirement in the regulation, we can conclude that the regulation does not ensure legal certainty and is not transparent as to its aims.

It is the view of the author that in order to optimize the resources exposed to this obligation, the regulator could consider establishing either a stand-alone centralized certification procedure of the functions of these innovative systems, as is established by the Innovative Technology Arrangements and Services Act[250] in Malta or the one stipulated by the Pilot Regime that allows the competent authority to request an audit to ensure IT and cyber solution chosen.[251] Alternatively, the regulators could allow for self-regulation similar to that in India where crypto-

---

[248] Furrer and Müller, (n. 66), p. 15.

[249] Furrer and Müller, (n. 66), p. 4.

[250] Innovative Technology Arrangement and Services Act (ITAS Act), cap. 592, <https://legislation.mt/eli/cap/592/eng/pdf> accessed 21 November 2020.

[251] Recital 30, Pilot Regime.

currency exchanges have developed their own good practices[252] or allow functional equivalence validation processes be conducted by privately established and managed certification bodies, such as self-regulating organizations (SROs).[253] The SROs would assess the specific products, applications or even algorithms that the developers of which seek to use on the market and regard the existing regulation unfit. Such initiative has been taken by the Virtual Commodity Association (VCA) developed from a "working group in 2018 working towards the goal of establishing an industry-sponsored, self-regulatory organization for the US virtual currency industry, specifically virtual commodity marketplaces".[254]

These alternatives allow the interpretation of the functional equivalence principle developed by Furrer and Müller to not be a burden for the supervisory authority or the court system by delegating the task to identify equivalence to the private sector or enforcing validation procedures prior to entry to the market. According to Furrer and Müller, the solution requires only minor amendments in the relevant regulations, if at all, such as a clause to state that the authorities need to secure equivalence of outcome to functionally equivalent solutions that have been subjected to a either a public or private certification or validation assessment procedure. Such approach has been adopted in France: as discussed in Article II, the French DLT Order stipulated that "the registration of securities on DLT is under the law comparable in effect to the registration of securities at CSD so that all the benefits enjoyed by CSD-registered instruments are extended to DLT-registered instruments".[255] Furthermore, such approach can be recognized also in the proposed Blockchain Records and Transactions Act of 2020[256] that is set to amend the Electronic Signatures in Global and National Commerce Act of the US to adapt the regulation of electronic signatures to also include smart contracts on blockchain under its regulation and consequently, to grant effects equivalence to functionally equivalent signatures and transactions.

The overall benefit of this interpretation of the principle has the same aim as the technology neutrality principle, which was to prevent "the legal system from continuing to lag behind the *de facto* technical development and thus behind actual practice"[257] "without endangering the legal protection functions guaranteed by classical law."[258] Furrer and Müller regard the recognition of the functional equivalence principle in such a way in accordance with the principle of

---

[252] Report by Samvad Partners. NOTE ON REGULATION OF CRYPTOCURRENCY EXCHANGES IN INDIA. 3 November 2020, p. 2 [held by author]

[253] FINMA website, <https://www.finma.ch/en/authorisation/self-regulatory-organisations-sros/> accessed 4 April 2020.

[254] VCA website. <https://virtualcommodities.org/> accessed 21 November 2020.

[255] Veerpalu (n. 88), p. 287.

[256] H. R. 8524 amending Electronic Signatures in Global and National Commerce Act 15 U.S.C. 7001(a). <https://www.govtrack.us/congress/bills/116/hr8524> accessed 26 December 2020.

[257] Furrer and Müller, (n. 66), p. 4.

[258] ibid.

contractual freedom on the free market, having a positive effect on digital society on the whole.[259]

In summary, if effects equivalence calls for action and neither interpretation nor waiver solution are sufficient to secure DLT neutrality, an adaptation of existing regulation might be called for based on the models, as discussed in the following section.

3.1.3 Adaptation of existing regulation strategy

There are a number of models that regulators could follow for the adaptation of existing regulation that are either based on examples used in the past (e.g., UNCITRAL model), used in the EU regulations (e.g., GDPR model) or discussed in previous literature that can be perceived also as the goals of better regulation initiatives of the EU (e.g, polycentric coregulation). The below does not pertain to exhaust the list of models or provide a comprehensive overview of all possible models, but merely portrays the models that either have been used or can be used to sustainable bridge the gap created by transformative innovation such as identified in bridging from online to offline dimension and currently from centralized to distributed infrastructure.

3.1.3.1 UNCITRAL model

Using the UNCITRAL functional equivalence model used in the drafting of model laws for electronic signatures as guidance, the approach of regulators for the adaptation of existing regulation should include the following steps:

(a) recognize the essential differences between the media, technology or infrastructure;
(b) identify the purpose of the rules in existing regulation applicable to the existing medium, technology or infrastructure;
(c) to make the best effort to identify the characteristics and technical- or model-setup-related qualities of the new medium, technology or infrastructure, as this is needed to understand how the 'functionally equivalent' rule could be constructed
(d) construct the new rule for the new medium, technology or infrastructure[260] or adapt the rule to be technology-neutral to the new context.[261]

This means that regulators need to understand the functions of the new medium, technology or infrastructure, its utility and the purpose of the rules in existing

[259] ibid.

[260] Harvey (n. 64), p. 60.

[261] UNCITRAL Model Law on Electronic Signatures (2001), 5 July 2001. <https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures> accessed 02 May 2020.

regulation in order to be able to adapt existing regulation in a technologically neutral way. The UNCITRAL model was used in relation to DLT in 2017 in the states of Delaware and Wyoming for corporate stock-certificate tokens, and the use of DLT networks for the creation and maintenance of corporate records along with stock ledger as discussed in Article II.[262] Malta and Lichtenstein have adopted rather comprehensive DLT regulatory frameworks,[263] and initiatives to this aim have been also taken by Luxembourg[264] and Germany[265] using the UNCITRAL model to ensure legal certainty and a level playing field for incumbents and innovators.

This means that the model can be used to develop national regulation and supranational regulation as suggested by Finck and the EU Blockchain Study. Furthermore, it seems to the author that the UNCITRAL model was also used to develop the MiCA Proposal in order to introduce the regulation for crypto-assets and partly also the regulation in the Pilot Regime. However, as indicated in this chapter, the Pilot Regime also includes many other models and regulative strategies as will be discussed below.

The author concludes that the advantage of the UNCITRAL model in general is legal certainty. Furthermore, the use of it in supranational regulation is the potential to harmonise regulation across the region. However, DLT has a wide range of applications across sectors and new use cases are revealed constantly, which means that regulation may need constant adaptation. Therefore, the UNCITRAL model is challenged by the sustainability goal of the neutrality principle. Although used for electronic signatures regulation, this model has not proven to be successful, as its adaptation could prove to be slow and require too many resources to be able to guarantee a sustainable neutral regulative solution.

Furthermore, Savin believes that this model where functional equivalence is used to draft new regulation on the basis of old regulation should be dismissed as a regulative strategy altogether as it is "typifying the Fourth Industrial Revolution to 'legacy' regulatory models".[266] Savin[267] shares this concern as discussed in the previous chapter due to the convergence of disruptive technologies. These new technologies cannot be as clearly placed under any sector-specific regulation and this, unfortunately, leads to the application of unfit regulation on convergent technologies.[268] His opinion is based on an analysis of the practice of applying the principle of functional equivalence to the extension of existing regulation by

---

[262] Veerpalu, (n. 89), p 283.

[263] EU Blockchain Study (n.15), p. 107.

[264] EU Blockchain Study (n. 15), p. 107.

[265] EU Blockchain Study (n. 15), p. 107.

[266] Savin (n. 63), p. 5.

[267] ibid.

[268] Also in the EU Blockchain Study, "the potential barriers in sectoral legislation" were identified as having a restrictive impact on the "socio-economic potential in the EU". EU Blockchain Study, p. 6.

EU institutions in law-drafting in domains such as (i) telecoms, (ii) media under editorial control and (iii) e-commerce. [269] According to Savin, the telecoms regulation is built on ideas developed two decades ago that have now been included in the Electronic Communications Code,[270] which subjects disruptive innovations called 'over-the-top' service providers to expired regulatory models because of the aim of the level playing field and video-sharing platforms to use regulation developed for linear TV.[271] Consequently, Savin claims that "the three regulatory circles that currently affect the Internet (e-commerce, audio-video and telecoms) are essentially based on old and well-tested regulatory models largely developed for pre-Internet technology".[272] However, according to Savin, this is not the only flaw in the telecoms regulation. The steepest concern is the separation of the sectors into regulatory silos[273] with typically stand-alone enforcement infrastructure and supervision authorities. These silos represent separate layers in relation to technology as the 'carrier layer' is represented by the telecoms who provide the infrastructure and the 'content layer' is represented by the information society services (attached to the regulatory bundle of consumer protection, e-commerce, copyright, privacy, etc.) and by 'media under editorial control' (attached to the regulatory bundle of consumer protection, advertising and protection of minors). These regulatory silos are not a good regulatory framework for convergent technology – technology that crosses many layers and sectors. DLT could also be one of these technologies; only the future shows whether the MiCA Proposal is sustainable for the development of crypto-assets across silos of financial regulation.

Consequently, it appears that if the innovation does not fit into a pre-assigned category, the silos developed in the regulatory framework will always prove to be unfit. As Savin claims, such practice has resulted in damaging the innovation brought by disruptive technologies. Furthermore, according to Savin, this is primarily linked to the lack or limited use of examination of the new technology along with its different layers and functions, but also to the limited examination of the effect of the application of existing regulation on the use cases of the new technology. The result of extending the sector-specific regulation on disruptive technologies could potentially be negative because the new technology could function in a very different way – compare telephone communication and Skype. Hence, even if effects equivalence is granted, existing regulation with its requirements may be unfit.

---

[269] Savin (n. 63), p. 5.

[270] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) PE/52/2018/REV/1 OJ L 321. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1575871089458&uri=CELEX:32018L1972> accessed 09 December 2019.

[271] Savin, (n. 63), p. 6.

[272] Savin, (n. 63), p. 6.

[273] Silos represent the industry or sector specific bundle of regulation.

The author stresses that convergence is not an unknown concept for DLT use cases. Tokenization challenges the regulatory silos of payments and securities regulation, as payment tokens[274] and utility tokens[275] can also be categorized as securities or fluid categories that later transform into securities.[276]

The author concludes that the convergence of technologies has caused changes in business models and disruptions in specific historically developed sectors that are subjected to regulatory framework silos. This has led regulators to search for regulative strategies to address the challenge created by the convergence and rapid pace of change. Therefore, effects equivalence requires equivalent treatment but not necessarily application of the extension of existing regulation through the UNCITRAL model, as the entire regulative intention or domain of regulation (considering the regulative silos and convergence) might be unfit for the new technology. This means that regulators should be guided rather by the waiver solution than the UNCITRAL solution as the first has more flexibility to adapt to the DLT innovative solutions.

3.1.3.2 GDPR model

Mireille Hildebrandt and Laura Tielemans[277] believe that the regulative design solution used in the GDPR could be an inspiration to address sustainability and neutrality concerns all in one.

Their claim is that the only acceptable route to future-proof neutral regulation, considering the fast-paced digital society, is to include in the text of the regulation only the interests, i.e. the objective, of the regulation (minimization of personal data, transparency, etc.) that need to be protected and not the specific requirements needed for said protection. Hildebrandt and Tielemans believe that the interest should be understood as the purpose and aim of the regulation.

This relates to the subsidiarity principle and the idea of Koops on the abstraction of the most sustainable law in the higher-level as presented in chapter 2 and also to Lessig's idea that the key in any regulation is to understand the influence the regulation wishes to achieve and not merely focus on the specific requirements. The regulative design solution described is in line with Koops'

---

[274] Also referred to as virtual currencies or cryptocurrencies. EBA (n. 240), p. 7.

[275] In early 2019, the European Banking Authority (EBA) defined utility tokens as follows: "Typically enable access to a specific product or service often provided using a DLT platform but are not accepted as a means of payment for other products or services. For example, in the context of cloud services, a token may be issued to facilitate access." ibid.

[276] These tokens usually provide either ownership rights or entitlements to profit distribution. In the context of an ICO, the asset tokens are issued in exchange for fiat money or other crypto-assets. EBA (n. 240), p. 7.

[277] Mireille Hildebrandt and Laura Tielemans, 'Data protection by design and technology neutral law', (2013) Computer Law & Security Review 29, p. 516.

position that the regulator's aim should be to secure the effect of protection and not to dictate the means of protection.

Koops stresses that existing regulation should be interpreted on the basis of these substantive values and interests under protection, which means the regulator – executive branch and judiciary – must interpret even technology-specific and less abstract regulation in a "functional, teleological way."[278] This is especially important because the regulation (specifically with a set of requirements and compliance norms) needs to identify first of all the interests that existing regulation aims to protect as well as the technical solution or business model currently under use in order to establish whether the interests that need protection are at risk given the technical solution or business model. It is possible that the set of requirements or compliance norms are out of place and that the development of rules for these to be complied with through a procedure other than a built-in solution could be unfounded. Similar to the Uber or Bolt drivers' example – if the consumer protection interests are not at risk if the business model is built on transparency and real-time economy – the need for burdensome compliance requirements may be obsolete.

This GDPR model is partly in line with the model for regulative strategy developed in the Lamfalussy report already in 2001 addressing the law lag in the European securities market. The report proposed 4 levels of regulatory framework in which level 1 – framework principles what would serve as the values and goals and be adopted through a lengthy regulative procedure; and level 2 – more dynamic and agile regulative process for technical implementation measures by using various newly founded committees and including stakeholders; and levels 3 and 4 dealing with implementation and monitoring.[279] These levels were introduced to speed up the regulative responses to dynamically changing securities market in Europe, but the challenge concerns the regulation of the dynamically changing financial system in general and is not only securities market specific.[280] In the larger financial sector regulation the level 1 and level 2 regulation is also sometimes referred to as macroprudential and microprudential regulation[281] respectively that need to address different market failures based also on functional approach to regulative design as discussed in section 3.1.3.6 below. It appears that this legislative solution would allow the innovators to design a technical solution or employ proper organizational measures which do not necessarily follow a technology-specific regulation, but instead aim to attain the fundamental

---

[278] Koops (n. 59), p. 25.

[279] Alexandre Lamfalussy et al. FINAL REPORT OF THE COMMITTEE OF WISE MEN ON THE REGULATION OF EUROPEAN SECURITIES MARKETS, Brussels, 15 February 2001. <https://www.esma.europa.eu/sites/default/files/library/2015/11/lamfalussy_report.pdf> accessed 8 March 2021.

[280] Steven L Schwarcz, Regulating Financial Change: A Functional Approach, 100 Minnesota Law Review 1441–1494 (2016) <https://scholarship.law.duke.edu/faculty_scholarship/3309> accessed 8 March 2021.

[281] ibid.

values the regulation protects through a novel technical or organizational (also business model-based) design.Therefore, the author concludes that the functional equivalence sub-principle guides the regulator on the basis of Lessig, Hildebrandt and Tielemans to use goals and objectives in higher-level laws that are vague as to the specific technical solution and more precise as to the objectives of the regulation and the interests the regulator wishes to protect.

This setup would give the market the option to come up with compliant solutions and business models to protect these interests. Hildebrandt and Tielemans regard the regulation provided in the GDPR under the 'privacy by design' heading to follow this construction exactly. They call the 'privacy by design' solution an open-ended solution, which is potentially in compliance with both the principle of technology neutrality and functional equivalence, as such a legislative design solution does not attach any value to a pre-existing technology, business model or infrastructure. In essence, the 'privacy by design' solution creates a requirement for the data processor, who is the obligated party, to design their product or service in such a way that the interests the GDPR aims to protect could be achieved but leaves it to the obligated party to come up with an effective system with "appropriate technical and organisational measures". [282] In order to allow the obligated parties to organize themselves under this design solution, the regulator specified "a general requirement stipulating that, at the level of the technical design, data protection obligations must be met, if technically and economically feasible."[283] According to Reed, a similar approach was also taken by the UK in the Financial Services and Markets Act from 2000, which laid down the general principles of law and iterated specific sets of lower-level rules in order to address difficulties presented by the online domain.[284]

---

[282] Recital 78 and Article 25 clearly leave it to the data processor to design an effective system of protection. Article 25 states:
"1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article."

[283] Hildebrandt and Tielemans (n. 282), p. 516.

[284] Reed (n. 60), p. 251.

Hildebrandt and Tielemans are of the opinion that such a model allows the disruptors and innovators to develop new technological solutions that are compliance-oriented and the regulation does not prevent innovation from coming up with more effective and advanced tools and techniques to protect the interests of data subjects. Hildebrandt and Tielemans concede that the solution is difficult for the judiciary to adopt as the judges need to somehow understand the technology through the inclusion of trustworthy technical experts who validate or even certify that the built-in technical system meets these protection obligations technically and organizationally.

Philipp Hacker and others have also found this form of regulation, which they refer to as a method of open-ended regulation, as the most suitable in case of DLT.[285] According to Hacker and others, this open-ended regulation would include an objective to influence and motivate the disruptors to design their solutions in accordance with the values under protection by the regulation by rewarding compliance. Hacker and others call this form of regulation 'regulation by design'.[286]

As discussed in sub-section 3.1.3.5, the Pilot Regime is partly the GDPR model and waiver model all at once – from one side, the protection interests are stated elsewhere – in regulation that governs the non-DLT solutions, and the Pilot Regime creates the waivers to these requirements.

3.1.3.3 Self-regulation

It is the view of the author along with other authors[287] that DLT has an internalised organic self-regulation mechanism in the form of the functioning of its protocol, the protocol inherent governance rules and consensus mechanism that could potentially transcend the problem of territorial fragmentation of regulation of global technology networks. This means that self-regulation and compliance with it is not something foreign or imposed by different national or regional governments on DLT networks but instead internal, or as suggested by Carla Reyes, "endogenous theory of decentralized technology regulation".[288]

[285] Hacker, Lianos, Dimitropoulos, and Eich (n. 69), p. 2.

[286] ibid.

[287] Finck (n. 41), p. 167.

[288] Reyes (n. 145), p. 195.

Self-regulation can either be required by the state or regional authorities[289] or initiated by the private sector or industry,[290] and its aim might be to promote the sector, make it more transparent or even prevent intervention by public authorities with statutory regulation. DLT-specific self-regulation examples are the ICO-regulated codes of conducts drafted and complied with by market participants during 2017–2018[291] and currently also the prevalent practise of DLT businesses in India who operate under self-imposed compliance rules in the context of legal uncertainty and ambiguity as the regulator has issued conflicting guidelines in relation to this innovation.[292]

The self-regulation idea is also included in Recital 27 of the EU Framework Directive, which states that "a cautious approach to *ex ante* regulation of newly emerging markets which 'should not be subjected to inappropriate obligation'"[293] should be adopted. Self-regulation in the EU has been defined as "the possibility for economic operators, social partners, non-governmental organisations or associations to adopt among themselves and for themselves common guidelines at the European level (particularly codes of practice or sectoral agreements)",[294]

---

[289] In relation to the Digital Single Market, the European Commission promotes self-regulation in the data portability and free flow of data (non-personal) areas as this leads to wider interoperability and technical standards. Article 6 (1) of European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union'COM (2017) 495 final, 8. M. Finck (n. 41), p. 169.

[290] An example from Estonia is the crowdfunding best practice principles and badges of compliance to those who comply with it (that are annually reviewed) developed by the finance sector public-private partnership FinanceEstonia. FinanceEstonia. *Ühisrahastuse platvormid muutuvad läbipaistvamaks.* [FinanceEstonia site. Crowdfunding platforms become more transparent]. <http://www.financeestonia.eu/news/uhisrahastuse-platvormid-muutuvad-labi-paistvamaks/> accessed 4 April 2020.

[291] Jonathan Keane. Switzerland's Crypto Valley launches an ICO code of conduct to protect investors and businesses. Tech.eu [blog] (9 January 2018). <https://tech.eu/brief/crypto-valley-ico-code-of-conduct/> accessed 21 November 2020.

[292] Report by Samvad Partners. NOTE ON REGULATION OF CRYPTOCURRENCY EXCHANGES IN INDIA. 3 November 2020, p. 2 [held by author].

[293] Kamecke and Körber (n. 65), p. 335.

[294] Self-regulation in the EU has been defined as "the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)". European Commission, 'Interinstitutional Agreement on Better Law-Making' [2003] OJ C 321/01, para 22. As defined by Julia Black self-regulation is "the situation of a group of persons or bodies, acting together, performing a regulatory function in respect of themselves and others who accept their authority". Black, Julia Constitutionalising Self-Regulation, (1996) *Modern Law Review* 59, pp 24–27. Hence, according to Michele Finck, self-regulation means "a situation in which regulation is devised through the collaboration of private actors with no or little involvement from the state". Finck (n. 41), p. 168.

which are used in "complex sectors such as nuclear energy and finance",[295] but also in the platform economy.[296] In the context of sharing economy platforms, the argument is that the industry or individual platform is much more aware of its users' needs and complaints than the regulator and is regularly introducing new iterations of its policies (terms of use, privacy policy, etc.). The platforms are also using technological constructs in order to be in compliance, and their business model is designed to incentivize the users and service or product providers to comply with the expected levels of performance (Uber drivers' car cleanliness, driving quality, customer service, etc.).[297]

As said, according to Kamecke and Körber,[298] upon establishing effects equivalence, the principle of technology neutrality does not guide the regulator to treat new technologies as old and rather the principle restricts than calls for an extension of existing regulation (designed for pre-existing technology) to the new technology.[299] Consequently, Kamecke and Körber argue that the principle of technology neutrality primarily rather supports self-regulation in relation to new technology than any other model of regulation. The self-regulation strategy is also known to Koops, who, nevertheless, calls for technology neutrality to be respected also in self-regulation.[300]

However, self-regulation is separated from customized regulation per regulation subject, also called 'individualised regulation'[301] or 'personalized regulation'[302] which could be hazardous (justice and equality between the treatment of individuals) and beneficial (all obligations and rights consider special needs and circumstances) at the same time. Nevertheless, as algorithmic regulation as a phenomenon growing out of the emerging data economy is able to develop individualized or personalized law that is customized per person into these new

---

[295] Finck refers to examples discussed by Neil Gunningham and Joseph Rees in 'Industry Self-Regulation: An Institutional Perspective' (1997) Law & Policy 19, p. 363 and by Elizabeth Howlett *et al*. 'The Role of Self-Regulation, Future Orientation and Financial Knowledge in Long-Term Financial Decisions', (2008) Journal of Consumer Affairs 42, p. 223.

[296] Platforms are regarded as the "de facto "rule-makers"". Marta Cantero Gamito, 'Regulation.com Self-Regulation and Contract Governance in the Platform Economy: A Research Agenda', (2017) European Journal of Legal Studies 9, p. 53. According to Parker, van Alstyne and Choudary "there is a significant tension between the social goal of promoting innovation and economic development, which argue for a relatively laissez-faire approach to regulating platforms, and the social gals of preventing harm, encouraging fair competition, and maintaining respect for the rule of law". Parker, Geoffrey G, Van Alstyne, Marshall W. and Choudary, Sangeet Paul *Platform Revolution: How Networked Markets Are Transforming the Economy – and How to Make Them Work For You*, (W.W. Norton & Company 2016), p. 230.

[297] Finck (n. 41), p. 168.

[298] Kamecke and Körber (n. 65), p. 335.

[299] Kamecke and Körber (n. 65), p. 331.

[300] Koops (n. 59), p. 27.

[301] Black (n. 294), pp. 24–27.

[302] See more in the forthcoming Busch/De Franceschi, *Algorithmic Regulation and Personalized Law. A Handbook* (2021 Beck Hart Sowon).

types of "granular legal norms" [303] and just might be able to overcome its perceived limitations.

Furthermore, self-regulation rules for blockchain have also been introduced by organizations termed as 'self-regulating organizations' (SROs).[304] According to Finck, "at an early stage of the technology's development, such processes [of setting up SROs] can be helpful, as they create awareness around the regulation, disincentivize 'lawless' behaviour and generate information as to where regulation is needed most".[305]

Nevertheless, different authors do not see self-regulation as a viable alternative as there is no oversight executed and might grant innovation to weigh less than compliance.[306] Also, the self-regulatory oligopolies or "transnational private regulatory regimes"[307] can breach competition law by potentially creating the same kind of protection regulation around the members of these oligopolies.[308] In the view of the author the incumbents are right now similarly lobbying the regulators to maintain the existing regulation that is tailored to them and that is not considerate of innovative new business models or technology. Consequently, in a way, the drawbacks of self-regulation, in the view of the author, are the same as the current existing regulation that is enforced by the states. In the opinion of the author, the code-based regulation discussed in this chapter below, would allow for the regulation to be more endogenous while requiring technology assisted compliance making it, therefore, susceptible to oversight. The author views the technology-assisted self-regulation as a viable option for DLT, as it is in line with

---

303 ibid.

304 The SRO concept in general is not new as there are a number of SROs operating, recognized and even obligatory to join in many countries. In some countries SRO regulations are approved by the authority, e.g., in Switzerland by FINMA, and SROs have to meet certain standards and requirements to become a recognized SRO and all the rules and regulations these SROs propose undergo a commenting period by the public. See: U.S. Securities and Exchange Commission SRO page for such commenting rounds. <https://www.sec.gov/rules/sro.shtml> and FINMA page <https://www.finma.ch/en/authorisation/self-regulatory-organisations-sros/> accessed 04 April 2020. See also: Korean Blockchain Association also introduced network independent self-regulation rules. Helen Partz, Korean Blockchain Association Reveals Self-regulatory Rules for 14 Member Exchanges. [blog]. (Cointelegraph 17 April 2018). <https://cointelegraph.com/news/korean-blockchain-association-reveals-self-regulatory-rules-for-14-member-exchanges> accessed 04 April 2020.

305 Finck (n. 41), p. 170.

306 ibid and Richard Epstein, 'Can Technological Innovation Survive Government Regulation?' (2013) Harvard Journal of Law and Public Policy 36, p. 87. <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=4977&context=journal_articles> accessed 04 April 2020

307 Imelda Maher, 'Competition Law and Transnational Private Regulatory Regimes: Marking the Cartel Boundary', (2011) Journal of Law and Society 38, p. 119. <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6478.2011.00537.x> accessed 04 April 2020.

308 ibid.

the organic compliance-orientation and rule-enforcement mode of action inherent to DLT. The suggested model is discussed further in section 3.1.3.6 below.

Nevertheless, the less contradictory but still flexible and sustainable alternative model is polycentric coregulation as proposed by Finck and explored in the following section.

3.1.3.4 Polycentric coregulation

Polycentricity in the wider context of command-and-control regulation, self-regulation and coregulation is itself not a new concept, as it stems from law and economics[309] and argues for multiple sources of regulation instead of merely single source of regulation. Finck believes that for constantly evolving technology, polycentric coregulation is the most efficient regulation as it is drafted involving key stakeholders and not solely by the regulator, allowing neutrality to be constantly challenged and securing sustainability through the subsidiarity principle. Polycentric coregulation as a strategy can also be used to develop supranational regulation, as the abstract general norms are introduced by the regulator in the higher-level and the more specific customized regulation by stakeholders in the lower-level.

3.1.3.4.1 Coregulation

Coregulation, polycentric or not, is based on the general presumption that "different regulatory designs [exist] for different problems, societies and institutional settings"[310] and that design-thinking should be taken as the foundation for rapid innovation-based solutions as "the fast-paced, iterative world of disruption does not mesh easily with the deliberative, slow-moving process of traditional rule-making".[311]

Coregulation, as defined by the European Commission, is a "mechanism whereby an [EU] legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, social partners, non-governmental organizations or

[309] Berman, Harold J. *Law and Revolution: The Formation of the Legal Tradition.* (Harvard University Press, 1983), p. 10. Erika Ilves, Polütsentriline õigus: riik ja õigus ei ole lahutamatud. [*Polycentric law: state and law are not inseparable*] (1999) Juridica 3, pp. 106–109.

[310] Jonathan Wiener quotation in M. Finck (n. 41), p. 171.

[311] Alice Armitage, Andrew Cordova and Rebecca Siegel 'Design-Thinking: The Answer to the Impasse Between Innovation and Regulation' (2017). UC Hastings Research Paper No. 250, p. 15. <https://repository.uchastings.edu/cgi/viewcontent.cgi?article=2568&context=faculty_scholarship> accessed 5 April 2020.

associations)."[312] This may mean that command-and-control regulation is mixed with self-regulation or something also termed as 'regulated self-regulation'.[313]

Coregulation allows the regulator to include private stakeholders in the development, enforcement and oversight of the codeveloped regulation and to be considerate towards the code or technology it regulates in a flexible and inclusive way.[314] This is also nothing new, as similar goals were set by the EU to improve regulation at the turn of the century.[315] Furthermore, coregulation is extensively used in relation to the Internet (e.g., control of counterfeit goods and intellectual property rights) as the joint effort of the cooperation of rights-holders, governments, non-state actors and service providers that Natasha Tusikov calls "revenue and access chokepoints"[316] on the basis of "informal nonbinding enforcement agreements".[317] Furthermore, "the E-Commerce Directive has been portrayed as a coregulatory legal framework as it entrusts the private sector with the enforcement of norms on the Internet".[318] The key aspects of coregulation are similar to the life of a computer code or a startup – iteration and pivoting – dubbed as "experimental learning and uncertainty"[319] that is "designed to adapt over time as the defined standards are constantly evaluated and reviewed".[320] This might not sound sustainable, but meets the expectations of the subsidiarity principle and Koops' description of higher-level and lower-level legal norms described in chapter 1.

The difference from self-regulation is primarily its goal and objective; contrary to self-regulation, its objective and aims are not only stated and configured by private stakeholders, but also by public authorities who have stated the values compliance requirements should aim for so that individual rights do not suffer. The private stakeholders involved, however, reduce the information asymmetry among the regulator and the Pacing Problem and address the Law of Disruption discussed by Downes, allowing the industry, the innovators and the stakeholders to address the specifics of the fast-paced technology challenge.

Furthermore, coregulation allows the necessary amount of flexibility to adapt to rapid change in a technologically neutral way and allows the innovators to keep

---

[312] European Commission 'Interinstitutional Agreement on Better Law-Making' (2003), OJ C 321/01, para 18.

[313] Finck refers to Wolfgang Schulz and Thorsten Held article 'Regulated Self-Regulation as a Form of Modern Government: An analysis of Case Studies from Media and Telecommunications Law', (John Libbey Publishing 2004). Finck (n. 41), p. 172.

[314] ibid.

[315] Finck refers to Joanne Scott and David Trubek 'Mind the Gap: Law and New Approaches to Governance in the European Union' (2002) European Law Journal 8/1, pp. 4–6 in Finck (n.41), p. 173.

[316] Natasha Tusikov, *Chokepoints. Global Private Regulation on the Internet.* (University of California Press 2017), p. 8.

[317] ibid.

[318] Finck (n. 41), p. 173.

[319] ibid.

[320] ibid.

innovating and experimenting with the technology. As "the need for adaptive legal frameworks in relation to blockchain is evident",[321] co-regulation as presented under GDPR model's principle-based approach in order to ensure sustainability should be considered. The principle-based approach coregulation is built on allows the framework to be flexible so that "it can take into account the evolving need of users, providers and national authorities'".[322]

Finck further seems to claim (without explicitly stating it) that coregulation helps to address "sociotechnical change"[323] and solve the Collingridge dilemma[324] by allowing the adaptation of existing regulation to the new technology to be led by private stakeholders, thus avoiding the Pacing Problem. Furthermore, the polycentricity of coregulation allows stakeholders, regulators and also the users of these networks to participate and through this collaboration to create a "fluid systems of power sharing".[325]

3.1.3.4.2 Polycentricity

Polycentricity in this context allows knowledge to be pooled from where knowledge rests and not depend on its transfer to the authority which is often the furthest away from knowledge. This kind of inclusion and engagement level is in line with the EU's 2015 Better Regulation Agenda[326] and Article 11 of the TEU[327] which promotes *ad hoc* consultations with stakeholders, obligates EU institutions to give citizens and representative associations the floor in public debate and "maintains open, transparent and regular dialogue with representative associations and civil society". The inclusion of multiple parties in coregulation establishes feedback and interaction channels but divides the regulation drafting authority among parties in a wider circle, including those within the industry, both as service providers and service users supporting pluralism on regulatory drafting.

Polycentric coregulation seems to allow the technology to be considered and respects the wider context of DLT. This conclusion is also supported by the

---

[321] ibid, p. 175.

[322] Also in the context of automated driving, Finck believes that the EU is aiming to approach the sphere aiming for flexibility and innovation. Finck (n.41), p. 175.

[323] Wiebe Bijker. *Of Bicycles, Bakelites and Bulbs: Toward a theory of Sociotechnical Change* (MIT Press 1995).

[324] Collingridge (n. 3).

[325] Finck refers to Joanne Scott and David Trubek 'Mind the Gap: Law and New Approaches to Governance in the European Union' (2002) European Law Journal 8/1, pp. 4–6 in Finck n. 41), p. 176.

[326] Communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of the Regions, "Better Regulation for Better Results – An EU Agenda", COM (2015) 215.

[327] Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390.

research of Hagemann, Skees and Thierer,[328] who predicted in 2018 that, given these shortcomings in relation to the sustainability goal, the traditional regulatory system will gradually be replaced by "an amorphous and constantly evolving set of informal 'soft law' governance mechanisms",[329] including multi-stakeholder processes and "informal governance mechanisms"[330] that are, according to Hagemann and others, already used today in the case of nanotechnologies.[331]

The reason for such development, according to them, is exactly as described above: the inability of the regulator to keep up with the demand to change the regulation at a very fast pace and with a high level of agility. The soft law, which, according to Hagemann, operates with the foundation in hard law, includes quasi-regulatory open-ended regulation that can be issued in the form of standards or guidelines developed by the private sector or regulators,[332] "proactive principles, policy guidance documents, best practices and voluntary standards, white papers, reports, advisory circulars, opinion letters and amicus briefs".[333]

Such research is in line with the initiative of the European Commission from 2016 to boost standardization as a competitiveness-enhancing regulatory technique,[334] EU's Rolling plan of ICT standardization[335] and the European Multi-Stakeholder Platform on ICT Standardisation.[336] It is very likely that standardization has already and will continue to replace command-and-control regulation in many complicated and fast evolving sectors in the future.[337] Furthermore, research indicates that adopting standardisation as a self-regulatory or coregulatory

---

328 Ryan Hagemann, Jennifer Huddleston and Adam D. Thierer, 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (February 5, 2018). Colorado Technology Law Journal. <https://ssrn.com/abstract=3118539> accessed 22 March 2020.

329 ibid, p. 37.

330 ibid.

331 Kenneth W. Abbott, Gary E. Marchant, Elizabeth A. Corley, Soft law oversight mechanisms for nanotechnology, (2012) Jurimetrics 52, pp. 279–312.

332 Hagemann, Ryan and Huddleston, Jennifer and Thierer, Adam D. (n. 328), p. 44.

333 ibid., p. 47.

334 Maastricht University, Programme for Standardisation as regulatory technique in the process of European integration: voluntary, inclusive and legitimate? <https://www.maastrichtuniversity.nl/events/standardisation-regulatory-technique-process-european-integration-voluntary-inclusive-and> accessed 25 December 2020.

335 EU Commission. Rolling plan of ICT standardisation [policy]. (5 August 2020) <https://ec.europa.eu/digital-single-market/en/rolling-plan-ict-standardisation> accessed 03 October 2020.

336 EU Commission. European Multi Stakeholder Platform on ICT Standardisation [policy]. (7 August 2020). <https://ec.europa.eu/digital-single-market/en/european-multi-stakeholder-platform-ict-standardisation> accessed 03 October 2020.

337 Finck (n. 41), p. 169. See also Cantero Gamito (n. 301).

technique allows for a more tailored and efficient regulatory framework,[338] and standards are also seen as a necessary measure in order to "become a leader in producing, adopting and governing new digital technologies such as blockchain and [DLT]".[339] Much effort has been put in to this goal by the ISO (developing several standards in relation to DLT with three finished standards[340] and nine under development), the IEEE Blockchain Working Group[341] and the ITU Focus Group on Application of Distributed Ledger Technology.[342] This is not to say that standardisation solves all possible problems, as there are numerous problems related to standardisation from constitutional concerns[343] to the overwhelming scope of these, but it does lead to the better consideration of technology and its wider context.[344]

Furthermore, part of this polycentric coregulation model of regulation is sandboxes and experimentation clauses. As recently as 16 November 2020, the Council of the EU adopted its conclusions on regulatory sandboxes and their role in EU regulatory framework. The conclusions identify that these experimentation clauses allow the enforcement of regulation on a case-by-case basis in order to ensure flexibility in "testing innovative technologies, products, services or approaches."[345]

---

[338] Lisa Bernstein, 'Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry' (1992) The Journal of Legal Studies 21/1, pp. 115. <https://www.jstor.org/stable/724403?seq=1> accessed 30 May 2020.

[339] Anna-Maria Osula, 'The Global Rush in Standards in Blockchain. Directions' [commentary] EU Institute for Security Studies (9 April 2020) <https://directionsblog.eu/the-global-rush-for-standards-in-blockchain/> accessed 03 October 2020.

[340] ISO 22739:2020 Blockchain and distributed ledger technologies – Vocabulary, ISO/TR 23244:2020 Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations and ISO/TR 23455:2019 Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems. Available on Standards by ISO/TC 307 website: <https://www.iso.org/committee/6266604/x/catalogue/p/1/u/0/w/0/d/0> accessed 3 October 2020.

[341] See more at IEEE Blockchain site: <https://blockchain.ieee.org/> accessed 03 October 2020.

[342] See more on the relevant International Telecommunication Union (ITU) website: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx> [03 October 2020].

[343] Cantero Gamito (n. 296).

[344] As an example in four years "between 1996 and 2000, the Occupational Health and Safety Administration (OSHA) promulgated 3,374 guidance documents, the National Highway Traffic Safety Administration (NHTSA) promulgated 1,225 guidance documents respectively, and the Environmental Protection Agency (EPA) promulgated 2,653 guidance documents". Furthermore, the US Food and Drug Administration (FDA) issues more than 100 guidances each year interpreting policies or changing previous interpretation. Hagemann, Huddleston, Jennifer and Thierer (n.313), p. 47, footnote 48. See also Crews, Clyde Wayne Mapping Washington's Lawlessness: An Inventory of Regulatory Dark Matter 2017 Edition 20, 49. <https://cei.org/sites/default/files/Wayne%20Crews%20-%20Map> accessed 30 March 2020.

[345] Council of the EU. Regulatory sandboxes and experimentation clauses as tools for better regulation: Council adopts conclusions [Press release.] <https://www.consilium.europa.eu/en/press/press-releases/2020/11/16/regulatory-sandboxes-and-experimentation-clauses-as-tools-for-better-regulation-council-adopts-conclusions/> accessed 21 November 2020.

Finally, coregulation also reconciles the centralized versus decentralized contrast that is dominant in blockchain technology networks and is the basis for the idea of the '28th regime' of supranational legal framework in the EU for maintaining a sustainable distributed ledger ecosystem with the purpose of avoiding "fragmentation between member states and a race to the bottom".[346] The very essence of this is to connect technological capabilities and innovations with regulatory challenges and find a socio-institutional solution that is integrated in "techno-economic reality".[347]

In the view of the author coregulation would allow neutrality to prevail sustainably only in case the stakeholders themselves can also set the boundaries between the regulation borders – where the amorphous and constantly evolving self-regulation in the form of "informal governance mechanism" ends and the traditional force-based regulation starts.

In the following sub-section, the author briefly examines the MiCA Proposal and Pilot Regime in the context of the regulative strategies discussed above in order to identify the regulative strategy pursued with these instruments by the EU.

3.1.3.5 MiCA Proposal and Pilot Regime

The MiCA Proposal and Pilot Regime are the only elements of the Digital Finance Package[348] that are discussed in this dissertation as follows.

3.1.3.5.1 Pilot Regime

The impact assessment conducted by the Commission identified various regulative strategies for the EU to use to address the digital finance package and the scope now addressed by the Pilot Regime. Among these were (a) an issuing interpretation in the form of guidance on the applicability of EU framework on financial services specifically to the crypto form of financial instruments; (b) the adaptation of existing EU regulatory framework on financial services and (c) an

---

[346] Finck (n. 41), p. 181.

[347] Finck (n. 41), p. 181.

[348] Digital Finance Package also addresse:

(i) Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU;

(ii) A Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014; and

(iii) A Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341.

Pilot Regime (n. 38), p. 2.

experimental and iterative regulation now known as the Pilot Regime.[349] The latter was considered the most appropriate as "there is presently not sufficient evidence to support more significant and wide-ranging permanent changes to the existing financial services framework in an effort to allow the use of DLT."[350]

In the opinion of the author, the further advancement of the waiver solution is a sandbox – or a pilot regime that waives the non-compliance of an innovative solution with formal or substantive requirements to observe and assess the suitability of the existing regulation or alternatively the need for adaptation of the existing regulation. These sandbox or pilot regimes require some level of new regulation to be adopted that also separate it from self-regulation. The need for regulation is either needed for the purpose of creation of a 'virtual environment' where experimentation is allowed or merely in recognition of the functions of the new technology on the basis of functional analysis. The Pilot Regime introduced as a proposal by the EU is based on this type of regulated waiver solution that is experimenting with the use of DLT for a temporary period of five years. This proposal is unique at the EU level and shows that, in EU law, experimentations and iterative law-making is an option to consider.

The Pilot Regime is an implementation of the Commission's FinTech Action plan[351] and aims to address the concern raised by EBA and ESMA, which, in their advice, argued that "provisions in existing EU legislation may inhibit the use of DLT".[352] Furthermore, the Pilot Regime text clearly states that it aims "to promote the uptake of technology and responsible innovation".[353] As the Commission recognizes that legal certainty is needed to be successful in this goal, the aim of the Pilot Regime is "to provide legal certainty and flexibility for market participants who wish to operate a DLT market infrastructure by establishing uniform requirements for operating these".[354] Furthermore, the Pilot Regime responds to the recommendations of the High-Level forum on the Capital Markets Union's final report recommending that the EU recognize the underused potential of crypto-assets and calling for the Commission to increase legal certainty for issuing and trading these.[355]

The EU Blockchain Study, the EU-developed Digital Finance Package along with the MiCA Proposal, the Pilot Regime and the Council's conclusions on sandboxes also show that these different regulative strategies have been tabled

---

[349] Pilot Regime (n. 38), pp. 6–7.

[350] Pilot Regime (n. 38), pp. 4–5.

[351] Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan, COM/2018/109 final, 08.03.2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109> accessed 21 November 2020]

[352] ESMA, Advice on 'Initial Coin Offerings and Crypto-Assets', 2019; EBA report with advice on crypto-assets, 2019.

[353] Pilot Regime (n. 38), p. 2.

[354] Pilot Regime (n. 38), p. 8.

[355] Pilot Regime (n. 38), p. 3.

and considered in response to the challenges stemming from the use of DLT. The Pilot Regime clearly states the sustainability goal[356] of the regulation and the challenges the existing regulation creates in respect of the technology neutrality principle in the EU. The Pilot Regime states that the proposal makes Europe's economy "future-ready"[357] and identifies its priority area to ensure that "regulatory framework is innovation-friendly and does not pose obstacles to the application of new technologies".[358]

In essence, the Pilot Regime temporarily waives certain requirements for the DLT market infrastructures that could potentially operate as hurdles to the development of DLT solutions in the financial sector.[359] This way, the Pilot Regime is a revolutionary instrument as, while being a regulation that is an approximation of laws under Article 114 TFEU, for the purposes of experimentation it creates a wide selection of transitional derogations from the requirements and compliance measures of other EU legal instruments which are part of the financial sector regulation and supports the use of DLT outputs defined as crypto-assets. The specific category of crypto-assets addressed is those that qualify as financial instruments and consequently fall under substantially tougher compliance regulation.[360] According to the Pilot Regime, the DLT application developer may apply for permission indicating the exemptions it needs for the infrastructure from the national competent regulator, and the national regulators are authorized to "remove regulatory constraints that can inhibit the development of DLT market infrastructures".[361] The regulator consults with ESMA to unify the practice on the market and ensure consistency, fair competition and a level-playing field to all participants.[362] On the basis of its assessment, ESMA issues a non-binding opinion and makes recommendations on the exemptions requested or the actual solution. The virtue of the Pilot Regime is that it grants these DLT solutions permissions that allow market participants to operate their network, referred to "a DLT market infrastructure", and provide their services in the EU.[363]

This means that the Regime follows both the waiver solution – permitting waivers and exemptions from formalized and substantial compliance requirements – and the GDPR solution – allowing the existing regulatory framework to stipulate the protection interests and the regulators' intention as an abstract goal. At the same time, the Pilot Regime aims to harmonize fragmented legal certainty on the EU market, allowing for a regional unified address of the market using the

---

356 ibid, p. 1.

357 ibid, Recital 1.

358 ibid, p. 1.

359 ibid, Recital 5.

360 ibid, p. 3.

361 ibid, p. 4.

362 ibid.

363 ibid, Article 7 and Article 8.

competent regulators in the respective national market as interpreters of the customizable regulation per respective DLT solution.

The author is of the opinion that the setup of the Pilot Regime could have included more elements of polycentric coregulation and more participation by innovation-focused stakeholders and not incumbents (CSDs and investment firms) in the functional analysis needed to grant the exemptions to a wider group of subjects than just CSDs and investment firm-type subjects. Only time will tell how sustainable this regulation and the approach will be; however, the author is looking forward to an abundance of research as to its success or failure.

3.1.3.5.2 MiCA Proposal

The MiCA Proposal identified an even wider selection of alternative regulative strategies than the Pilot Regime, from (i) an opt-in regime that allows to passport licenses regionally, (ii) full harmonisation, (iii) bespoke regulation for stablecoins, (iv) an expanding eMoney Directive for stablecoins, and (v) limiting the use of stablecoins. The MiCA represents Option 1 and 2 together to address the risks the Commission has identified in relation to stablecoins.[364]

The functional equivalence sub-principle has been expressed in the MiCA Proposal through the extension of the existing EU regulation qualifying some of these crypto-assets as financial instruments under Directive 2014/65/EU[365] irrelevant of the technology used to issue or transfer them. This means that the EU approach employs regulative strategy (ii), application of existing regulation, and regulative strategy (iii), adapting existing regulation by developing bespoke crypto-asset regulation for the hybrid DLT outputs that are jointly referred to as crypto-assets.

The concern here is similar as that presented in Chapter 2 – the application of the existing regulation could hinder DLT-based outputs in the case that the existing regulation is not considerate of the contextual changes and technological differences of DLT and its outputs. Similar concerns were identified in relation to the differences of publishers in the offline and online domain and telecommunication services versus OTT services. However, as the Pilot Regime addresses this concern by allowing for waivers or derogations from existing regulation for DLT-based experimentation according to MiCA Proposal, the majority of crypto-assets fall outside existing regulation under Directive 2014/65/EU and consequently, the MiCA Proposal creates a new bespoke regime that addresses the services related to trading platforms, exchange and the custody service of crypto-assets categorized into *sui generis* categories of:

---

[364] MiCA Proposal (n. 42), p. 7–8.

[365] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance OJ L 173, 12.6.2014, p. 349–496.

(i) crypto-assets other than asset-referenced and e-money tokens;
(ii) asset-referenced tokens; and
(iii) electronic money tokens (e-money tokens).

Both categories (ii) and (iii) include a certain type of stablecoins, which the EU sees as a potential risk for financial stability[366] and which are completely new hybrid categories specific only to DLT. This is again an example of a contextual change, similar to that discussed in Chapter 2, which has resulted in the development of a completely new regulation while aiming to achieve effects equivalence across technologies. As mentioned in Chapter 2, the difficulty of achieving neutrality in such case is related to the fact that these *sui generis* categories partly are and partly are not similar to existing categories of e-money, securities, etc. Given this fact, the questions remain whether the effect of the MiCA Proposal is neutral across technologies since it was introduced as a DLT-specific bespoke regulation, and whether the EU regulator, by placing crypto-assets into bespoke categories, is compliant with the technology neutrality principle. The author anticipates an abundance of legal research to be pursued also in relation to this regulation.

As the last section in this chapter, the author explores the last mile paved in the context of cyberspace regulation already by Lawrence Lessig in the 1990s and, in the context of DLT, by de Filippi, Wright and Reyes – the code-based regulation.

3.1.3.6 Code-based, endogenous and functional approach to regulation

While the opt-in regime, the pilot regime and full harmonisation might be the regulative strategies presently suggested for the digital finance regulation in the EU, de Filippi and Wright are of the opinion that such a path is difficult due to the global reach of DLT infrastructure. DLT infrastructure is neither national nor regional phenomena and any regulative strategy taken will have a territorial scope. Consequently, all competing territorial regulative strategies will create a fragmented legal certainty for the use of the global infrastructure and the trading of these crypto-assets within this infrastructure.

Consequently, de Filippi and Wright are suggesting that regulators should experiment with code-based regulation to achieve certain policy goals and constrain the developed DLT applications.

[366] See MiCA Proposal (n. 42), p. 2.

3.1.3.6.1 Code-cased regulation

Using the MiCA Proposal as an example, the crypto-asset could be included in the content layer, and regulation of the transportation layer (similar to the way the *Tom Kabinet* case showed) could dictate its ownregulation. Introducing regulation through code is further explained by Carla Reyes, who states that the regulators could

> "undertake the dual task of enacting a law or regulation via statute and then implementing that statute through code by engaging in an iterative and cooperative process with the technologies' core developers and with consensus from the network, so that regulation is endogenously incorporated into the decentralized ledger technology and the applications running on top of the technology".[367]

Furthermore, as explained by de Filippi and Wright, both statutory and contractual terms can be systematically translated into "simple and deterministic code-based rules that are automatically executed by the underlying blockchain network",[368] and this in turn can pave the way to the endogenous theory of regulation that Carla Reyes believes DLT can endure.

The idea is simply understandable if you consider stating something in English in the normative text and including it in the programming language in the respective protocol. This means that DLT does not only challenge the substance of law, model or strategy but as seen in this chapter – the delivery of regulation or the form of its expression e.g., model and strategy. Consequently, DLT not only innovates the content layer of regulation (the substance), but also enables to deliver regulation to subjects in a different form – a code. Such path of using the code itself for delivery of regulation is presented by de Filippi and Wright in their concept of "*lex cryptographica*"[369] using the examples of *Lex Mercatoria* and *Lex Informatica.* However, it is noted by the said authors that while *Lex Mercatoria* and *Lex Informatica* provided rules for the private law relationships, DLT infrastructure needs to be also governed by public law, e.g., anti-money laundering regulation, financial compliance regulation, public registries related regulation, etc.

Furthermore, code-based regulation could, similarly to the Pilot Regime and the MiCA Proposal, operate an opt-out or opt-in regulation, allow compliance measures to be performed through real-time economy methods, use the transparency of the networks as disclosures, etc. Nick Grossman has also suggested similar opt-out real-time economy-based compliance solutions for platform economy,[370] as the compliance subjects "implement mobile dispatch, e-hailing

---

[367] Reyes (n. 141).

[367] De Filippi and Wright (n. 12), p. 195.

[368] De Filippi and Wright (n. 12), p. 193.

[369] De Filippi and Wright (n. 12), p. 194.

[370] Parker, Van Alstyne, and Choudary (n. 296), p. 254.

and e-payments and 360-degree peer-review of drivers and passengers and provide an open data API for the public auditing of system performance with regard to equity, access, performance and safety".[371] This allows the regulator to obtain live data on the compliance subjects and their data that is subject to taxation or should be monitored for the protection of the interests of users.

On the basis of Grossman's work, the author concludes that Grossman is recommending to ease the compliance rules and requirements applicable to platforms because (i) aims of the regulator can be achieved through other means; (ii) compliance and supervision are more effective using the related technology in the same way it is used in the innovative solution; and (iii) applying the existing regulation on these platforms (due to cumbersome licensing and compliance regulation that tends to be different per jurisdiction) would be impossible to enforce or at least ineffective. The solution suggested by Grossman is based on open innovation and "tempered by data-driven transparency and accountability"[372] but has the same regulatory aim as existing regulation of "creating trust and fostering fairness, security and safety".[373] The same aim is fulfilled if compliance is executed through screening and certifying taxi drivers, requiring insurance coverage, monitoring the cleanliness and safety of hotels, etc. The solution suggested by Grossman is similar to the transparency secured by open-source software solutions, such as Bitcoin, due to the transparency of the code that all users can inspect and analyse. In the case of a code-based regulation, (either regulator-backed or self-enforced) the transparency theoretically functions in a similar way: as a feature of discipline hidden in the programming language functions of the code but detectable and recognizable to those able to inspect it. In the words of de Filippi and Wright, "the best way to regulate a code-based system is through code itself."[374]

By enabling the delivery of the regulation to be in the form of the code, DLT also enables to fulfil the compliance requirements of regulation by self-executing code. Furthermore, such can be seen in the Pilot Regime proposal that allows the financial sector to waive certain requirements for financial compliance. This means the regulators must recognize also the potential use case of DLT as not merely influencing the content layer (the content of the provisions of regulation themselves), but also through transport layer (the delivery tool of the content of the provisions) paving the way for code-based regulation that would also potentially allow compliance through the use of the same code (DLT used as compliance tool).

However, the problem of territorial scope of national and regional regulation (even if translated into code) will remain unless a self-regulative strategy or private international law assists in solving such a challenge.

---

[371] ibid.

[372] ibid, p. 253.

[373] ibid.

[374] De Filippi and Wright (n. 12), p. 194.

Nevertheless, given the general task of regulation – to guide the behaviour of the subjects – and relying on the example of the DLT network governance rules already inherent in its protocol, it can be concluded that the goal of implementing regulation in the protocol itself should be possible.

3.1.3.6.2 Endogenous regulation and functional approach to regulation

A step further from *lex cryptographica* is endogenous[375] regulation that was promoted for DLT by Carla Reyes already in 2016. Reyes reiterated that the endogenous regulation is known in the regulatory strategy discussion as there has been endogenous approach used in the financial regulatory research and theory. The approach is also known as functional approach to financial regulation.

This functional approach is premised on the fact that rapid changes take place in unpredictable ways in the financial system and that makes the market very dynamic. On the basis of this premise, the approach guides the attention away from the financial architecture and rather focuses on the economic functions. Such an approach allows to react with agility to dynamic changes in highly complex and rapidly changing structure.[376]
As stated by Steven Schwarcz:

> "In thinking about regulating a dynamically changing financial system, it may be more effective – or at least instructive – to focus on the system's underlying, and thus less time dependent, economic functions than to tie regulation to any specific financial architecture."[377]

As further explained by Schwarcz, this functional or "black box" approach focuses on investigating the functions rather than the structure allowing to analyze the unknown rapidly changing structure in a systematic manner even if it is highly complex like the financial system. The functions are economic functions and the fundamental functions of financial markets can be listed as the provision, allocation, and deployment of capital. Consequently, the primary task of the regulation is to address and resolve failures that restrict or hamper these listed functions.

Such approach that is based on the investigation of functions allows to overcome the complexities in order to resolve market failures through regulation. Nevertheless, regulation is endogenous in the financial system as without regulation the economic functions would lack effect, therefore, "the financial system

---

[375] According to Carla Reyes endogenous means "[h]aving an internal cause or origin" and in economic theory the endogenous regulation is "incremental, and continuous, producing small effects at each individual step but cumulatively resulting in ever deeper levels of cooperation." Reyes (n. 145), p. 223.

[376] Reyes (n. 145), p. 224.

[377] Schwarcz (n. 280), p. 1444.

can be characterized as a law-related system"[378] having elements of private law and public law.

The application of the functional equivalence and the functional method of the comparative theorists described in chapter 2 above could be used to resolve the dynamic change inflicted disruption. The functional method would guide the comparative theorist rather to the question which legal institution in the DLT infrastructure would be able to successfully resolve the challenge and consequently, resort to exploration onto endogenous regulation path. DLT in the context of the comparative legal theory can be considered as the foreign legal system with its protocol, built-in governance rules, programming language and consensus mechanism. Given these circumstances the legal analysis should rather revolve around the foundational tools and concepts already used in DLT and how these could be employed to achieve the behaviour of subjects participating in the DLT networks. This, in the opinion of Reyes, leads to "two-way regulation design process that requires the participation of core developers in the decentralized ledger technology ecosystem"[379] that could potentially develop "in a holistic, organic, and functional way – an endogenous way"[380] "flexible, adaptable, and feasible regulation that minimizes a variety of risks to a high degree".[381]

However, the problem of territorial scope of national and regional regulation (even if translated into code) will remain unless a self-regulative strategy or private international law assists in solving such a challenge.

Nevertheless, given the general task of regulation – to guide the behaviour of the subjects – and relying on the example of the DLT network governance rules already inherent in its protocol, it can be concluded that the goal of implementing regulation in the protocol itself should be possible. This non-comprehensive introduction to code-based, endogenous and functional approach to regulation is merely a reflection of the discussions present in this domain and aims to promote the consideration for code-based or algorithmic regulation as a regulatory technology[382] for DLT. This might expand the conventional dimensions of regulative strategies, however, DLT is the technology removing intermediaries from infrastructures including potentially also the national – or regional regulators themselves. The topic of regulation and algorithms, and their impact on one another seems to be obtaining more and more relevance and therefore, should not be overlooked.[383]

---

[378] ibid, p. 1469.

[379] Reyes (n. 145), p. 227.

[380] ibid, p. 233.

[381] ibid, p. 227.

[382] Finck (n. 41).

[383] See Busch/De Franceschi, *Algorithmic Regulation and Personalized Law. A Handbook* (forthcoming 2021 Beck Hart Sowon). Giovanni Comandé, Martin Ebers, Mimi Zou (eds.) *Machine Intelligence, and Law. Data Science, Machine Intelligence, and Law* (Springer 2020). Ebers, Martin; Cantero Gamito, Marta 'Algorithmic Governance and Governance of Algorithms: An Introduction' in Martin Ebers; Marta Cantero Gamito (eds.). *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges*. (Cham: Springer Nature 2020).

3.2 Conclusions

As clearly stated in the Pilot Regime, the EU follows the principle of technology neutrality, but existing regulation is created for centralized structures and has not been designed with DLT in mind. This results in accepting the possibility that existing regulation may be hindering the use of DLT and creating discrimination against its use. In order to establish which regulation specifically is discriminatory and has a bias included in its text, use case analyses must be conducted as presented in the following chapter. However, in order to resolve this non-compliance with technology neutrality principle, in this chapter the author presented different regulative strategies, such as (i) wait-and-see; (ii) application of existing regulation and (iii) adapting existing regulation that are based on the EU Blockchain Study. Furthermore, the author presented regulative models specifically used for technology regulation that were not discussed in the named study. Regulative strategies (i) to (iii) along with the models introduced by the author were assessed in terms of their compliance with neutrality principle and sustainability goal. In the current chapter, the author also provided examples of these regulative strategies and models pursued in the DLT context by either national regulators or the EU.

As the presented research shows, the different regulative strategies and models discussed in this chapter have their shortcomings and advantages in relation to sustainability and neutrality, and wait-and-see and self-regulation seem to be often merely transitional phases on the path to another model or strategy. Furthermore, as seen in the chapter, various national regulators and the EU have taken up different strategies to respond to the challenges stemming from DLT. While in line with the Pacing Problem, the wait-and-see solution and the application of existing regulation is often the most used strategy. It is the view of the author that instead of the wait-and-see strategy, the models such as the functional-teleological interpretation and the waiver model can be adopted as these strategies can be used in a technology neutral way. Nevertheless, the application of these two models requires the respective regulators to observe, research and understand DLT in a similar way as they need to do the impact assessment when designing any new regulation.

Furthermore, the GDPR model, self-regulation and polycentric coregulation models seem to grant a certain level of sustainability and flexibility that allows regulators or multi-stakeholders to iterate technology neutral regulatory responses to the fast-paced technological and use-based changes that DLT brings about. These models challenge the balance between legal certainty and sustainability but allow the market players themselves be involved in rule-making and often also in the enforcement. This development is based (as also portrayed by the Pacing Problem) on the inability of regulators to keep up with the fast paced technological and high level of agility that is needed to support innovation. Therefore, soft law and hard law functioning together in a Hagemann's "quasi-regulatory

open-ended regulation" that includes codes of conducts, standards and guidelines that are developed by the market or regulators.[384]

The code-based regulation discussion presented in the chapter merely opened the door to this wide and fast-paced developing topic that could soon find a number of applications in developing personalized algorithm-based regulation. As a result of these presented models, the author suggests to recognize that regulators are also intermediaries that DLT is potentially able to replace both in law-making and also in compliance enforcement.

This chapter showed that, upon choosing a regulative strategy, regulators must first aim to understand (i) the technology and (ii) the intention of the regulator with regulation. As described in Chapter 2, after conducting a functional analysis and identifying functional equivalence, the principle of technology neutrality calls for effects equivalence to follow. Effects equivalence can be secured in two ways: (i) under existing regulation or (ii) by adapting existing regulation. The first alternative requires not only waiting and seeing, but also action - to interpret existing regulation in a functional-teleological way or to apply the waiver solution suggested on the basis of the sub-principle of functional equivalence by Furrer and Müller. The second alternative is to adapt existing regulation in a sustainable way, thus securing DLT neutrality.

Lastly, the EU-developed Digital Finance Package along with the MiCA Proposal and the Pilot Regime show that the different regulative strategies and models described above have been considered and employed to respond to DLT challenges. As mentioned, the Pilot Regime is nothing short of a revolutionary instrument, as it is a directly applicable customized list of exemptions from compliance requirements based on specific DLT applications. The Regime shows the willingness of the EU regulator to be flexible and iterate in their regulations and clearly aims for sustainability and adaptation to the needs of distributed infrastructure. However, both the MiCA Proposal and the Pilot Regime address the financial sector and, as shown above, DLT has an array of use cases across sectors and is not only a financial sector tool. This means that the national regulators along with EU regulators need to come up with regulative strategies to address non-financial regulation and the wider regulatory framework of the digital society in a technology neutral and sustainable way. Considering that DLT, after all, is a globally used technology and that crypto-assets usually also target global markets, the author briefly discussed the code-based regulation presented by previous research qualifying it merely as a transport layer or a delivery tool of content. Nevertheless, this regulative delivery measure is an alternative to consider when considering the expansion of DLT-specific regulative initiatives.

The chapter aimed to find an answer to the research question: how to ensure DLT neutrality in regulation? This chapter addressed the research question on a foundational level. This means that, in responding to this question, regulators should not only search for the response on how to amend a certain specific pro-

[384] ibid, p. 47.

vision in a fragmented and isolated context of one specific DLT use case, but there should be a wider perspective considered. Furthermore, the choice of regulative strategy and the models therein should consider the wider context of the DLT, specifically its functions and potential to replace intermediaries. The chapter is a portrayal of alternatives and is not arguing for any specific regulative strategy or model as all of these should be considered as part of impact assessment research. Nevertheless, all regulators should take it as their goal to ensure DLT-neutrality sustainably and choose carefully the regulative model or models for achieving this goal considering the strengths and weaknesses of these alternatives. As said, many of these strategies and models can be utilized in parallel or to complement each other and none of these can be regarded as an end result but rather as a constant work in progress.

The following chapter presents an analysis of the chosen use cases of DLT on the basis of the principles of technology neutrality and the sub-principle of functional equivalence in order to identify the specific biases in specific existing regulation against DLT. Upon discovering non-compliance with the principle of technology neutrality, the author suggests sustainable and DLT-neutral regulative strategies on the basis of the selection of regulative strategies provided in this chapter. Therefore, the overview provided in this chapter should be regarded as relevant to finding sustainable and neutral solutions to the functional analysis conducted in Articles I–III and the following chapter.

IV APPLICATION OF THE PRINCIPLES OF TECHNOLOGY NEUTRALITY AND FUNCTIONAL EQUIVALENCE IN DLT USE CASES

In this chapter the author applies the principles introduced earlier in this dissertation to a selection of DLT use cases and upon identifying non-compliance explores how to resolve the non-compliance on the basis of the regulative strategies and models presented above. The selection of use cases is related to different substantive regulation from private – and public law and the aim of the choice of these use cases is to provide an overview of different sectors where DLT can be used and to show that bias and causes for bias vary per use case.

The discrimination can be either apparent, such as the preferred treatment of existing technology, or non-apparent, such as the involvement of centralized intermediaries in order to gain trustworthiness without any consideration for the technology's functions. The problem with such discrimination is the effect on the development of the technology and its applications. If the requirements of the regulation render the advantages of the new technology useless, the technological innovation has lost all of its assets.

The current chapter includes the analysis of the three DLT use cases as problem-clusters and the respective cluster-based existing regulation for application of the technology neutrality principle and identification of bias against DLT in these regulatory frameworks.

4.1 Bitcoin exchange use case

The use case under examination is related to the operation of an exchange service provider of virtual currency (bitcoin) to and from fiat currency. The analysis is based on two court cases during the period from 2013–2016, one originating from Estonia (*de Voogd*) and the other from Sweden (*Hedqvist*), and the then existing regulation of Estonia and the EU. The CJEU has not addressed the issue of qualification of bitcoin or cryptocurrency in cases other than *Hedqvist*. In the use case analysis, the author uses the problem-cluster approach and delves into the existing regulation valid at the time to be able to test the compliance of the existing regulation with the principle of technology neutrality. In the examination of this use case, the author explores the categorization of bitcoin and bitcoin exchange-service providers on the basis of the then existing regulation under different versions of the Money Laundering and Terrorist Financing Prevention Act (MLPA)[385] of Estonia, different versions of the AML Directive (also referred

[385] Money Laundering and Terrorist Financing Prevention Act of Estonia [*rahapesu ja terrorismi rahastamise tõkestamise seadus]* – RT I 2008, 3, 21(MLPA I), Money Laundering and Terrorist Financing Prevention Act [*rahapesu ja terrorismi rahastamise tõkestamise seadus]* – RT I 06.07.2016, 13 (MLPA II) and Money Laundering and Terrorist Financing Prevention Act of Estonia [*rahapesu ja terrorismi rahastamise tõkestamise seadus]* – RT I, 17.11.2017, 2 (MLPA III).

to as AMLD)[386] and different versions of the VAT Directive.[387] The research question addressed in the current DLT use case is whether the anti-money laundering regulation in Estonia and its application to bitcoin and its traders was technologically neutral in a similar manner to the VAT regulation and its application to bitcoin and its traders in the EU? As the respective regulation analysed based on Estonian law is no longer in force, the research conducted is valuable for the purpose of identifying biases in the respective regulations against bitcoin and its traders that were the grounds for the difference in the treatment of bitcoin and its traders under Estonian anti-money laundering regulation.

4.1.1 Description of the problem

The legal problem related to DLT in this use case is (i) the treatment of a DLT output – bitcoin – in comparison with the treatment of fiat currency and (ii) the treatment of bitcoin exchange service providers in comparison with fiat currency exchange service providers. The substantive law focus in this use case in relation to the treatment of bitcoin exchange service providers is based on the MLPA, the AMLD and the VAT Directive. The problem addressed is the difference in the treatment of these categories and the bias for centralized system output as the cause for the difference in treatment.

The court cases analysed were based on similar facts that took place approximately at the same time (2012–2015) in different jurisdictions, although the core dispute was in relation to different substantive law. The individuals involved were either considering or accused of operating a virtual currency-fiat currency exchange service platform.

In the case of *Hedqvist*, the individual planned to buy and sell bitcoin as a trader and profit from the exchange rate difference. In search of legal certainty, he asked the Swedish Revenue Law Commission for clarification on whether his activities would be tax exempt, similar to the same activity if it were conducted

[386] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) OJ L 309, 25.11.2005, p. 15–36 (hereinafter: AMLD). Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) (hereinafter: the 4th AML Directive or AMLD), OJ L 141, 5.6.2015, pp. 73–117. On 30 May 2018 the 4th AMLD was amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) (hereinafter: the 5th AML Directive or AMLD) PE/72/2017/REV/1, OJ L 156, 19.6.2018, pp. 43–74.

[387] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax OJ L 347, 11.12.2006, p. 1–118 (VAT Directive).

with fiat currency on the basis of the VAT Directive and relevant Swedish national regulation. In essence, the dispute, which was sent for preliminary ruling to the CJEU, was about whether bitcoin should be qualified as equal to legal tender and whether transactions with bitcoin should be qualified as equivalent to fiat currency for the purpose of VAT-related obligations.

In the case of *de Voogd*, the individual was accused of already operating a bitcoin exchange platform and the essence of the dispute was related to whether bitcoin can be treated equally with fiat currency or whether it falls under the *sui generis* category of 'alternative means of payment' which existed under the then existing regulation. The qualification under the *sui generis* category would have subjected the operator to more strict compliance requirements under anti-money laundering regulation.

4.1.2 Statement set for defence

For the purposes of value-added taxation regulation, bitcoin (as a virtual currency) and fiat currency are considered functionally equivalent under *Hedqvist* ruling and granted effects equivalence under VAT regulation. Furthermore, the service of exchange with virtual currency and that with fiat currency are functionally equivalent and should be granted effects equivalence under the compliance regulation with consideration for the specifics of DLT. Equivalence was established under the *Hedqvist* ruling for the purposes of the treatment of the traders with bitcoin and fiat currency. Similar treatment of bitcoin should have been granted for bitcoin and its traders under anti-money laundering regulation under Estonian law.

4.1.3 Reasoning

To ease the understanding of the reasoning the section on reasoning is divided into two subsections based on the two different court cases discussed in Article I as follows.

4.1.3.1 Hedqvist

Mr Hedqvist, as the potential operator of the currency exchange platform, was seeking to understand what the VAT treatment of bitcoins and the exchange service provider activity were under the Swedish law and sought legal certainty and clarity from local tax authorities. The comparative analysis executed by AG Kokott of multiple language versions of Article 135 (1)(e) of the VAT Directive[388] showed that the text of the existing regulation was ambiguous and not transparent, as in some languages the text of the Article referred to the term 'currencies',

[388] Opinion of Advocate General Kokott delivered on 16 July 2015 in *Hedqvist*, para 34.

which could include both centralised and decentralised currencies and, in other language versions, the Article was less neutral[389] in regard to the issuer and the issuing process of the currency and consequently resulted in excluding virtual currencies from its scope. However, as stated in earlier cases by the CJEU, "the concepts used in that provision must be interpreted and applied uniformly in light of the versions in all languages of the European Union".[390] The English version of the text afforded VAT exemption to:

> "transactions, including negotiation, concerning currency, bank notes and coins used as legal tender, with the exception of collectors' items, that is to say, gold, silver or other metal coins or bank notes which are not normally used as legal tender or coins of numismatic interest".[391]

On the basis of the VAT Directive and the national regulation, the Swedish Revenue Law Commission (the Commission) regarded bitcoin as "a means of payment used in a similar way to legal means of payment", which according to the Commission was also an interpretation that was consistent with the "objective of the exemptions laid down in Article 135(1) (b)–(g) of the VAT Directive, namely, to avoid the difficulties involved in making financial services subject to VAT."[392] On the basis of this qualification, the Commission granted bitcoin equal treatment to that of fiat currency on the grounds that bitcoin functions equivalently as any other means of payment, including legal tender. Consequently, according to the author, the Commission's interpretation complied with the principle of technology neutrality and its sub-principle of functional equivalence by treating the categories of bitcoin (as virtual currency) equivalently to those of fiat currency for the purposes of VAT regulation.

Unfortunately, the Swedish tax authority (*Skatteverket*) disagreed with the Commission, stating that the VAT exemptions did not apply to bitcoin as it was not legal tender. The respective authority stated that the VAT exemptions of the VAT Directive applied only for fiat currency that was legal tender and not to any other means of payment, such as virtual currency. This led the case to go to the CJEU for a preliminary ruling under the VAT Directive.

The CJEU used the teleological and functional interpretation of the VAT Directive aiming to identify the aim of the existing regulation, stating that "the transactions exempt from VAT under those provisions are, by their nature,

---

[389] English version 'currency, bank notes and coins' referring to 'currency' in the singular – meaning that as long as one side used fiat currency the wording was inclusive, German version used the term 'Devisen' meaning foreign currencies in plural meaning that both currencies must be fiat currencies, the Italian and Finnish versions did not even require that any of the currencies be legal tender meaning that also transactions with no fiat currencies included could be covered by that Article. Veerpalu (n. 85).

[390] *Hedqvist*, para 45. See also *Velvet & Steel Immobilien*, CJEU Case C-455/05, paragraph 16 and the case-law cited, and *Commission* v *Spain*, CJEU Case C-189/11, paragraph 56.

[391] Article 135(1) (e) of the VAT Directive.

[392] *Hedqvist*, para 17.

financial transactions"[393] and "the exemptions laid down by Article 135(1)(e) of the VAT Directive are intended to alleviate the difficulties connected with determining the taxable amount and the amount of VAT deductible, which arise in the context of the taxation of financial transactions".[394] The CJEU was of the opinion that bitcoin as a virtual currency "is a direct means of payment between the operators that accept it"[395] and any transactions with bitcoin are financial transactions.[396] Such conclusion is coherent with the VAT Directive's intent, as the aim of the exemption – alleviating the difficulties connected to the determination of taxable amount – is equivalent in relation to bitcoin as to legal tender.[397]

The author concludes that with this line of argument, the court addressed the effects equivalence or the equivalence of outcome, stating that it "follows from context and the aims of Article 135(1)(e) that to interpret that provision as including only transactions involving traditional currencies would deprive it of part of its effect."[398]

Consequently, the CJEU ruled in the *Hedqvist* case that according to "the requirements of the principle of fiscal neutrality inherent in the common system of VAT",[399] transactions with bitcoin as financial transactions must enjoy equal treatment with other financial transactions for the purposes of VAT treatment. The ruling, in the opinion of the author, is in compliance with the technology neutrality principle, including its sub-principle of functional equivalence.

In order to reach this position, the CJEU, Advocate General Kokott (AG) and earlier also the VAT Committee needed to examine the functions of bitcoin. To that effect, AG stated that currencies used as legal tender "have no other practical use than as a means of payment"[400] and, therefore, "that which applies for legal

---

393 ibid, para 37.

394 ibid, para 48.

395 ibid, para 42.

396 The CJEU stated that: "Transactions involving non-traditional currencies, that is to say, currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to a transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions." ibid, para. 49.

397 In the ruling, the CJEU accepts the argument of Mr Hedqvist that "the case of exchange transactions, in particular the difficulties connected with determining the taxable amount and the amount of VAT deductible, may be the same, whether it is a case of the exchange of traditional currencies, normally entirely exempt under Article 135(1)(e) of the VAT Directive, or the exchange of such currencies for virtual currencies with bi-directional flow, which – without being legal tender – are a means of payment accepted by the parties to a transaction and vice versa." ibid, para 50.

398 ibid, para 51.

399 *Hedqvist*, para 35.

400 Opinion of Advocate General Kokott in *Hedqvist*, para. 14.

tender should also apply for other means of payment with no other function than to serve as such"[401] as, "for VAT purposes, they perform the same function".[402]

Without any assessment visible in the ruling, the court contended that "it is common ground that the 'bitcoin' virtual currency is neither a security conferring a property right nor a security of a comparable nature"[403] and also "it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment".[404]

In the ruling, the earlier analysis of the VAT Committee on bitcoin was not used as a basis for qualification, but in order to understand the scope of functional analysis that needs to be conducted, the alternative considerations of the Working Papers should be considered. The Committee considered the qualification of bitcoin as "(i) electronic money; (ii) a currency; (iii) a negotiable instrument; (iv) a security; (v) a voucher; or (vi) a digital product".[405] In the October 2014 analysis, the VAT Committee dismissed bitcoin from being e-money, currency, a security and a voucher and, consequently, a negotiable instrument or a digital product being the runner-up categories without a single winner. It was unclear whether for the decision of the Committee to consider bitcoin a digital product (electronically supplied service) was regarded as "a step too far". The other category suitable for bitcoin was referred to as a negotiable instrument described on the basis of CJEU ruling *Granton Advertising*[406] as "a right to claim a sum of money, closely linked to a payment instrument".[407]

In April 2015, the VAT Committee issued another Working Paper analysis on the VAT treatment of bitcoin,[408] under which the alternative categories for qualification were the same as the two alternative categories for bitcoin; however, the digital product was examined more than it was earlier.

In the post-*Hedqvist* Working Paper No. 892 issued by the VAT Committee in February 2016, none of these two alternative categories suitable for bitcoin (negotiable instrument or digital product) were further discussed, as the court

---

401 ibid.

402 ibid, para 15.

403 *Hedqvist*, para 55.

404 ibid, para 52.

405 European Commission. Directorate-General Taxation and Customs Union, VAT Committee (Article 398 of Directive 2006/112/EC), Working Paper No. 811, Question concerning the application of EU VAT provisions, Subject: VAT treatment of Bitcoin, 23 October 2014, p. 5.

406 *Granton Advertising BV versus Inspecteur van de Belastingdienst Haaglanden/kantoor Den Haag*, CJEU C-C-461/12, Judgment of the Court (Fifth Chamber) 12 June 2014.

407 VAT Committee (n. 385), p. 23.

408 European Commission. Directorate-General Taxation and Customs Union, VAT Committee (Article 398 of Directive 2006/112/EC), Working Paper No. 892, Question concerning the application of EU VAT provisions, Subject: CJEU Case C-264/14: Bitcoin, 4 February 2016.

regarded bitcoin "a direct means of payment between the operators that accept them"[409] and equated bitcoin and legal tender currencies for VAT purposes.[410]

Consequently, the author concludes that in the earlier working papers, the VAT Committee used textual interpretation of the wording of Article 135 (1) (e) and allowed the terminology to restrict the effect of the VAT Directive. By failing to consider the functional – and teleological interpretation of the exemption grounds, the VAT Committee interpreted the legal norm in a technologically discriminatory way, which the CJEU later ignored and rectified. The author points out that such analysis of functions and effect of the regulation that was conducted by the CJEU and earlier by the VAT Committee was needed and should be executed by each regulator upon trying to implement and enforce the applicable existing regulation.

4.1.3.2 de Voogd

In the *de Voogd* case, the dispute was similarly related to bitcoin qualification under the existing regulation in Estonia. The Money Laundering and Terrorist Financing Prevention Act of Estonia valid at the time of proceedings (MLPA I) stipulated the *sui generis* category 'alternative means of payment'[411] in subsection 4 of § 6 of MLPA I and subjected the providers of alternative means of payment services to this customized regulation. The legal norm stipulating the *sui generis* category in MLPA I was worded broadly and under subsection 4 of § 6 of MLPA I included the following definition:

> "funds of monetary value by which financial obligations can be performed or which can be exchanged for an official currency."[412]

Furthermore, the service provider who used the alternative means of payment was defined in subsection 4 of § 6 of MLPA I as "a person who in its economic or professional activities through communications, transfer or clearing system buys, sells or mediates"[413] this category of funds.

The supervising authority for MLPA I is the Financial Intelligence Unit of the Estonian Police and Border Guard (FIU), who notified Mr de Voogd, who operated the domain btc.ee, claimed that he was selling and buying bitcoin to interested parties. The FIU qualified Mr de Voogd as a provider of alternative means of payment service and requested, with precept no. 1-9/1011, that he provide evidence of his compliance with the compliance measures customized for 'alternative means of payment' service providers under MLPA I.

---

409 *Hedqvist*, para 51.

410 VAT Committee (n. 408), p. 7.

411 Subsection 4 of § 6 of MLPA I.

412 ibid.

413 ibid.

The case ended up in administrative court as Mr de Voogd challenged this interpretation as well as due to the applicability of MLPA I to his activities. According to the Supreme Court ruling in the *de Voogd* case, the court concluded in favour of the FIU, reasoning that "on the basis of the wording of the legal norm, the providers of the cryptocurrency exchange service are, under the valid law, considered the providers of an alternative means of payment service."[414]

As the grounds for such conclusion, the Supreme Court identified certain characteristics: (i) bitcoin can be exchanged to fiat currency; (ii) on exchange platforms, bitcoin has an exchange rate measurable in money; and (iii) instead of official currency, bitcoin can be used as a means of payment on the basis of transactions. However, no separate functional analysis of bitcoin or its difference from fiat currency was conducted. No functional interpretation of the specific legal norm was made in the ruling to assess whether the legal norm constructed prior to DLT was discriminatory or proportional for the use case of DLT. Also, the characteristics of alternative means of payment service providers were not explored in the ruling. The court identifies that bitcoin has the sole function of being used as means of payment but does not state that bitcoin is functionally equivalent to fiat currency.

The *de Voogd* Supreme Court ruling was issued on 11 April 2016 and the *Hedqvist* CJEU ruling on 22 October 2015 (AG opinion on 16 July 2015). In the *de Voogd* case, the Supreme Court did not discuss, mention or refer to the *Hedqvist* ruling or AG's opinion or mention why the ruling is not relevant.

4.1.3.2.1 Alternative means of payment

The respective legal norm on the new *sui generis* category was termed very broadly, using as a definition the wording "funds of monetary value by which financial obligations can be performed or which can be exchanged for an official currency". The definition of the *sui generis* category of 'alternative means of payment' is as vague as the definition of crypto-assets based on the MiCA Proposal, which defines 'crypto-asset' as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology";[415] however, the MiCA Proposal has sub-categories of crypto-assets in order to explain the types of crypto-asset for which the regulator envisions to provide more content. Contrary to the crypto-assets *sui generis* category, the 'alternative means of payment' category under MLPA I had no sub-categories to explain neither its scope nor the intention of the regulator to treat it differently from fiat currency.

---

[414] *de Voogd*, para 5.4.

[415] Article 3 Section 1 subsection (2) of the MiCA Proposal.

According to the explanatory memorandum[416] of the respective legal act, the *sui generis* category was introduced on the basis of concerns raised by the FATF, the IMF and the UN Office of Drugs and Crime over risks stemming from the category referred to as 'Internet money'. 'Internet money' was described as enabling "instantaneous, easy, safe and anonymous transfers of monetary value".[417] The explanatory memorandum of the respective legal act in the context of Internet money discussed the existence of electronic purses (wallets) and e-silver and e-gold potential payment methods.

Under Directive 2005/60/EC (AMLD) no such category for an alternative means of payment service provider as an obliged entity category was introduced in the EU. Consequently, this specific *sui generis* category in MLPA I was introduced in Estonia not on the basis of EU law but as an initiative of the national regulator in order to address e-silver and e-gold payment methods and 'Internet money'.

The respective version of the MLPA was adopted by the parliament on 19 December 2007 and entered into force on 28 January 2008. The whitepaper for bitcoin, as the first example of cryptocurrency, was published on 31 October 2008.[418] As explained by Kiel Institute, bitcoin is merely a limited subcategory of all virtual currencies:

> "Cryptocurrencies are a special case of digital/virtual currencies. While cryptocurrencies use cryptographic functions in the processes of e.g. authorizing or verifying transactions, digital currencies include all currencies that are implemented on computer systems (including, for example, in the form of a simple database). Cryptocurrencies can therefore be considered a special case of digital currencies. Characteristic features include the absence of a central counterparty, non-discriminatory public access, and security against fraudulent spending."[419]

Furthermore, as pointed out in the proposal for the Directive 2015/849 (5th AMLD) by 30 May 2018, which was the first legal instrument in the EU that introduced regulation for virtual currencies and their exchange platforms as obliged entities,

---

[416] 137 SE Eelnõu seletuskiri, Seletuskiri rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu juurde (Explanatory Memorandum of Draft Law 137 SE on Money Laundering and Terrorism Financing Prevention Act 2007). <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/046802d9-335d-415b-c4a1-650aa487eb33/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus> accessed 02 May 2020.

[417] Veerpalu (n. 86), p. 69.

[418] Marie Huillet, '11 Years Ago Today Satoshi Nakamoto Published the Bitcoin White Paper' (Cointelegraph 31 Oct 2019) [blog]. <https://cointelegraph.com/news/11-years-ago-today-satoshi-nakamoto-published-the-bitcoin-white-paper> accessed 21 November 2020.

[419] Kiel Institute 'Virtual Currencies Monetary Dialogue'. In-depth analysis requested by the ECON committee. Study for the World Economy Directorate-General for Internal Policies, (July 2018) Policy Department for Economic, Scientific and Quality of Life Policies, PE 619.016. <https://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf> accessed 21 November 2020.

no Member State had any legislation on virtual currencies (nor had ever notified of having any) until 2018.[420]

Lastly, before Mr *de Voogd* was approached by the FIU case, the regulator in Estonia (e.g., the Estonian central bank and the Financial Supervisory Authority (FSA)) had on several occasions stated in the media or press releases that virtual currencies, cryptocurrencies and bitcoin, along with the activity of exchanging them, is unregulated and does not fall under supervision in Estonia.[421] Only after fiat currency exchange service provider Tavid, operating on the Estonian market, submitted a query on 23 January 2014 to the regulator seeking legal certainty as to the regulation of bitcoin exchange service providers[422] did the regulator's communication and also actions change. The FIU contacted Mr de Voogd for the first time on 13 February 2014 requesting proof of compliance with anti-money laundering regulation. Only nine days after Tavid's query, the regulator (specifically the FIU) for the first time stated publicly that it considered bitcoin to fall under the alternative means of payment regulation under MLPA I. Mr de Voogd later inquired from the FIU why the regulator did not inform the public of their interpretation of the law earlier, to which the FIU responded "we just did not saw [sic] the need for composing something like that earlier".[423]

4.1.3.2.2 Extension of AMLD obligated entity categories

The AMLD is a minimum harmonisation directive, leaving the EU Member States discretion to issue stricter regulation and widen the scope of regulation "to counter the important threats they maybe face with at the national level".[424] Consequently, under Article 4 of the AMLD:

1. Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the institutions and persons referred to in Article 2(1), which engage in

---

[420] MiCA Proposal, p. 12.

[421] Rainer Saad, 'Mida arvab Eesti Pank bitcoinist?' [*What does the Bank of Estonia think of bitcoin?*], (Äripäev 18 December 2013) <https://www.aripaev.ee/uudised/2013-12-18/mida_arvab_eesti_pank_bitcoinist>; Financial Supervisory Authority, 'Virtuaalraha pakkujad ei kuulu järelevalve alla' [*Providers of virtual currency do not fall under supervision*], (Website of Financial Supervisory Authority 05 February 2014) <http://www.fi.ee/index.php?id=21561> accessed 14 November 2018.

[422] Kadri Inselberg, 'Tavid kaalub Bitcoiniga kauplemise alustamist' [*Tavid is considering trading Bitcoins*] (Postimees.ee 23 January 2014) <https://majandus24.postimees.ee/2671592/tavid-kaalubbitcoiniga-kauplemise-alustamist> accessed 14 November 2018.

[423] Btc.ee website. Court documents. <http://btc.ee/appeal.html> accessed 22 December 2018.

[424] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance){SWD(2013) 21 final} {SWD(2013) 22 final}, p. 9.

activities which are particularly likely to be used for money laundering or terrorist financing purposes.

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

The Article 4 notification obligation is a flexible way to expand the directive's scope, which is certainly in line with the sustainability goal of the technology neutrality principle, but for legal certainty and further development purposes requires states to notify the Commission of new categories of obligated entities. As the Supreme Court also confirmed, no such notification had been sent by Estonia.[425]

The Supreme Court stated that the fact that Estonia did not inform the Commission that Article 4 of the AMLD provides grounds for extension "has no relevance as to the validity and applicability of the regulation". The Supreme Court also noted that Article 5 allows the EU Member State to "adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing". The Supreme Court concluded that the Articles 4 and 5 of the AMLD are "clearly understandable and sufficiently clear" and, consequently, there is *acte clair* and there is no basis or reason to request preliminary ruling on these norms by the Court of the European Union.[426]

To the author, however, first, it remains unclear whether the extension of the scope of the AMLD under Article 4 (1) of the AMLD is allowed for a global phenomenon such as bitcoin or whether the extension option was intended to counter important threats Member States may be faced with at the national level. Second, if it is not allowed to extend the AMLD to a global phenomenon such as bitcoin, does the extension become non-compliant with the AMLD? Furthermore, does Article 5 of the AMLD allow stricter provisions in the field covered by the AMLD only within the scope of the obliged entities named in the AMLD (the wording is "stricter provisions in the field covered by this Directive") or are stricter provisions also allowed for the obliged entities to which the AMLD scope is extended? Lastly, if stricter provisions are allowed for obliged entities not covered by the AMLD, does Article 5 allow stricter provisions and difference in treatment based on the technology used for the transfer of funds?

Given these circumstances as provided above and the aim of the freedom to provide services, freedom establishment in the EU, the general proportionality[427] and non-discrimination principle of administrative law and procedure,[428] and § 14

---

[425] *de Voogd*, p. 18.

[426] *de Voogd*, p. 18.

[427] § 3 section 2 of the Administrative Procedure Act, the administrative acts and measures shall be appropriate, necessary and proportionate to the stated objectives. Administrative Procedure Act [*haldusmenetluse seadus*] – RT I 2001, 58, 354; RT I, 13.03.2019, 55.

[428] SCALC judgment, 17th February 2003, case 3-4-1-1-03, p. 14.

of the Constitution[429] that obligates the legislature, the executive, the judiciary, and of local authorities, to guarantee the rights and freedoms provided in the Constitution, the author suggests that in order to support legal certainty the Supreme could have responded to these questions in the *de Voogd* ruling or in order to find legal certainty also in the EU on this issue the Supreme Court could have clarified the issue on the basis of a preliminary ruling request to CJEU.

4.1.3.2.3 Difference in treatment

Under subsection 8 of § 15 of MLPA I, the person who was qualified as to providing the alternative means of payment service was obligated to identify the customer while being present in the same place as the customer (meaning face-to-face meetings) and the measures needed to be taken

(a) upon initiation of the business relationship; and
(b) in the case of transactions with the customer exceeding EUR 1000 a calendar month.

Under subsection 2 of § 12 of MLPA I, the provider of fiat currency exchange services needed to take similar measures as point (a) but, in regard to point (b), only when transactions with the customer exceed EUR 15,000 per transaction. This meant that the alternative means of payment exchange service provider was treated differently than the fiat currency exchange service provider due to the risks associated with 'Internet money' and e-gold and e-silver.[430]

Consequently, as pointed out, the AML compliance requirements for fiat currency exchange service providers and alternative means of payment service providers have substantial differences. For alternative means of payment, the transaction amounts were grouped together for an entire calendar month and AML compliance was triggered at a very low level of 1,000 euros' worth of transactions per month. This means that the difference in transaction amounts that were triggering compliance were more than 15 times lower for bitcoin than fiat currencies without any proper explanation for such difference in the explanatory memorandum of the legal act. The negative effect of the qualifying bitcoin under the *sui generis* category was the face-to-face identification requirement starting from a very low monetary value which meant that for virtually every transaction the user and the service provider should have met in person.

---

[429] Constitution of the Republic of Estonia [*Eesti Vabariigi Põhiseadus]* – RT I, 15.05.2015, 2.

[430] 137 SE Eelnõu seletuskiri, Seletuskiri rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu juurde [*Explanatory Memorandum of Draft Law 137 SE on Money Laundering and Terrorism Financing Prevention Act 2007*]. <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/046802d9-335d-415b-c4a1-650aa487eb33/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus> accessed 02 May 2020.

The Supreme Court conceded with the position that the effect of this compliance measure of the practice is unclear and instructed the legislature to consider assessing the impact of the specific legal norms in question.[431] Said compliance measure certainly had the effect of completely stopping any such bitcoin exchange business in Estonia. This was due to the fact that bitcoin was a globally used virtual currency existing only virtually and the clients interested in the currency were not only the individuals or businesses in close proximity to one another. Such circumstances made the face-to-face identification requirement difficult to comply with.

4.1.4 Findings and alternative courses of action

The research question addressed in the current DLT use case was whether the anti-money laundering regulation in Estonia and its application to bitcoin and its traders was technologically neutral, similarly to the EU VAT regulation and its application to bitcoin and its traders in the EU? The separation of a new *sui generis* category such as 'alternative means of payment' from fiat currency in MLPA I cannot be regarded as contrary to the principle of technology neutrality. However, considering the CJEU categorisation of bitcoin as functionally equivalent to fiat currency for, VAT purposes under the EU law in *Hedqvist*, the difference in the treatment of fiat currency and 'alternative means of payment' for AML compliance purposes can be considered contrary to the principle of technology neutrality under Estonian law.

Considering that in *Hedqvist,* the functions of bitcoin and those of fiat currencies were regarded by the CJEU as functionally equivalent for VAT purposes, then for the purposes of assessing the compliance of MLPA I and the 'alternative means of payment' regulation with the technology neutrality principle, it is necessary to assess whether the Supreme Court in the *de Voogd* case identified any grounds related to anti-money laundering regulation objectives that justified this difference in treatment. Considering the statements of the Supreme Court in the *de Voogd* ruling, the court was not of the opinion that the treatment was proportionate to, sustainable or considerate of the technological and global use aspects of bitcoin.[432] The court clearly states these concerns in the ruling, but, unfortunately, these findings did not affect the ruling to apply the relevant existing regulation for alternative means of payment.

The effects of MLPA I on bitcoin and its traders were not equivalent to those on fiat currency and its traders, although, according to *Hedqvist*, effects equivalence was demanded from VAT regulation, the same was not by AML regulation. The author agrees with the Supreme Court in *de Voogd*, that the AML compliance requirements were not considerate of technological innovation, the features of bitcoin and its global use. It is the opinion of the author that on the

[431] *de Voogd,* para 25.

[432] ibid*,* paras 26–28.

basis of the principle of technology neutrality, it is the task and obligation of the regulators, including the executive authority and the judiciary, to evaluate the effect of existing regulation on the new technology or its use cases in order to make sure that the effect does not restrict innovation and decrease competition simply for the reason that the regulators are not familiar with the new technology.

Although, in the ruling of the *de Voogd* case, the court urged the legislature (i) to consider amending the existing regulation in order to take into consideration the characteristics of bitcoin transactions, (ii) to assess the effect of existing regulation on this business and as a result (iii) to ensure sufficient flexibility in the regulation that applies to the innovative technology. Nevertheless, the court itself failed to interpret MLPA I in a functional-technological way, as it could have used the *Hedqvist* qualification and placed bitcoin under fiat currency compliance measures.[433] In essence, such a solution would not have been substantially different for bitcoin and its trading, as their trading would have still required face-to-face identification measures to be followed and such compliance measure could have still had the same cumbersome effect on bitcoin trading as the application of the 'alternative means of payment' compliance measures had, but at least the thresholds for these measures to be complied with would have been higher.

Of separate importance is the value of legal certainty and clarity in relation to the *sui generis* category and the related regulation. In this legal certainty context, the court partially applied the technology neutrality principle by stating the sustainability goal as follows:

> "the obligated entity is determined on the basis of general characteristics and the law does not include reference to traders of virtual or cryptocurrencies, however, this cannot be regarded as a reason for the existing regulation to be legally uncertain. The legal act must be worded with a high-level of abstraction to ensure avoidance of gap in legislation and to ensure flexibility, the law cannot enlist all existing and future alternative means of payment."[434]

The irony of it all is that the court regards it as understandable to any 'reasonable' person dealing with bitcoin that this is regarded as a non-traditional or alternative means of payment.[435] This is ironic because the authorities had themselves constantly reassured the subjects of law that activities with virtual or cryptocurrencies were unregulated[436] and, when an incumbent inquired about it from the FIU, the FIU responded that they did not see any need for such clarification.[437]

---

[433] *de Voogd*, para 28.

[434] ibid, para 6.4.

[435] ibid, para 6.4.

[436] On 18th December 2013 Head of the Payments and Settlement Department of the Bank of Estonia, Mr. Mihkel Nõmmela: "First of all, with virtual currency schemes we have an area which, thus far, is unregulated and no authority is supervising the area of activity". Rainer Saad (n. 426).

[437] Upon Mr de Voogd inquiring from the FIU why they have not informed the public of their interpretation of the law earlier to which the FIU responded that: "We will public [sic] our

Therefore, based on the above, the author is of the opinion that, considering that:

(i) subsection 4 of § 6 of MLPA I created an additional category of obliged entity that was not established under the AMLD;
(ii) under Article 4 of AMLD, a Member State was under an obligation to inform the Commission thereof of any new categories of obligated entities;
(iii) the Estonian regulator had not informed the Commission of any new category of undertaking as obliged entities to which it has decided to extend the relevant provisions of the AMLD, including of the new category 'alternative means of payment service provider';
(iv) the regulator had repeatedly told the public through the media that bitcoin is unregulated,
(v) in the *Hedqvist* case, the CJEU had ruled that bitcoin is considered functionally equivalent to fiat currency for the purposes of EU VAT regulation and is consequently treated equivalently; and
(vi) the principle of technology neutrality is aligned with the primary purpose of the procedure in administrative courts – "to protect the rights of individuals against unlawful actions performed in the course of the exercise of executive authority" – described in subsection 1 of § 2 of the Code of Administrative Court Procedure[438] (CACP),

the Supreme Court, in line with the technological-functional interpretation goal and aiming for legal certainty, should and could have asked the CJEU for a preliminary ruling. The preliminary ruling could have addressed at least the following issues:

(a) Whether the extension of the scope of the AMLD under Article 4 (1) of the AMLD is allowed for a global phenomenon such as bitcoin or whether the extension option is intended to counter important threats the Member States may be faced with at the national level?
(b) If it is allowed, whether failure to notify the Commission under Article 4(2) of the AMLD on the extension of the regulation to a global phenomenon such as bitcoin leads to the extension not being compliant with the AMLD?
(c) If the failure to notify does not lead to non-compliance with AMLD, does Article 5 of the AMLD allow stricter provisions only for the obliged entities named in the AMLD (the wording is "stricter provisions *in the field covered by this Directive*") or are stricter provisions also allowed for the obliged

opinion regarding the matter of bitcoins on our website soon.[...] and for your information we have not kept our opinion in [sic] secret – we just did not saw [sic] the need for composing something like that earlier" (Court documents. <http://btc.ee/appeal.html> accessed 02 May 2020).

[438] Code of Administrative Court Procedure [*halduskohtumenetluse seadustik*] – RT I, 13.03.2019, 54; RT I, 23.02.2011, 3.

entities which the AMLD scope does not cover and to which the respective Member State extends the regulation?

(d) If stricter provisions are allowed for obliged entities not covered by AMLD, does Article 5 allow stricter provisions and, consequently, difference in treatment based on the technology used for the transfer of funds, such as bitcoin, which was considered for EU VAT regulation purposes under *Hedqvist* functionally equivalent to fiat currency?

As a conclusion, the analysis of the bitcoin exchange use case shows that the court itself needs to conduct functional equivalence and effects equivalence analyses and be diligent in securing the application of the principle of technology neutrality in order to not discriminate against the innovators and early adopters of any new technology, as this has a chilling effect on any development related to DLT technology and its use cases.

It is the opinion of the author that:

(i) in the *Hedqvist* case, the CJEU analysed the functions of bitcoin by conducting a functional and technical interpretation of the relevant norms and, in conclusion, applied the EU VAT Directive in compliance with the principle of technology neutrality;

(ii) in *de Voogd* case, although the court conducted a functional interpretation of the relevant norms and found these to be disproportional and unfit (point 26–28 of *de Voogd* ruling), it nevertheless upheld these discriminatory legal norms, the application of which to bitcoin and its traders did not pass the technology neutrality compliance check;

(iii) the case facts in the *Hedqvist* case show that the referring court in Sweden was interested in securing technology neutrality and legal certainty in the context of regulatory uncertainty in relation to bitcoin, and the CJEU applied the existing regulation in a functional-teleological way;

(iv) the case facts in the *de Voogd* case show that the Supreme Court was sceptical as to the suitability of the compliance measures for the DLT use case due to reasons of proportionality and confirmed that the impact of these measures on the use case (considering the face-to-face identification requirement) is unclear; nevertheless, the court still applied the existing regulation to bitcoin traders and in taking that step created legal certainty in relation to bitcoin trade in Estonia, which, due to its cumbersome compliance measures on traders, lead to all such activity being temporarily suspended until the respective regulation was amended and eventually repealed by the legislature.

As a final note, MLPA I and the respective difference of treatment that was the subject of the dispute in the *de Voogd* case were amended by MLPA II to allow online identification just a few months after the Supreme Court ruling in *de Voogd*

case.[439] Lastly, the entire regulation on the *sui generis* category of alternative means of payment was repealed along with MLPA II by MLPA III in November 2017 (1 year and 7 months after the *de Voogd* case) due to early transposition of the 5th AMLD. Though the respective regulation analysed is no longer in force, the research conducted is valuable to identify methods to reveal biases in regulation against DLT use.

4.2 Shareholder ledger use case

The second DLT use case discussed in this dissertation and in more detail in Article II is focused on the administration of a shareholder ledger for a private limited liability company (OÜ) in Estonia. To the knowledge of the author, no analysis of the use of DLT in shareholder ledger maintenance in Estonia has been previously conducted.

4.2.1 Description of the problem

DLT at its core is a ledger technology and, consequently, the wider question in relation to shareholder ledgers is whether DLT can be used to operate private or public ledgers in order to facilitate trade in shares and the liquidity of this asset. In this subsection, the author explores whether the existing regulation in Estonia allows DLT to be used for the shareholder ledger maintenance of the shares of private limited liability companies (OÜs) not registered in the central securities depository (CSD).

As stated in Chapter 1, in the EU Blockchain Study, the analysis of the MiCA Proposal and Pilot Regime has shown that regulation developed for centralised structures hinder the use of DLT. Such hindrance may present itself by either not granting DLT-based solutions effects equivalence based on functional equivalence or subjecting the functionally equivalent solution to unnecessary compliance requirements as is visible from the Pilot Regime. Consequently, the use case in question explores whether the shareholder ledger maintenance regulation addressing OÜs includes similar types of biases that result in hindrances in the use of DLT for the administration of the non-CSD shares of an Estonian OÜ.

Given the recent Digital Finance Package introduced by the EU, it is clear that the existence of DLT-based crypto-assets is changing the reality of capital markets, multilateral trading and securities settlement. Furthermore, it is antici-

[439] Act Amending the Identity Documents Act, Credit Institutions Act and Money Laundering and Terrorism Financing Prevention Act *[isikut tõendavate dokumentide seaduse, krediidiasutuste seaduse ning rahapesu ja terrorismi rahastamise tõkestamise seaduse muutmise seadus*] – RT I, 06.07.2016, 2.

pated that DLT will also substantially impact company law.[440] Consequently, the use of DLT to facilitate shareholder ledger maintenance and trading of shares for the purpose of easing trading and ledger maintenance and increasing investor protection is an equally relevant issue.[441] The present DLT use case addresses this issue in a scope limited to the maintenance of the shareholder ledgers of private limited liability companies (OÜs) in Estonia. Specifically, the current section and Article II seek to explore the existing regulation in Estonia that applies to the shareholder ledger maintenance of OÜs from the perspective of compliance with the principle of technology neutrality and in order to identify whether currently valid existing regulation holds biases against the use of DLT.

The relevance and objective of the analysis is in line with the goal of the Pilot Regime – to allow for the use of DLT to "expedite and condense trading and settlement to nearly real-time and enable the merger of trading and post-trading activities"[442] related to OÜ shares. The Pilot Regime, which surfaced only at the end of September 2020, is proposing exemptions to certain requirements of the CSDR[443] and MIFID II[444] to enable DLT to be used in the trading of financial instruments and also to allow "a DLT MTF[445] to perform some activities normally

---

[440] Florian Möslein, 'Blockchain Applications and Company Law' (2020) Legal Technology Transformation in Practice (October 27). <https://ssrn.com/abstract=> accessed 26 December 2020.

[441] As recently as in December 2020 Germany along with their Blockchain Strategy adopted a new law on DLT and securities that influences company law. See more here: <https://www.bundesfinanzministerium.de/Content/EN/Pressemitteilungen/2019/2019-18-09-joint-release-with-bmwi.html> and 'Gesetz zur Einführung von elektronischen Wertpapieren' can be found here: <https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2020/12/2020-12-16-gesetz-zur-einfuehrung-von-elektronischen-wertpapieren.html> accessed 26 December 2020. Steve Kaaru, 'Germany passes law legalizing electronic securities on blockchain' (Business Coingeek 21 December 2020) <https://coingeek.com/ germany-passes-law-legalizing-electronic-securities-on-blockchain/> accessed 27 December 2020

[442] Recital 9 of Pilot Regime.

[443] Regulation (EU) No. 909/2014 of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No. 236/2012 (OJ L 257, 28.08.2014, p. 1–72) (hereinafter: CSDR).

[444] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance OJ L 173, 12.6.2014, p. 349–496 (Market in Financial Instruments Directive, MiFID II).

[445] According to Recital 7 of the Pilot Regime, a "DLT market infrastructure should be defined either as a DLT multilateral trading facility (DLT MTF) or a DLT securities settlement system." Furthermore, according to Recital 8, "DLT MTF should be a multilateral trading facility that is operated by an investment firm or a market operator that operate the business or a regulated market and maybe the regulated market itself, authorised under Directive 2014/65/EU (Markets in Financial Instruments Directive, MiFID II), and that has received a specific permission under this [Pilot Regime]. Such a DLT MTF should be subject to all the requirements applicable to a multilateral trading facility under the framework of Directive

performed by a [central securities depository]".[446] Consequently, the EU regulator is making policy decisions and regulatory amendments to accommodate DLT use in securities settlements and trading.

Furthermore, as discussed in Chapter 3 of this dissertation, the changes brought about by the Digital Finance Package are motivated among other objectives by the goal of technology neutrality in regulation. This is a testament to the position that technology neutrality is a general principle of law and does not need to be reiterated in each separate substantive law.

Also, the use case analysis in this subsection is conducted from the perspective of the technology neutrality principle and whether the regulation is compliant with the principle, even though the principle is not specifically stated as applicable in this specific area of substantive law in Estonian regional law.

Consequently, the research question of the second use case is whether the regulation of the Estonian Commercial Code (CC) on the shareholder ledger administration of the non-CSD shares of an OÜ is technology-neutral and allows for the effective use of DLT in ledger maintenance. Shareholder ledger administration using DLT is aimed at the ease of record-keeping and trading with the respective asset. Therefore, for the purposes of the use case analysis, the regulation on ledger maintenance and share transfer is of relevance. Under Estonian law, depending on the administrator of the shareholder ledger (either the CSD or the management board), the share transfer regulation has different requirements, and the trustworthiness of the ledger data also differs. To be more specific, the shares maintained in the management board shareholder ledger have more stringent share transfer requirements than CSD-registered shares. On the basis of existing regulation, all of these more stringent requirements are waived in the case that the shareholder ledger is administered by the CSD.[447] Therefore, in the present use case analysis, it is explored whether these more stringent requirements for share transfer should be waived in the case that DLT is used for shareholder ledger maintenance by the management board and whether the entries in the DLT-based shareholder ledger should be granted effects equivalence with the entries in the CSD-maintained register.

The present use case analysis has posed a list of challenges as, since the publication of Article II, not only has the CC been amended, but also substantial amendments have been proposed by the EU in the form of the Digital Finance Package, which influences the analysis and relevance of the use case. The compendium text will address the CC amendments that have entered into force and partly also the EU initiatives under consideration at the time of writing this dissertation.

2014/65/EU (Markets in Financial Instruments Directive, MiFID II), Regulation EU No. 600/2014 of the European Parliament and of the Council (the Markets in Financial Instruments Regulation, MiFIR) or any other EU financial services legislation, except if it has been granted one or several exemptions by its national competent authority in accordance with this [Pilot Regime]."

[446] Recital 9 of Pilot Regime.

[447] Veerpalu (n. 88).

4.2.2 Statement set for defence

On the basis of the principle of technology neutrality, the regulator should not prefer a centralised ledger maintenance system, such as a CSD register, to a decentralised ledger-maintenance system, such as a DLT-based ledger. Such technology preference can be expressed in the existing regulation by (i) assigning trustworthiness to ledger entries based on their administrator and (ii) the difference in the share transfer rules applied to the shares maintained by the different ledger administrators. Any different and biased treatment of non-CSD shares recorded in a functionally equivalent DLT-based ledger granted effects equivalence. On the basis of the functional equivalence sub-principle, if the functions of a human intermediary or centralised administrator can be performed in an equivalent manner by any chosen administrator using the DLT solution, the use of such solution should receive equivalence of outcome (effects equivalence) under the existing regulation.

4.2.3 Reasoning

The shareholder ledgers contain important source information as to the power to control and govern the company. Now more than ever, shareholder ledgers are digitally maintained and, therefore, there often is no paper attached to the ownership of shares. As a result of this development, the voting rights at respective management bodies depend on the reliability of the data entered into shareholder ledgers. The ledger data entries are also the source for the right to dividends and therefore the trustworthiness of the data entries is of utmost importance. The entries must be true and the amendment process must be tamper-proof. Therefore, the ledger maintenance must be transparent and based on auditable logs and rules. As DLT is a ledger technology and permissionless ledger networks use auditable and transparent protocols for ledger maintenance, DLT seems to be a technology worth considering for maintaining shareholder ledgers.

The main substantive law addressed in this analysis is the existing regulation on shareholder ledger administration based on the CSDR, the Commercial Code (CC), the Public Information Act (IPA)[448] and the Securities Register Maintenance Act of Estonia (SRMA).[449]

[448] Public Information Act [*avaliku teabe seadus*] – RT I 2000, 92, 597; RT I, 14.11.2018, 5.

[449] Securities Register Maintenance Act [*väärtpaberite registri pidamise seadus*] – RT I 2000, 57, 373; RT I, 26.06.2017, 1.

4.2.3.1 Specifics of OÜ shareholder ledger maintenance

As regulated in § 148(6) of the CC, OÜ shares are recorded in book-entry form as required by the CSDR[450] and no share certificates are issued. Furthermore, there can only be one true source of information, meaning that there is only one shareholder ledger per business entity. To administer the shareholder ledger of an OÜ in Estonia, there are currently two options available under existing regulation:

1) Shares are registered at any central securities depository (CSD)-maintained register operating under Estonian law – so-called *CSD registered shares* or *CSD shares.*
2) Shareholder ledgers are maintained by the management board of an OÜ – so-called *non-CSD registered shares* or *non-CSD shares*.

Under Article 23 (1) of the CSDR, an authorised CSD in the EU may provide services provided that said services are covered by the authorisation. The CSD option is the lesser used of the two in Estonia, amounting to less than 5% of all OÜs.[451] Consequently, more than 95% of shareholder ledgers in Estonia are maintained by management boards. This is not unique, as management boards also maintain shareholder ledgers in the UK, Finland, Sweden, Denmark, Latvia, Germany and the Netherlands.[452]

The advantage of CSD ledger maintenance is primarily linked to the following:[453]

---

[450] Article 3(1) of the CSDR "any issuer established in the Union that issues or has issued transferable securities which are admitted to trading or traded on trading venues, shall arrange for such securities to be represented in book-entry form as immobilisation or subsequent to a direct issuance in dematerialised form."

[451] The Chamber of Notaries has data stating that in 2018 the indicator was 1.7%, yet the Explanatory Memorandum of 148 SE indicated that the % is less than 5%. Chamber of Notaries (2018). *Notarite Koja arvamus ühinguõiguse revisjoni muudatusettepanekute kohta.* Opinion on the analysis-concept paper of company law revision working group, 17 December 2018, p. 2 [online] Available from: <https://www.just.ee/> [12 January 2019]. Explanatory Memorandum for the draft law 148 SE to amend Commercial Code, Notarisation Act and Notary Fees Act (Explanatory Memorandum 148 SE). *Seletuskiri äriseadustiku, tõestamisseaduse ja notari tasu seaduse muutmise seaduse 148 SE eelnõu juurde.* Available at: <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/a771f589-ef25-4298-802b-2532822eb4b90/%C3%84riseadustiku%20muutmise%20seadus%20(osa%20v%C3%B5%C3%B5randamine)> [9 May 2020]

[452] Ministry of Justice. (2018) Ühinguõiguse revisjon Analüüs-kontseptsioon (Revision of Company Law, hereinafter Analysis-concept paper), 15 September 2018, p. 489. [online] <https://www.just.ee/sites/www.just.ee/files/uhinguoiguse_revisjoni_analuuskontseptsioon.pdf> accessed 12 January 2019.

[453] § 149 sections 4–5 of CC.

(i) Share transfer transaction requires no specific form.
(ii) Due to the freedom of form,[454] transaction costs are lower as no notary fee is applicable.
(iii) Theoretically, there is more transparency and data integrity as to ledger data and transaction history.

The latter is theoretical, as the data submitted to the CSD is still initially submitted by the same management board, whose role and responsibility was to maintain the ledger up until registration and whose role is also to update the CSD ledger data in cases other than share transfer transactions.

In effect, the difference for shareholders between the two options is still the liquidity and ease of transfer related to shares, which is in turn closely related to the form requirement for share transfers that was substantially amended in 2020 as described in the following section below. However, considering that, as described in Article II, access to the CSD alternative is limited due to fees and issues related to the difficulties of opening securities accounts in credit institutions, the option of having the management board maintain the shareholder ledger is still the most popular. Therefore, it is of relevance to examine whether management boards can employ DLT in maintaining shareholder ledgers as opposed to whether CSDs are allowed to use this technology. Furthermore, the use of DLT in the latter option has already been sufficiently addressed by the regulation suggested by the Pilot Regime.

4.2.3.1.1 Recent amendments to CC affecting ledger maintenance

Depending on the administrator of the shareholder ledger – either the CSD or the management board – the share transfer requirements are different and shareholder ledger entries are treated and valued differently. For example, the non-CSD-registered share transfer rules are more stringent than the CSD-registered share transfers. More specifically, at the time of writing Article II, both the disposition for a transfer of non-CSD-registered shares and a transaction constituting an obligation to transfer non-CSD-registered shares required a notarially authenticated transaction under § 149 Section 4 of the CC. At the same time, as stipulated in § 149 Section 5, the CSD-registered shares were and still are exempted from fulfilling such form requirement and, consequently, CSD shares can be transferred on the basis of any form of transaction. Therefore, the aim of the research presented in Article II and herein is to identify whether existing regulation should also allow for a similar exemption for non-CSD shares in the case that the

[454] Sein, K. Tehingu vorminõuded ja nende järgimata jätmise tagajärjed [*The form requirements of the transaction and the consequences of failure to abide by these requirements*], (2010) Juridica VII, p. 509; Section 77 (1) of the GPCCA; § 8(1) and § 11(1) of the Law of Obligations Act.

management board uses DLT in shareholder ledger maintenance on the basis of the functional equivalence sub-principle.

However, in between the publication of Article II and the writing of this dissertation, the existing regulation was amended. The amendments were lobbied by the startup community in Estonia and formalised into a request on 3 September 2019, which led to a draft law by 24 October 2019 and entered into force on expedited schedule on 24 May 2020. Therefore, the new version of § 149 Section 4 of the CC only requires that the disposition for the transfer of the non-CSD registered share be notarial and grants all transactions that constitute an obligation to transfer non-CSD registered shares in free form. The latter change was motivated by the burden of using notaries to conclude shareholder agreements and option agreements (as these contain obligations to transfer shares as part of drag-along, tag-along or co-sale rights), which is common practice in startup companies. Along with these amendments, there was also a limited liberation as to the disposition for the transfer agreement form. The liberation is reflected in the new regulation in the form requirement under § 149 Section 6, which currently allows the notarial requirement of the disposition for the transfer of non-CSD shares to be waived in addition to CSD-registered shares by the OÜs that meet the following conditions ('Startup Exemption'):

(i) Share capital is at least EUR 10,000.
(ii) Share capital is fully paid.
(iii) All shareholders must be in favour of this resolution to waive the notarial requirement.
(iv) The articles of association must include such waiver.

Upon meeting these conditions, the disposition for transfer transactions does not enjoy full freedom of form, instead, under § 149 Section 6 of the CC, the transfer transaction needs to be at least in a format that can be reproduced in writing.

This means that, upon the writing of this dissertation, the existing regulation has different content than it did during the writing of Article II, and the summary herein conveys said differences. Nevertheless, in both versions of the existing regulation, there are certain functions to be fulfilled, which the regulator has decided can only be fulfilled by a human intermediary, such as a notary. Given that the notarial authentication rule remains in place, the functions the notary fulfils upon authentication of these transfer contract are of interest. As explained in Article II, the notarial authentication involves four functions:

(i) *evidentiary function*[455]
(ii) *identification function* – also discussed in Article III

[455] Sein, K. (n. 454), p. 509

(iii) *warning function*[456]
(iv) *consulting function*[457]

Consequently, the existing regulation requires additional functions to be performed in the case that the ledger is administered by the management board. The amendments to share transfer regulation have an impact on non-CSD shareholders; however, currently less than 5% of the shares of OÜs are registered in the CSD and only approximately 9.6% of OÜs[458] can make use of the Startup Exemption. This leaves 85% of OÜs still struggling with the more stringent regulation on share transfer. Consequently, this majority did not experience any effects from the amendments, and the conclusions of Article II are still relevant.

4.2.3.1.2 Applicable requirements

There is no requirement of medium (form) or technology as to the management board's task of administering the shareholder ledger stipulated in existing regulation. According to § 182 Section 1 of the CC, "the management board shall keep a list of shareholders which shall set out the names, addresses, personal identification codes or registry codes and the nominal value of their shares" and, under 1^1 of the same § 182, shareholders must "immediately inform the management board about any changes in the information on the shareholders". Therefore, it appears that there are no specific or other functions required to be performed by the management board to maintain the ledger other than keeping the ledger up to date on the basis of information submitted by specific individuals – the shareholders.

The management board does not perform any identification function on the shareholders, does not collect the transfer documents (other than in cases where the other shareholders have the right of pre-emption under § 149 Section 2 of the CC) and does not validate any data, which in turn makes the regulation on ledger maintenance technology-independent, as it stipulates the content of the ledger and the obligated subject (the management board) but remains mute as to the process and functions.

---

[456] SCCLC Case No. 3-2-1-49-03 and SCCLC Case No. 3-2-1-85-04.

[457] According to Section 18(1) of the Notarisation Act "the notary shall also explain to parties the meaning and legal consequences of the transaction and the different possibilities for entry into the transaction" and "the notary shall ensure that errors and doubts are precluded and the rights of inexperienced or incompetent parties are not damaged". See also SCCLC case no. 3-2-1-49-03; SCCLC case no. 3-2-1-127-03 (2003), SCCLC Case No. 3-2-1-141-14, paras. 34–35.

[458] Appendix to the Explanatory memorandum of draft law 148 SE. [*148 SE Eelnõu Seletuskirja lisa (märkused ja ettepanekud). Äriseadustiku muutmise seaduse (osa võõrandamine) eelnõu seletuskirja juurde*] <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/a771f589-ef25-4298-802b-2532822eb4b9/%C3%84riseadustiku%20muutmise%20seadus%20(osa%20v%C3%B5%C3%B5randamine)> accessed 29 November 2020.

As discussed in Article II, under § 1^2 Sections 2 and 3 of the Securities Register Maintenance Act (SRMA), the CSD register is a database for the registration of shares, debt obligations and other securities and operations performed with such securities. The CSD maintained register is a public register belonging to the state information system and consequently falls under the legal category of database in the meaning of § 43^1 Section 1 of the IPA. The SRMA and the CSDR regulate the activity of the registrar. Under § 1^2 Section 3, the CSD is a central depository that has been granted the right to maintain the register based on § 25 of the SRMA, which grants the decision on the registrar to the respective minister who is entitled to enter into a contract under public law with the registrar for not more than ten years. The said contract is supervised by the Ministry of Finance for compliance. Furthermore, there are a number of CSDR Level 2 measures adopted which set the technical standards, settlement disciplines and prudential requirements[459] established for CSDs, creating a complex web of regulations aimed at securing settlements and harmonising regulation. As mentioned, for the purposes of allowing DLT to be used for functions performed by CSDs on securities registration and settlement under the CSDR, the Pilot Regime has been introduced by the EU regulator which creates a number of exemptions from SCDR and MIFID II requirements.

4.2.3.1.3 Replication of data in the Commercial Register

The Commercial Register is relevant in the scope of this use case because the entries in the shareholder ledgers administered either by the management board or the CSD are duplicated in the Estonian Commercial Register (CR). Under § 182 Section 7, all data in the shareholder ledger, except for the addresses of shareholders, can be examined through the CR as the data of the business file. Consequently, under the new amendments to § 182 Section 1^2 of the CC, the management board must immediately inform the CR of any changes in the shareholder ledger data unless a notary has already informed the CR of the respective change.

Unfortunately, this practice degrades the trustworthiness of all CR data, as the users do not separate which data they can trust and which data they should not trust. Such a situation has created confusion among consumers of this data, including the courts.[460] Also, the Supreme Court has regarded such entry of this

---

[459] Societe General. PUBLICATION OF LEVEL 2 MEASURES FOR CSDR [Press release]. 1 January 2017 <https://www.societegenerale.lu/en/societe-generale-luxembourg/press-release-news/press-release-news/news/publication-level-measures-for-csdr/> accessed 28 November 2020.

[460] Kõve V. Kas kinnistusraamatu ja teiste kohtulike registrite korraldus vajab reformi? [*Does the public title book and the maintenance of other registries operated by the courts need a reform?*] (2013) Juridica VII, p. 461. <https://www.juridica.ee/article_full.php?uri=2013_7_kas_kinnistusraamatu_ja_teiste_kohtulike_registrite_korraldus_vajab_reformi_&pdf=1> accessed 01 January 2018. See also Case no 3-2-1-133-11, Estonian Supreme Court (Civil Chamber), 14 December 2011, para. 24. Case no 3-2-1-163-11, Estonian Supreme Court (Civil Chamber), 22 February 2012, para. 33.

kind of data in the business file of the CR as "somewhat misleading"[461] because the data has no constitutive value in comparison with other data entered into the CSD and cannot be relied on by third parties. [462]

In essence, this duplication of ledger data in the CR is not a hindrance for DLT use *per se*, as it supports user friendliness (one-stop-shop for data), rather the question is whether DLT-based ledger data has a similar value as ledger data without CR entries. The research herein also examines this aspect for the purpose of a technology neutrality compliance check.

4.2.3.1.4 Value of ledger data

As stated by the Supreme Court, the CSD's aim is to ensure the truthfulness of data in the register and the unity of the data in the register that verifies rights and, through such activity, the CSD contributes to the protection of the rights of the shareholders.[463] The existing regulation grants shareholder ledger entries constitutive value only in cases where the shareholder ledger is administered by a CSD.[464] The CSD pulls the data directly from the securities accounts and makes this visible in the CSD register. This means that only through the use of a CSD as an administrator aggregating data is the ledger is presumed to fulfil certain functions that allow for the constitutive value of a ledger entry.

The data of CSD is a source of both positive and negative trust,[465] meaning that a person acting in good faith can rely on the data stored on the securities account to be correct and complete (negative trust means that a person acting in good faith can rely on the fact that the rights not entered in the securities account do not actually exist).[466] This gives the ledger entry constitutive value. Consequently, the function of the register maintained by the CSD is to be a trustworthy source of information on the data category (shareholders and shares) and

---

[461] "Mõneti eksitavalt kajastatakse äriregistri infosüsteemis lisaks n-ö ehtsatele registriandmetele kodukorra § 311 lg 1 p-de 4 ja 13 järgi "registrikaardiväliste andmetena" ka nõukogu liikmeid ja nende ametiaja kestust, kuid neil andmetel õiguslikku tähendust ei ole." ["*Under § 311 section 1 point 4 and 13 of the Rules of Procedure of the Court Registry Department [kohtu registriosakonna kodukord], the Commercial Register is recording additionally to real registry data also somewhat misleadingly also the members of the supervisory board and their term as the "non-registry data", although such data has no legal meaning*."] Case no 3-2-1-133-11 (2011), Estonian Supreme Court (Civil Chamber), 14 December 2011, para. 24

[462] Case No. 3-2-1-163-11 (2012), Estonian Supreme Court (Civil Chamber), 22 February 2012, para. 33; Case No. 3-2-1-133-11 (2011), Estonian Supreme Court (Civil Chamber), 14 December 2011, para. 24; Saare, K. et al, *Ühinguõigus I*, (2015) Juura, pp. 53–54.

[463] Case No. 3-4-1-3-12 (2012) Estonian Supreme Court (Constitutional Review Chamber), 6 July 2012, para. 52.

[464] § 9(2) of SRMA.

[465] Case No. 3-4-1-3-12 (2012) Estonian Supreme Court (Constitutional Review Chamber), 6 July 2012, para. 52.

[466] ibid.

the history of transactions linked to this specific data category. Consequently, the CSD is a centralised trustworthy source of information on (i) the current status of the shareholder ledger, (ii) shareholder data and (iii) the historic overview of the transactions leading to the current status.

As further explained in Article II, the entries of data on shareholders in the management board-maintained shareholders ledger, even with the CR replication, have no constitutive value, which makes share acquisition in good faith impossible for the non-CSD shares of an OÜ. The question is whether this treatment of entries in a DLT-based shareholder ledger is technology-neutral or whether the entries in the DLT-based shareholder ledger are functionally equivalent to CSD register entries and should therefore be granted effects equivalence with the entries in the CSD register.

4.2.3.2 Using DLT in shareholder ledger maintenance

Under Recital 1 of the CSDR, CSDs "contribute to a large degree in maintaining post-trade infrastructures that safeguard financial markets and give market participants confidence that securities transactions are executed properly and in a timely manner".[467] The CSDs and their registers "play an important role in maintaining investor confidence".[468] Given that the aim of the CSDR was to contribute to the openness of the internal market to cross-border securities settlement that should allow investments in all securities offered in other EU Member States,[469] the use of DLT in the maintenance of shareholder ledgers of shares could assist in targeting the same goal in relation to cross-border transactions with the non-CSD shares of OÜs. Similar path has been taken with DLT-specific adaptations in regulation both in France[470] and Germany.[471]

As shown by the Pilot Regime, which created a number of exemptions for crypto-assets trading on the internal market, and as maintained by the EU Blockchain Study and the MiCA Proposal, the compliance rules drafted for centralised structures are often unfit for the new technology built using decentralisation and distributed networks. Reed calls such unfit requirements 'legal impurities' and states that, "building those requirements into any blockchain-based system

---

[467] Recital 1 of CSDR.

[468] ibid, Recital 2.

[469] ibid, Recital 4.

[470] See more in details in Veerpalu (n. 88), p. 287.

[471] Steve Kaaru, 'Germany passes law legalizing electronic securities on blockchain' (Business Coingeek 21 December 2020) <https://coingeek.com/germany-passes-law-legalizing-electronic-securities-on-blockchain/> accessed 27 December 2020. See also discussion on the shortcomings of previous regulation and solutions DLT offers in Florian Möslein, 'Blockchain Applications and Company Law' (2020) Legal Technology Transformation in Practice (October 27) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3720222> accessed 26 December 2020.

introduces features which are not necessary for performing its core functions".[472] These legal impurities are the same as those referred to as biases by the author in this dissertation. The bias in the ledger maintenance system allocates preferential treatment to CSDs – a shareholder needs the participation of this particular trusted intermediary in order for constitutive value to be granted to the data in the ledger and freedom of form for share transfer transactions to be enjoyed.

According to Reed and others, "the primary legal function which blockchain performs is to provide reliable evidence"[473] and DLT is "a technologically 'pure' system for recording entitlements to assets and undertaking transactions relating to those assets".[474] He explains that, by this purity, he means that the technology is not specifically built to fit the requirements of the existing regulation and is purely structured as a tamper-resistant ledger not allowing the regulator (including the judiciary) "to interfere and restrict or reverse a transaction".[475] Given the purity of the ledger as to the evidentiary function, the ledger records can be trustworthy as to the entitlement of the asset, and any transaction that amends the ledger records is authorised "using the private key that corresponds to the public key recorded in the ledger, and the ledger is the definitive record of rights"[476] related to these datapoints recorded in the ledger.

As previously mentioned, the CC does not require the use of any technological or organisational measures for the maintenance of the shareholder ledger by the management board. Therefore, without a doubt, it is possible under the CC to use DLT to maintain the shareholder ledger of non-CSD shares. However, the question is: will this actually ease liquidity and transactions with shares? Unfortunately, if the CC does not enable the same waivers it allocated to CSDs to DLT-based ledgers, the positive effect that DLT use can have on shareholder ledger maintenance is rather limited. So, instead of comparing DLT-based shareholder ledger maintenance to CSD register maintenance requirements, the functional equivalence analysis in this case is conducted against the requirements that apply for non-CSD share transfers. As in the majority of cases, share transfer transactions require notarial authentication, which needs to fulfil evidentiary, identification, warning and consultation functions, a functional analysis of DLT in share transfer transactions will follow.

---

[472] Chris Reed, Uma M. Sathyanarayan, Shuhui Ruan, Justine Collins, 'Beyond BitCoin—legal impurities and off-chain assets', (2018) International Journal of Law and Information Technology 26/2, p. 160. <https://doi.org/10.1093/ijlit/eay006> accessed 28 November 2020.

[473] ibid, p. 161.

[474] ibid, p. 162.

[475] ibid.

[476] ibid.

(i) evidentiary function

According to Reed, "the main function of any distributed ledger system is to provide evidence about assets, participants and transactions between participants".[477] Given the technical functions of DLT, any ledger using DLT certainly fulfils the evidentiary function, as it is a timestamped, tamper-resistant, append-only ledger and reflects the trail of transactions in a trustworthy manner. The use of DLT for share transfers is of a higher evidentiary value than a transfer transaction agreement in a paper format or a form that can be reproduced in writing due to the use of encryption keys used as attributes in DLT-based transactions.[478] Furthermore, Article III provides an analysis of DLT-based smart contracts in the context of the typology of contract forms and argues that DLT-based smart contracts perform the functions of a contract in an electronic form.

(ii) identification function

Furthermore, as stated by Reed, the ledger also records "important attributes which are relevant to ownership but do not necessarily evidence ownership".[479] By this, Reed means attributes like a wallet address or public key that are linked to the asset and no one else; however, the one controlling the private key has control over this specific asset. Though the technology is built to link participants pseudonymously and without an identification function, as described in Article III, it is possible to use applications on DLT to fulfil the identification function.

Furthermore, if the replication of data to the CR remains, the wallet addresses or public keys can serve as security account numbers in CSD aggregation, linking the names known to the CR to the wallet address or public key. Lastly, in the context of DLT, the idea of self-sovereign identity could be considered. This means that identification data is not placed in the public domain and, in order to protect the personal data of shareholders, the identity data is actually controlled by the person whom that data identifies. This idea is discussed in more detail by Christopher Allen,[480] who proposes that "individuals should own and be in control of their own online identity".[481] It is claimed that in the digital world, "it

---

[477] Reed et al. (n. 472), p. 165.

[478] According to Reed: "distributed ledger systems produce evidence of entitlement and attributes which are of even higher evidential value than signed paper documents." Reed et al. (n. 477), p. 168.

[479] ibid, p. 161.

[480] Christopher Allen, *The Path to Self-Sovereign Identity*. (Life with Alacrity [blog], 25 April 2016). <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html> accessed 29 November 2020

[481] Reed et al (n. 472), p. 173.

is the natural evolution of online identity mechanisms"[482] and the EU has followed this evolution by introducing the EBSI platform that is implementing this concept of self-sovereign identity model in Europe in essence allowing individuals to have more control over their own identity across the national borders.[483] In line with this evolution, DLT would only allow the parties to reveal their identity to one another, thereby controlling the closed loop of information on a need-to-know basis.[484] Reed is of the opinion that regulators need to adapt existing regulation to be fit for DLT systems used to perform the identification function, otherwise these systems and the centralised practise of identification will remain in conflict and act as a deterrent to the use of DLT.[485]

(iii) warning and consultation function

As the warning and consultation functionality are not required from CSD share transactions, the question remains as to whether these functions are considered necessary for non-CSD share transactions, otherwise this differentiation is unfair treatment and not technology-neutral. As with any technology, these functions could be automated and added to DLT to a certain degree as well, though they will not be comparable to how these functions are performed by the notary.

In summary, DLT is efficient in fulfilling the evidentiary function but has to be adapted for or is unable to fulfil all of the other functions, leading to the conclusion that the existing regulation should be adapted to not differentiate between the value of data and share transfer transaction requirements in the case that the shares are maintained by a management board under DLT or by the CSD. Any difference in the treatment of OÜ shares simply due to the administrator in cases where the solutions provided by these administrators are functionally equivalent is not in compliance with the principle of technology neutrality. Consequently, as discussed, it is possible to use DLT for shareholder ledger maintenance for non-CSD shares under the CC; however, this would be pointless if share transfer transactions would still need to go through a notary. Therefore, the Estonian regulator should consider adapting existing regulation by either introducing a similar waiver for these transfer requirements as has been implemented for CSD-registered shares or altogether deleting the form requirements for the transfer of non-CSD shares.

---

[482] Andrew Tobin and Drummond Reed. *The Inevitable Rise of Self-Sovereign Identity*. Sovrin Foundation White Paper September 2016, updated March 2017, pp 6–9. <https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf accessed 29 November 2020

[483] EBSI platform. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI> accessed 02.12.2020.

[484] Reed et al (n. 472), p. 173.

[485] Reed et al (n. 472), p. 176.

Using DLT for ledger maintenance with the form requirement still intact creates a hurdle to the use of DLT that can be considered non-compliant with the technology neutrality principle. The bias identified by the author is the fact that effects equivalence (free form of share transfer and value of entry data) is attached to the subject and not a process or a set of functions. This means that the existing regulation does not attach value to the functions used in shareholder ledger maintenance or the aims these functions have or the values these functions protect, but rather waives certain requirements for CSDs and does not waive these requirements in cases where the management board uses a functionally equivalent solution. This means that the existing regulation of the CC has a bias towards centralised intermediaries, such as the CSD and the notary. The author proposes to consider extending similar waivers to DLT-based shareholder ledgers as those granted to CSD in identifying the functions shareholder ledgers must meet in order to be granted these waivers. This solution is similar to the regulative strategy used in the Pilot Regime in relation to the CSDR.

Nevertheless, considering:

(i) that the Estonian regulator considered the warning and consultation functions irrelevant for CSD-registered shares and shares meeting the Startup Exemption conditions;
(ii) that the Revision Working Group reiterated that no such form requirement for share transfer transactions exists in Finland, Sweden, Latvia, Lithuania or Delaware; [486]
(iii) the arguments used to introduce the CC amendments;
(iv) that presently 85% of all OÜs do not fulfil the conditions set for the Startup Exemption,

it remains unclear to the author why is it necessary to treat certain non-CSD shares and their transfer transactions differently from others, thereby creating a technology-favouring hurdle to the use of DLT in relation to the shareholder ledgers of the majority of OÜs in Estonia.

4.2.4 Findings

In conclusion, the shareholder ledger of CSD-registered shares has a legal validity that is not comparable to the shareholder ledger entries of the non-CSD registered shares. There is no effects equivalence for these two ledgers no matter the technology or application used or the functions performed by the solution used by the

[486] Explanatory Memorandum, p. 3. For more information: Ministry of Justice. (2018) Ühinguõiguse revisjon Analüüs-konseptsioon (Revision of Company Law), 15 September 2018. [online] <https://www.just.ee/sites/www.just.ee/files/uhinguoiguse_revisjoni_analuus-kontseptsioon.pdf> accessed 12 January 2019.

management board for shareholder ledger administration. Consequently, the bias in existing regulation is attached to the subject that administers the shareholder ledger and not to the process of how the ledger is administered. This means that existing regulation subjectively waives the more stringent requirements of share transfers for CSDs and grants value subjectively to CSD entries without any consideration for how ledger maintenance is organised by the management board and without providing the option to grant effects equivalence if a functionally equivalent solution is used. This means that the existing regulation of the CC is biased towards centralised intermediaries such as the CSD.

The technical – and organisational measures for maintaining the ledger can be chosen by the management board. However, the regulator is mute as to these measures and the effect of the entries does not depend on the differences related to the measures. The author is of the opinion that the existing regulation and the recent amendments to the CC do not provide the company with the opportunity to choose between equal alternatives, even if DLT-based or other technology-based shareholder ledger maintenance is used to maintain non-CSD shares, as the functions of the management board-maintained ledger will never, under existing regulation, be able to receive equivalent effects to the ledger maintenance of CSD-registered shares as there is no waiver clause allowing for such treatment.

As said, DLT is a ledger technology and theoretically has the functionality to ensure trust, transparency and verification of data. This means that any DLT-based shareholder ledger could potentially perform the functions performed by the CSD equivalently. The existing regulation in essence does not restrict the management board in using DLT or any other technology in shareholder-ledger maintenance. However, as mentioned, the existing regulation is technology-independent and does not require or forbid the use of any technological solution. Given the exemptions allowed under the Pilot Regime, on the basis that "the exemption requested is proportionate to and justified by the use of its DLT",[487] to certain requirements of the CSDR and MIFID II, it is proportional to expect the Estonian regulator to enable the use of distributed ledger technology in the shareholder ledger maintenance of non-CSD shares of OÜs, granting such maintenance effects equivalence under the CC.

Even with the recent amendments, the existing regulation is not in compliance with the principle of technology neutrality because of the bias towards CSDs, as only CSDs can enjoy the constitutive value of the ledger entry, and 100% of CSD-registered shares can be transferred enjoying freedom of form. The regulation would be technology-neutral if the shareholder ledgers of non-CSD shares, upon meeting certain objectives (without becoming a CSD), are given the chance to enjoy effects equivalence, i.e. the same treatment as CSD shares under existing regulation. Given the Startup Exemption, the problematic effect of existing regulation would partly be solved if the majority of OÜs increase their share capital to EUR 10,000 and pay it in, as well as pass a unanimous shareholder resolution and amend the articles of association stating such waiver of form. Nevertheless,

[487] Article 5 of the Pilot Regime.

the author fails to grasp the reason the regulator requires OÜs to make the aforementioned changes.

4.3 Hybrid smart contract agreement

The third DLT use case involves exploration into contracts used in Initial Coin Offerings (ICO). ICOs sprung into popularity in 2016 and 2017 as a new way to raise capital for innovative and, initially, DLT-employing services and products. The capital raised during ICOs was in the form of virtual currencies (e.g., BTC and ETH). The individuals participating in the capital raise were usually globally dispersed and the project material disseminated electronically. In return for the virtual currency transferred, the ICO organizer typically issued tokens directly to the individuals who had participated in the ICO. In order to automate and simplify the ICO process, the tokens were often issued by the ICO organizer using an automatically executing protocol called a 'smart contract'.

In this dissertation, the author explores the qualification of such 'smart contract' and the surrounding elements typically used in the ICOs, which the author calls 'hybrid smart contract agreement'. The exploration is executed on the basis of the EU and Estonian existing regulation. The key question in this use case for the author is whether DLT-based smart contract signature can be regarded functionally equivalent to be qualified electronic signature under eIDAS and consequently, whether eIDAS regulation is technology-neutral.

4.3.1 Description of the problem

For transferring certain property or rights, including shares or real estate, a specific form of contract is needed. In ICOs, all sorts of tokens were transferred or issued that represented different rights or claims. The qualification of the form of contract the parties have entered into in these ICOs is therefore of importance to maximize the odds of these contracts being regarded as valid. Consequently, the dissertation presents the finding to the question whether ICO smart contracts can be qualified as contracts in an electronic form, which in some jurisdictions are equivalent to written form contracts. This matter is also marked as an important aspect to observe by the EU Blockchain Study.[488]

In order to qualify an agreement as an agreement in an electronic form, the requirements need to be fulfilled for this purpose under the existing regulation and whether the agreement meets these requirements securing the required level of trust must be examined. Moreover, for this qualification, not only contract law is relevant, but also regulation applying to electronic signatures. Therefore, in this use case, the author explores the EU electronic signature regulation. The existing

[488] EU Blockchain Study (n. 15), pp. 8, 9, 52, 59–89.

EU electronic signature regulation aims to be technology-neutral. Such aim has been stated even in Recital 27[489] and Recital 16[490] of the eIDAS.[491]

In order to enable growth through globalization in the interconnected online market, there is a high demand for trusted online services. The eIDAS aims to establish common standards for electronic identification and trust services in order to enable electronic transactions in the EU. For this purpose, the eIDAS aims to harmonise the regulation of electronic signatures so that these can be trusted across borders to enable online transactions and pursue online business opportunities. Therefore, the eIDAS is a regulatory tool that applies the principle of technology neutrality by enabling the use of cross-border electronic transactions, which, in effect, creates the preconditions for electronic transactions to be considered functionally equivalent to paper-format transactions. Nevertheless, each existing regulation has been drafted on the basis of the understanding of how electronic signing works in practice using existing technology. In relation to the electronic signature required for the electronic form of a contract the legacy model the eIDAS has been built on is the Public Key Infrastructure (PKI) model. PKI is:

> "a combination of policies, procedures and technology needed to manage digital certificates in a public key cryptography scheme. A digital certificate is an electronic data structure that binds an entity, being an institution, a person, a computer program, a web address etc., to its public key. Digital certificates are used for secure communication, using public key cryptography, and digital signatures. The purpose of a PKI is to make sure that the certificate can be trusted."[492]

This means that although the eIDAS claims to be technology-neutral, it is still built on the PKI model. The PKI model depends on the use of the digital certificates and cryptographic keys issued by verified sources. The verified sources can be both public – and private service providers who have been granted qualified status by a national competent authority and included in so-called 'trusted lists' known as the Trusted List Browser or the European List of Trusted Lists (LOTL).[493]

These trust service providers need to be trusted as they issue certificates and private keys to users to enable the users to be linked to the signature. The issue

---

[489] Recital 27 states among other things that "this Regulation should be technology-neutral".

[490] Recital 16 states among other things that "the requirements established should be technology-neutral".

[491] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).

[492] European Union Agency for Cybersecurity. Glossary <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/public-key-infrastructure-pki> accessed 10 May 2020.

[493] Trusted List Browser is a tool to browse the so-called national eIDAS Trusted Lists and also the EU List of eIDAS Trusted Lists also referred to as LOTL <https://webgate.ec.europa.eu/tl-browser/#/> accessed 10 May 2020.

of the certificates is done through the use of a qualified signature creation device discussed further below. Consequently, as stated by Anna Nordén, the existing EU electronic signature regulation often fails to be technology-neutral as it is meant to achieve trust using the PKI model even though the regulation terminologically hides behind more neutral terms.[494]

The PKI model is not the only solution for electronic signatures that is required for a contract to be regarded in an electronic form, but it is a model that the regulator understands. As stated earlier, due to the Pacing Problem, it is difficult for the regulator to amend and adjust existing regulation on the go in order to adapt to any new alternative technical solution. DLT as described in introduction involves a bundle of technologies and as explained in Section 4.3.3 below some of these are similar or equivalent to the technologies used in electronic signing that use the PKI model. However, DLT-based infrastructure is based on the assumption that trust is built into the protocol and its governance. Consequently, DLT-based electronic signing does not depend on certificates and private keys issued by verified entities. The keys used in the DLT cryptography are (depending on the users' preferences) issued directly to the user by the protocol and, unlike the PKI model, there is no other entity or authority centrally controlling these keys or protocols. This change in the DLT infrastructure challenges the PKI-model-based existing regulation in an unexpected way, as the centralised trust system is no longer the only option.

In this dissertation, the author researches the criteria built into existing regulation that results in the trusted electronic signature and also whether the set criteria can be fulfilled by an alternative model based on DLT infrastructure. Consequently, the third DLT use case explores the regulation of the qualified electronic signature of the eIDAS (which is the required signature for a contract to be regarded as in an electronic form) in order to examine whether the ICO smart contract qualifies under the hierarchy of contracts as a contract in an electronic form. If these requirements of the eIDAS are not met by the ICO smart contract, the ICO contract form cannot be qualified as in an electronic form, which, under existing regulation, could turn out to be a hindrance to the use of smart contracts in certain transactions that require electronic form or hand-written form in order for the contract to be considered valid.

The key resources used for the legal analysis under this DLT use case are primarily the eIDAS, in parts also the UNIDROIT Principles of International Commercial Contracts of 2016 (UNIDROIT Principles)[495] and, in relation to the electronic form of contracts and the hierarchy of forms, the General Part of the Civil Code Act (GPCCA)[496] and the Estonian Electronic Identification and Trust

---

[494] Nordén, Anna (2005). 'Electronic signatures in a legal context' in Magnusson Sjöberg, Cecilia (ed.), *IT Law for IT Professionals – an introduction* (Studentlitteratur 2005), p. 173.

[495] Full text available <https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016> accessed 23 July 2018.

[496] General Part of the Civil Code Act (GPCCA) [*tsiviilseadustiku üldosa seadus*] – RT 2002, 35, 216; RT I, 23.05.2020, 4.

Services for Electronic Transactions Act (EEITSETA)[497] in Estonia. As the qualification of a smart contract as a contract under the UNIDROIT Principles is discussed in Article III, the analysis in the present compendium will primarily focus on the problems related to the qualification of the electronic signature of the hybrid smart contract agreement as a qualified electronic signature under the eIDAS and the respective qualification of the contract as in an electronic form under Estonian law. A specific national law is chosen for this qualification as there is no regional or international regulation to guide such determination.

4.3.2 Statement set for defence

The signature used in the DLT-based smart contracts of the ICO process can be considered functionally equivalent to the qualified electronic signature under the eIDAS in cases where the identification function has been fulfilled either off-chain or on-chain and the users use non-custodial wallets. The Centralized Authority (CA)-centric PKI-model-based trust system is not needed for key management in the case of DLT-based smart contracts as the keys are generated by the DLT network protocol and managed by the individual. The electronic signature regulation of the eIDAS is not in compliance with the principle of technology neutrality because of the dependence on the PKI model and LOTL's centralized trust system, as it does not grant effects equivalence to the functionally equivalent DLT-based solution. As an extension of the above, DLT-based hybrid smart contract agreements should be regarded as functionally equivalent to contracts in an electronic form and should therefore receive equivalence of outcome as to the validity and recognition of the DLT-based contract.

4.3.3 Reasoning

The smart contract protocol exists in a larger context and not in silos. In this dissertation, the term smart contract is used to include more components than merely the protocol. Rather, it includes the terms agreed between the parties and the processes the user needs to complete in order to conclude the Token Sale Agreement,[498] such as accepting the terms and conditions (T&C)[499] in order to

---

[497] §24(1) of the Estonian Electronic Identification and Trust Services for Electronic Transactions Act defines a digital signature as "an electronic signature that conforms to the requirements for a qualified electronic signature set out in Article 3(12) of [eIDAS]." Estonian Electronic Identification and Trust Services for Electronic Transactions Act *[E-identimise ja e-tehingute usaldusteenuste seadus]* RT I, 25.10.2016, 1, English version

<https://www.riigiteataja.ee/en/eli/511012019010/consolide

[498] Terms and Conditions of the Ethereum Genesis Sale. 21 July 2014 <https://web.archive.org/web/20140723212709/https://www.ethereum.org/pdfs/TermsAndConditionsOfTheEtherEumGenesisSale.pdf> accessed 1 May 2019.

[499] Ethereum Website. <https://www.ethereum.org/terms-of-use/> accessed 1 May 2019.

register on the ICO launch site and make a transfer of virtual currency in return for issue of the token.

4.3.3.1 The components of the smart contract

To be more specific, the smart contract analysed in this dissertation is referred to as either 'ICO smart contract' or 'hybrid smart contract agreement',[500] a term coined by Primavera de Filippi and Aaron Wright, and is considered to have the following three components:

a. *The offer* made to the public by the ICO organizer (including the terms indicated in the White Paper, the Token Sale Agreement, the T&C and the auditable protocol of the smart contract).
b. *The acceptance* of the offer with all of its components by the user, which is usually executed by either:
   i. user registration (including accepting the T&C) and possibly also completion of the Know-Your-Customer (KYC) procedure;[501] and
   ii. the transfer of funds in the virtual currencies accepted by the ICO organizer to a specific wallet address.
c. *The execution* of the protocol designed or employed by the ICO organizer in the form of issuing tokens to the user as an automatic process.[502]

Therefore, if the ICO smart contract includes the components as described above, it is possible to identify the different features of a contract, e.g., identifiable substance, terms and parties. The exact qualification of whether the components can be regarded as identified, whether these meet the requirements of a contract and, if so, which form of contract, depends on the components included in every separate ICO smart contract. The question addressed in this use case is rather: is an ICO smart contract a contract in an electronic form?

---

[500] de Filippi and Wright (n. 12), p. 80.

[501] Statistics show that the KYC procedure is executed only 45% of the ICOs monitored. Statistics by Rhue, Lauren (2018). Trust is All You Need: An Empirical Exploration of Initial Coin Offerings (ICOs) and ICO Reputation Scores (May 16, 2018), p. 14. <https://ssrn.com/abstract=3179723 or http://dx.doi.org/10.2139/ssrn.3179723> accessed 24 July 2019. While some ICO organizers, such as Tezos, completed the KYC procedure after the ICO period in relation to the subsequent litigations that still are ongoing. Read more of the recent developments with litigation here: <https://www.civic.com/blog/4-key-takeaways-decentralized-kyc-for-icos-and-token-sales/> accessed 24 July 2019. Coleman, Lester (2018). Tezos Investors Forced to Undergo KYC Nearly 1 Year after ICO. 12 June 2018. <https://www.ccn.com/tezos-investors-forced-to-undergo-kyc-nearly-1-year-after-ico/> accessed 24 June 2019

[502] As this executes the code prepared by the ICO organizer and the execution involves a similar process as that of electronic signing under the eIDAS, this process can also be regarded as the electronic signing of the contract by the ICO organizer. If point (a) is merely considered as an invitation to make an offer, then point (b) is the offer and (c) is the acceptance.

4.3.3.2 Does an ICO smart contract comply with the electronic form?

Under §80 of the GPCCA, in order to comply with the requirements for the electronic form, a contract must meet the following preconditions:

1. It must be entered into in a form that enables repeated reproduction.
2. It must contain the names of the persons entering into the transaction.
3. It must be electronically signed by the persons entering into the transaction.

The author explores these preconditions further in the following subsections.

(i) Enabling repeated reproduction

On the basis of the functions of contract forms as discussed in Articles II and III, the author concludes that the aim of this specific criteria is to perform the *evidentiary function* of the contract. The evidentiary function means that the intent and substance of the parties can be evidenced by the object at any later stage. Considering that there is a list of components of the ICO smart contract as listed above (including the Token Sale Agreement and the T&C provided in a durable medium that contain the terms the smart contract protocol executes), the author concludes that the ICO smart contract enables repeated reproduction.

A further aspect to consider is the fact that the transaction of transferring funds to ICO organizers and the issuing of tokens are also recorded on the DLT network ledger (blockchain); these transactions are publicly visible and available for repeated reproduction. This means that there is sufficient evidence, without an in-depth investigation, that the ICO smart contract enables repeated reproduction for the purposes of *evidentiary function*.

(ii) Contains the names of the persons entering into the transaction

This criterion is meant to execute the *identification function* as described in Article III. In the DLT protocol, there is usually no identity attached to the keys used to conclude or execute transactions. The same protocol generates the keys and facilitates the conclusion of these transactions. However, neither the protocol itself nor the developer of the protocol that generates the keys usually identifies or records the identity data of the holder of the keys.

Nevertheless, it is possible for the ICO organizer to separately collect and record such KYC data outside the blockchain network (also referred to as *off-chain*). If the ICO organizer needs to fulfil KYC compliance obligations under the existing regulation, the identification function may be fulfilled as part of the onboarding process. Alternatively, the ICO organizer may opt to use a separate

on-chain KYC solution to identify the names of the persons participating in the transaction, such as AuthCoin,[503] CertCoin,[504] SCPKI,[505] Civic.[506]

Furthermore, given that in the offline world, anonymous or pseudonymous transactions are allowed between the parties, perhaps it is time to grant these options for online world transactions and allow the users of online contracts to remain either anonymous or pseudonymous while still being party to a contract in an electronic form. This option would be in line with the rising trend of individuals to use private browsing,[507] TOR or a VPN[508] than ever before. Said liberalisation would promote the principle of freedom of contract, as the parties

---

[503] Its security features are discussed here: Norta, A., Matulevĭcius, R., & Leiding, B. Safeguarding a Formalized Blockchain-Enabled Identity-Authentication Protocol by Applying Security Risk-Oriented Patterns. (2019) Computers & Security <https://www. sciencedirect. com/science/article/pii/S0167404818302670?dgcid=author> accessed 10 July 2019.

[504] Polyswarm. Blockchain in Cyber Security: Who is Who. (10 January 2018) <https://medium.com/polyswarm/blockchain-in-cyber-security-who-is-who-269d89feadc1> accessed 10 July 2019.

[505] "The primary proposition of SCPKI is to write such a smart contract with functionality for the operation of a public key infrastructure and identity management system, where public keys and identity attributes are stored on the blockchain and can be managed by the smart contract." Al-Bassam, M. (2017, April). SCPKI: a smart contract-based PKI and identity system. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts ACM. <http://www0.cs.ucl.ac.uk/staff/M.AlBassam/publications/scpki-bcc17.pdf> accessed 3 July 2019.

[506] Civic provides a reusable KYC service depending on multi-factor authentication without a third-party authenticator or physical hardware. <https://www.civic.com/solutions/kyc-services/ accessed: 25 July 2019

[507] According to statistics, the younger the users are, the more they use private browsing (incognito mode) and around two-thirds of Americans wish their browser would give better privacy protection – no tracking, no cookies, no ads, no saving user data, etc. Bojan Jovanović. 'Browser statistics: Catching the best surf on the Web.' DataProt [blog], December 2, 2019. <https://dataprot.net/statistics/browser-statistics/> accessed 03 October 2020. "…online anonymity is now regarded as a fundamental factor in the protection of private information and in reducing the dangers of the Web, such as hacking and malware (Hoang and Pishva, 2014), as a facilitator for participation in discussions about sensitive topics, health issues, for instance, in computer-mediated communication (McLeod, 2011), and as an option for citizens to avoid government surveillance in highly repressive as much as highly liberal contexts (Jardine, 2016)." Thais Sardá, Simone Natale, Nikos Sotirakopoulos, Mark Monaghan. 'Understanding online anonymity.' Media Culture & Society 41(4):016344371984207, (April 2019). DOI: <10.1177/0163443719842074> accessed 03 October 2020.

[508] Technically, the anonymity in exchanging information or engaging in transactions on the Internet can be achieved through different measures in addition to private browsing on traditional Internet browsers, such as through the use of a proxy, a VPN and The Onion Router (Tor). Sardá, Natale, Sotirakopoulos, Monaghan (n. 487). Tor being a browser that provides a certain level of confidentiality by linking a computer network and layers of encryption between the information source and the actual user seeking this information, allowing both sides anonymity. Tomas Minárik, Anna-Maria Osula, 'Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law.' (2016) Computer Law and Security Review, 32 (1), 111−127.10.1016/j.clsr.2015.12.002.

themselves can choose the conditions of the contract and whether they know the counterparty's identity or not. Such choice would also strengthen the pursuit of privacy in relations that are conducted entirely online.

Nevertheless, according to Harlev and others, anonymity and pseudonymity on DLT networks might already be a concept of the past. This is due to the possibility "to cluster together Bitcoin addresses and link such clusters to real-world identities"[509] using already developed technology.

Even the US Securities and Exchange Commission in January 2019 publicly called upon vendors dealing with wallet addresses to provide insight as "to whom a particular address belongs",[510] knowing that technologies are being developed towards this end constantly. Furthermore, while in common law jurisdictions there is a "purely evidence-based approach" which does not require the technology to perform the identification function, civil law jurisdictions approach the matter differently and "considered independent evidence of the identity of a signatory to be an important factor if electronic signatures were to be given legal validity".[511] Lastly, the EU Blockchain Observatory and Forum report of 2019 also revealed that "while not always identifiable at the moment of the transaction, given enough time and effort, many parties to a transaction can be unmasked."[512]

On the basis of the above, the author concludes that, upon the conclusion of the ICO smart contract, it is possible to perform the *identification function* employing multiple techniques using either on-chain and off-chain solutions or separating the identification function altogether from the signature. Consequently, even though the DLT-based smart contract itself typically does not tie the identities to the keys used for signing the transactions, the parties are still identifiable through the use of additional technology or a policy decision could be made that this function is not required at all.

(iii) Is electronically signed by the persons entering into the transaction

This criteria appears to be for *evidentiary function*, but as can be seen from its components, the criteria aims to additionally link the evidence (the existence of the signature) with the identity and consequently aims to execute the *identification function*. In order to find out what electronic form and electronically

---

[509] Harlev *et al.* 'Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning', (2018) Proceedings of the 51st Hawaii International Conference on System Sciences. <https://core.ac.uk/download/pdf/143481278.pdf> accessed 8 July 2019.

[510] More information on this: https://www.fbo.gov/index?s=opportunity&mode=form&id=c18a03f93cf06df47dab8a1c1a7f87a9&tab=core&_cview=0 accessed 08 July 2019.

[511] Reed (n. 100), p. 273.

[512] EU Blockchain Observatory and Forum. Legal and regulatory framework of blockchains and smart contracts. A thematic report prepared by the EU Blockchain Observatory and Forum, v1.0 – Published on 27 September 2019, p. 14. <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 26 January 2020.

signed mean in this context – the national law of Estonia, specifically the GPCCA and the EEITSETA, and regional law, specifically the eIDAS, are explored.

4.3.3.3 Electronic signature for electronic ICO smart contract

Under the EEITSETA,[513] the electronic signature[514] requirements stipulated in the GPCCA are equivalent to the signature with the highest assurance level under the eIDAS, known as a *qualified electronic signature*. The requirements for a *qualified electronic signature* under the eIDAS are stipulated in Article 3(11), (12), (23). In the following subsection, the author explores these criteria on the basis of the ICO smart contract.

The CA-centric PKI-model-based existing regulation raises concerns as to its applicability to any DLT-based signature on ICO smart contracts. Firstly, as discussed, a traditional permissionless public blockchain-based smart contract involves no CA in LOTL and there is no issue of digital certificates.[515] Specifically, the ICO organiser and network operators such as the nodes or wallet service providers typically do not issue qualified or non-qualified[516] certificates and none of the participants offering services are typically listed as *qualified trust service providers*. However, the existing regulation does not prohibit any of these partici-

---

[513] §24(1) of the Estonian Electronic Identification and Trust Services for Electronic Transactions Act defines digital signature as "an electronic signature that conforms to the requirements for a qualified electronic signature set out in Article 3(12) of [eIDAS]." Estonian Electronic Identification and Trust Services for Electronic Transactions Act, *[E-identimise ja e-tehingute usaldusteenuste seadus]* – RT I, 25.10.2016, 1, English version <https://www.riigiteataja.ee/en/eli/511012019010/consolide>

[514] Anna Nordén the term "digital signature" was traditionally avoided in regulation as the term "electronic signature" was considered more neutral. The term digital signature is known as the term that covers any technical solution that can be used as an electronic confirmation of declaration of intention. However, GPCCA Section 80(3) stipulates that a digital signature is also an electronic signature that fulfills GPCCA Section 80(3) requirements (the highest assurance level). Estonian legislature mostly uses the term digital signature in national legal acts instead of qualified electronic signature. It is unclear why Estonian legislature, upon transposing the EU Directive 1999/93/EC, did not translate electronic signature into Estonian as *"elektrooniline allkiri"* (in English electronic signature) and instead started to use the term in Estonian "*digitaalallkiri"* (in English digital signature). The terminological situation was also unaffected by the eIDAS. The regulation creates uncertainty due to the term "also" in GPCCA Section 80(3), as if suggesting that in addition to qualified electronic signatures there are other electronic signatures that could be accepted as having equal weight as qualified electronic signatures. However, as far as the author understands, there are no such signatures. Nordén, Anna (2005). Electronic signatures in a legal context, in Cecilia Magnusson Sjöberg, (ed.) *IT Law for IT Professionals – an introduction*, (Studentlitteratur 2005), p. 173.

[515] ESMA (n. 55).

[516] The wallet where the virtual currency is stored can be created and maintained using multiple alternative service providers, e.g., hardware wallets, MetaMask or Parity Signer. Read more here <https://support.mycrypto.com/how-to/getting-started/how-to-create-a-wallet> accessed 09 July 2019.

pants from applying to be registered as a *trust service provider*;[517] the question is rather whether the registration would serve any purpose.

The function provided by *trust service providers* is the generation and issue of keys and certificates to link the keys to the individuals performing both *evidentiary* and *identification functions*. In the case of DLT-based signatures, the participants of the DLT network do not generate or issue the keys needed for electronic signing nor do they tie the keys to the individual through the issue of digital certificates. The keys are typically generated by the protocol and the keys are therefore not tied to an individual, rather to a hardware device which operates the protocol. The interactions on the network, including transactions between participants are either anonymous or pseudonymous. Upon assessing functions as seen in Article II (specifically in Table 2), the technology used in the different infrastructure of electronic signatures is the same. Consequently, as a conclusion, the author is of the opinion that the functional capabilities of the PKI-model-based signatures and the DLT-based *ICO smart contract* signatures for the *evidentiary function* can be considered functionally equivalent.

Looking specifically at Article 3(10) of the eIDAS, the "'electronic signature' means data in an electronic form which is attached to or logically associated with other data in an electronic form and which is used by the signatory to sign".[518] This means that the legal definition of electronic signature is void of any technical requirements and includes a broad range of electronic signatures (also a name in an e-mail)[519] and is "meant to be able to cover future technologies for authenticating data."[520] On the basis of eIDAS, a name in an e-mail without any verification of identity is not considered a sufficiently secure link between the signatory and their declaration of intention[521] to qualify for a contract in an

---

[517] Also, the EU Blockchain Observatory has concluded that smart contract signatures meet the criteria of simple and advanced electronic signatures, but because these signature issuance processes do not include the trust service providers listed in the LOTL, they first have to undergo "the arduous process of becoming a recognised [trust service provider]." Legal and regulatory framework of blockchains and smart contracts. A thematic report prepared by the EU Blockchain Observatory and Forum, v1.0 – Published on 27 September 2019. <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 26 January 2020.

[518] Martin Hogg, 'Secrecy and Signatures – Turning the Legal Spotlight on Encryption and Electronic Signatures', in Lilian Edwards and Charlotte Waelde, *Law & the Internet*. *A framework for electronic commerce*. (Hart Publishing 2000), p. 37.

[519] Article 2 (3) of eIDAS.

[520] Article 1 b) of eIDAS.

[521] Study material included four countries (Estonia, Luxembourg, Iceland and Austria), while in the other member states "the number of electronic signatures was fewer, or it was not possible to gather enough information about the country". Ernst & Young Baltic AS, *Study Report SUMMARY OF THE STUDY: "USAGE OF QUALIFIED ELECTRONIC SIGNATURE WITHIN EUROPE UNION"* (2015). <https://mkm.ee/sites/default/files/summary_of_the_study_usage_of_qualified_electronic_signature_within_europe_union.pdf> accessed 21 July 2019, p. 2.

electronic form. Therefore, in order to establish the form in which the contract is concluded, Articles 3(11), (12) and (23) of the eIDAS must be more closely examined in relation to the ICO smart contract, which is provided below on the basis of the following list of criteria required for a *qualified electronic signature*.

(a) the signature is uniquely linked to the signatory

In the case of an ICO smart contract, the public-private keys linked to the wallet address serve as the identifiers and the wallet address is the public key unique to the signatory. Operating under the assumption that only one individual uses the key-pair (the same assumption applies to keys used for electronic signatures that are based on the PKI model), the conclusion can be made that the electronic signature in an ICO smart contract is uniquely linked to a signatory.

(b) the signature is capable of identifying the signatory

As discussed, the identity of the signatory of the ICO smart contract is not publicly available for checking nor directly linked to the keys used for signing – there is no certification process as such. Although, the public key (wallet address) as the identifier is linked to the private key that links the identifier to the actual identity of the individual.

One of the parties to the ICO smart contract is the ICO organizer, whose identity is disclosed in the ICO smart contract and whose electronic signature is attached to the contract upon transferring the issued token. Although, in the case of a legal entity as an ICO organizer, it remains unclear who actually controls the wallet address and whether the individual who controls the wallet is actually authorized to act on behalf of the legal entity. The other party to the ICO smart contract is the participant in ICO fundraising – the party who transfers either ETH or BTC to the ICO organizer from the participant's wallet address (the public key as the individual's identifier), controlling the wallet with the participant's private key.

Furthermore, as earlier described, it is possible to fulfil the *identification function* requirement with either an off-chain solution, such as a separate KYC procedure carried out by the ICO organizer, the wallet service provider (in the case of custodial wallet service) or the controller of the permission-based ledger, or an on-chain solution. This means that the identity of the controller of the public key can be linked to the wallet address through a separate identification process. As in, whoever controls the public key with their private key is considered the signatory of the transaction and the off-chain or on-chain linking of the identity to the key pair allows the identity to be linked to the electronic signature.

Although, due to the identifier being present and publicly visible in the ledger chain of transactions, all of the transactions are already linked to an identifier that we can also regard as a pseudonym. Hence, all transactions between publicly

visible wallet addresses can be regarded as pseudonymous transactions, as the identifier is like a placeholder for an identity not revealed but potentially linkable to the signature.

Furthermore, as explained above, the link between the identity and the signatory can be created through additional solutions. With the innovative solutions of big data analytics and machine learning and the public key (of a non-custodian wallet) as an identifier, it is possible to identify the signatory.[522]

Consequently, on the basis of this analysis, a question arises: depending on the linkage to the identity of the signatory and its fluctuation over time, could the contract form and signature type on the contract change depending on whether the link between the signature and identity can be made? Or does the eIDAS requirement '*capable of identifying the signatory*' presume the signatory identifying capability to be innate to the technology, meaning that this capability cannot be substituted externally?

On the basis of the above, the author concludes that, although the DLT-based electronic signature does not use the CA-centric PKI model, there are a plethora of alternative solutions that can be used to perform the *identification function*, which is performed by the CA in the PKI model, and this function does not have to be performed innate to the technology.

Furthermore, there is no requirement in the eIDAS that the linking of the identity to the signatory must be innate to the signing technology and cannot be substituted by a solution that may result in the identity being linked to the technology, as this would be a functionally equivalent solution. According to Reed, even if a regulator decides that a particular function is essential for achieving a certain legal result, such as identification, in these circumstances, "the regulator can achieve some level of neutrality between different technology implementations by drafting the legal requirements in such a way that non-compliant implementations can be modified to become compliant".[523] Reed refers to this solution as potential neutrality. The author suggests that, in such cases, the modifications

---

[522] Harlev *et al.*: "it is indeed possible to cluster together Bitcoin addresses and link such clusters to real-world identities". Harlev *et al.,* 'Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning', (2018 Proceedings of the 51st Hawaii International Conference on System Sciences). <https://core.ac.uk/download/pdf/143481278.pdf> accessed 8 July 2019. In January 2019, the Securities and Exchange Commission publicly sought vendors who can provide insights on "to whom a particular address belongs" in relation to wallet addresses. More information on this: <https://www.fbo.gov/index?s=opportunity&mode=form&id=c18a03f93cf06df47dab8a1c1a7f87a9&tab=core&_cview=0> accessed 08 July 2019. Also, the EU Blockchain Observatory and Forum report stated that "While not always identifiable at the moment of the transaction, given enough time and effort, many parties to a transaction can be unmasked. Therefore, at this point there is no question of total impunity for blockchain actors." Legal and regulatory framework of blockchains and smart contracts. A thematic report prepared by the EU Blockchain Observatory and Forum, v1.0 – Published on 27 September 2019, p. 14. <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf> accessed 26 January 2020.

[523] Reed (n. 100), p. 273.

do not have to be innate to the specific technology, especially considering that DLT is a fusion of technologies. The identification function can be added to the fusion, however, without dictating in which way the addition must take place.

On the basis of the principle of technology neutrality, the author concludes that the accepted solution for linking the signature to the identity in order to qualify an electronic signature as a *qualified electronic signature* cannot merely be the CA-centric PKI model, but must also allow the use of other solutions. Although allowing these other solutions could have the consequence that the form of contract is fluid – in the sense that when there is no linkage to identity – the qualification is different from when the link between the identity and the signature is actually verified, and the contract's form is then requalified.

(c) the signature is created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control

The referred *electronic signature creation data* are the keys used for signing. The electronic signatures on the ICO smart contracts of a non-custodial wallet meet the data requirement. In the case of non-custodial wallets, the private key, which is linked to the public key, is used to send the funds to the ICO organiser similarly to the PINs used in the PKI model. This means that in the case of non-custodial wallets under this category, these signatures are functionally equivalent.

(d) the signature is linked to the data signed therewith in such a way that any subsequent change in the data is detectable

The hash function secures the integrity of the data in the ICO smart contract similarly to the way it functions in PKI-model-based electronic signatures. If the data in the ICO smart contract is in any way tampered with, the hash value changes automatically. Consequently, the ICO smart contract meets requirement (d).

(e) created by a qualified electronic signature creation device

As discussed above, according to Article 3(23) of the eIDAS, the 'qualified electronic signature creation device' refers to software or hardware that is used to create an electronic signature and needs to meet the requirements in Annex II to the eIDAS. On the basis of the principle of technology neutrality and the analysis conducted in Article III, the author concludes that the requirements stated in Annex II to the eIDAS are met by the ICO smart contract,[524] except the requirement in Section 3 that discusses trust service providers.

---

[524] Under 1(a), the confidentiality of the keys of the electronic signature creation data of the ICO smart contract is reasonably assured. Under 1(b), once the keys are used the verification process starts, and this means that it can practically occur only once. Under 1(c), the keys

The requirement in Section 3 stipulates the need to involve the trust service provider in the signing and execution of the ICO smart contract. However, in case of smart contracts there usually is no trust service provider involved. It is the understanding of the author that in case the keys are used in electronic signing, the ICO smart contract that is linked to a non-custodial wallet, then no need for the keys to be issued by a separate trust service provider as the keys are neither generated nor managed on behalf of the signatory by an entity requiring trust. Therefore, there is no need to involve the trust service provider in this process.

In the case that the signatory uses custodial wallets, the requirement to involve the trust service provider seems pointless, as the keys are not issued to the signatory at all since these belong to the custodian and the custodian is using the wallet with its own keys.

(f) based on a qualified certificate for electronic signatures

Article 3(15) of the eIDAS stipulates that the qualified certificate for an electronic signature is the certificate for electronic signatures issued by a qualified trust service provider and meeting the requirements laid down in Annex I to the eIDAS. As established, these requirements are aimed at fulfilling the *evidentiary* and *identification function* and, as has been established by the author, both of these functions can be executed by alternative solutions used in the ICO smart contract.

4.3.4 eIDAS needs adaptation

In conclusion, the third DLT use case shows that the certification-centric authentication technology regulation needs to be amended in order to ensure equal treatment for these alternative ways to perform the *evidentiary* and *identification function* and to secure equivalence of outcome to the alternative solutions. However, as stated by Anna Nordén, simply fulfilling the *evidentiary function* equivalently through the use of a technical capability without the backing of a regulatory framework is not sufficient as this "does not produce much result in legal certainty".[525] The author agrees with this warning, as the equivalence of outcome or effects equivalence needs to be ensured by regulation, otherwise the principle of technology neutrality fails in its impact.

Consequently, in order to qualify the *ICO smart contract* as a contract in an electronic form on the basis of the hierarchy of contract forms, existing regulation

---

cannot be derived from each other and the signature is reasonably protected against forgery. Under 1(d), the keys can be reliably protected against other users. Under 2, the DLT technology itself cannot alter the data signed. Even if verification of the transaction happens (by miners adding the transaction to the blockchain), the data remains unaltered. The requirements in Section 4 are also met as the ledger entries are duplicated exactly in accordance with Section 4.

[525] Nordén, (n. 494), p. 161.

needs to be amended to ensure the same weight and value to functionally equivalent electronic signatures on DLT-protocol-based electronic contracts. The aim of such a stipulation would be to be in line with the aim of Article 9 of the Ecommerce Directive,[526] which requires Member States to "ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means". Such stpilation must be equally extended to smart contracts.

Furthermore, the regulator should assess whether any regulation built around one infrastructure is open to alternative infrastructure; in this case, specifically to infrastructure not based on LOTL. As explained above, technically, the signing processes based on the PKI model and DLT are rather similar. As DLT is a fusion of technologies, it binds together technologies such as cryptography, P2P networks, consensus mechanism and linked timestamping without involving centralized trust structures, nevertheless, using much of the same technology as the PKI model. Additionally, the trust in the technical setup and auditable protocol creates decentralized trust without the need to involve LOTL-based centralized trust providers.

For the purposes of identifying the moment the hybrid smart contract agreement is electronically signed, the author concluded that it is the moment the user uses their private key to control the wallet, e.g., to transfer the virtual currency to the wallet address of the ICO organizer. At a later stage, the smart contract protocol issues tokens in return for the virtual currency collected during the ICO period. However, this act can be considered an execution of the contract, as the electronic signature with the private key was already appended to the protocol when the protocol was prepared and presented for auditing. The author is of the opinion that both the ICO organizer and the user participating in the ICO have expressed their will, are identifiable and have appended their electronic signature on the agreement through the use of the private key in relation to their wallet.

Contrary to the existing trust source, the entire DLT network is built on a protocol to instil trust without centralized authority and a central trust list, as all communication under the protocol in a DLT network is encrypted and uses linked timestamping,[527] which is also how the electronic signing under the eIDAS functions.[528] The DLT-based smart contract uses public-private key encryption

---

[526] Article 9 of e-Commerce Directive.

[527] Konstantinos Christidis, Michael Devetsikiotis, 'Blockchains and Smart Contracts for the Internet of Things'. Special section on the plethora of research in the internet of things (IoT). (3 June 2016). doi:<10.1109/ACCESS.2016.2566339> or <http://people.cs.pitt.edu/~mosse/courses/cs3720/blockchain-iot.pdf> accessed 1 June 2019.

[528] ENISA. 'Security guidelines on the appropriate use of qualified electronic signatures. Guidance for users.' V 2.0 Final (December 2016) <https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures/at_download/fullReport> accessed 11 May 2020.

that originates from a cryptography algorithm similar to the EU technical standards for the eIDAS interoperability framework.[529]

As stated by Herian,[530] DLT-based smart contracts are "post-trust electronic agreements". In the opinion of the author, this merely means that the trust is dependent on centralised-system based characteristics and predetermined features that do not grant effects equivalence to functionally equivalent trust systems. This does not mean a blank check should be given to all DLT-based smart contract users or that the outputs of this protocol are functionally equivalent to the electronic signatures protocol and trust system under the eIDAS, it merely means that the system under the eIDAS is tilted towards granting effects of validity and recognition to only electronic signatures that originate from the system of trust fulfilling the requirements and standards created under the eIDAS.

The author concludes based on the above, any regulation which does not grant equivalence of outcome to functionally equivalent alternative systems fails to comply with the technology neutrality principle. This is a substantial shortcoming considering the growth of electronic commerce and the popularity of the financial technology and regulation technology startups that compete on the market to provide different on-chain or off-chain solutions to potentially substitute the CA-based electronic identification system.[531] Consequently, liberalisation should be welcomed due to the fact that any models dependent on the centralized identification function are internally vulnerable due to the presence of a single point of failure such as the LOTL.[532]

Furthermore, given that in the offline world anonymous or pseudonymous transactions are allowed between the parties, perhaps it is time to equalize these options for the online world by amending the existing regulation to allow users of ICO smart contracts to remain either anonymous or pseudonymous but still be a party to a contract in an electronic form.

---

[529] ENISA. 'Standardisation in the field of Electronic Identities and Trust Service Providers. Inventory of activities' Version 1.0, December 2014 <https://www.enisa.europa.eu/publications/standards-eidas/at_download/fullReport> accessed 11 May 2020.

[530] Robert Herian, 'Legal Recognition of Blockchain Registries and Smart Contracts.' (EU Blockchain Observatory and Forum 2018) <http://oro.open.ac.uk/59481/> accessed 1 May 2019.

[531] Eric Borgsten, Oskar Jiang, 'Authentication using Smart Contracts in a Blockchain', Master's thesis in Computer Systems and Networks, (University of Gothenburg and Chalmers University of Technology 2018), p. 15. <http://publications.lib.chalmers.se/records/fulltext/256254/256254.pdf> accessed 10 July 2019.

[532] As shown by the DigiNotar hack in 2011 in the Netherlands. See more on this by: Werbach, Kevin, (August 1, 2017), p. 510.

4.4 Conclusion

The bias in regulation identified in the first use case was for centralised means of payment and against any alternative means of payment (not specifically against DLT-based means of payment). The conclusion is based on the bitcoin's functional equivalence to fiat currency identified in the *Hedqvist* case that did not result in effects equivalence in the *de Voogd* case. Analysis of *Hedqvist* demonstrates that even if regulation is not constructed in a technology neutral way, it can be implemented neutrally if the regulator conducts functional analysis, employs functional-teleological interpretation and allocates resources for research of the technology, objectives of existing regulation and the impact of the existing regulation on the innovative solution.

On the basis of the court cases analyzed, as demonstrated in the first DLT use case, innovative individuals, entities and early adopters will act justifiably differently amongst legal uncertainty in cases their innovative business models meet with existing regulation. These modes of action are either to seek clarity through open communication with the regulator or act without such communication. It might seem that the first option is always better, however, in case of open communication with the regulator is not subjected to a sandbox-type process, the individual can be subjected to long administrative proceedings or even disputes (that is visible from the *Hedqvist* case) where the simple request for legal clarity in the midst of innovation took an innovative individual down the path of dispute with the Swedish tax authorities (*Skatteverket*) that reached the CJEU and lasted for more than 2 years.[533] This example shows that this mode of action is not a very efficient way for any startup to seek legal clarity or obtain legal certainty.

The other mode of action is not to open communication with the regulator and not to try to understand whether the embarked business model "fits a box" under the existing regulation. As also can be seen in Article I, Mr. de Voogd took that particular mode of action and ironically also ended up in a legal dispute of more than 2 years[534] for a regulatory requirement that after the final ruling in *de Voogd* survived less than hundred days. Furthermore, these two court cases also show

[533] Hedqvist applied for the decision of the Swedish Revenue Law Commission (SRLC) to obtain legal clarity in the issue of taxation related to bitcoins in 2013 and received the SRLC decision on the issue on 14th October 2013, which was challenged in the administrative court by another authority, the Swedish tax authority (*Skatteverket*), and ended up under the preliminary ruling procedure on the table of CJEU from which a ruling came down on 22 October 2015 in favour of Hedqvist. Most likely Hedqvist approached his tax advisors much earlier than October 2013 and spent a considerable amount of funds to finance the communication with these different authorities and the legal battle at the Swedish administrative court and CJEU.

[534] On 13th February 2014 the FIU initiated the communication with De Voogd that was followed by a precept to comply on 24th March 2014 and led to the FIU submitting a claim against De Voogd in an administrative court on 21st April 2014 that was finalised with an Estonian Supreme Court decision on 11th April 2016 in favour of the FIU's position on the interpretation of a norm De Voogd was refusing to comply with.

that the public communication to build and share "knowledge" about what the regulation requires and how the authorities interpret the regulation should be a substantially higher priority for regulators. Furthermore, in case the public is repeatedly misinformed by the regulator on the subject matter, such factors should mitigate any failures of the public to operate in conformity with the regulation.

de Voogd case is an outcome of Collingridge dilemma and clearly exemplifies the Pacing Problem, yet, these interpretations of the requirements of the regulator needed to be more transparency, include less discriminatory effect and should have been made public in advance.

The bias in regulation identified in relation to the second use case was related to CSD – in case the shares of a private liability company under Estonian law were administered by the CSD – the more stringent requirements related to share transfer transactions were waived and freedom of form for share transfer and pledge transaction prevailed.

Furthermore, the entry of shareholder data in the CSD-maintained ledger carries constitutive value, while the CC grants entries in the non-CSD ledgers no such value, irrespective of how ledger maintenance is organised or what technological solution is used by the ledger administrator. As the author presented, the regulation includes no flexibility to grant effects equivalence to a non-CSD ledger maintenance solution even if it is functionally equivalent to the CSD ledger. Such conclusion proves that the existing regulation is based on a bias for centralised intermediaries such as the CSD and is non-compliant with the technology neutrality principle. Given that the CSD ledgers have not been successful in attaining their goal of easing share transfers and their popularity among users is even more discouraging, the non-compliance of the CC with the technology neutrality principle is creating an obstacle on the market that also cannot be said to meet the requirements of the Services Directive discussed in Chapter 2 above as this regulation is not:

(a) non-discriminatory;
(b) justified by an overriding reason relating to the public interest;
(c) proportionate to that public interest objective;
(d) clear and unambiguous;
(e) objective;
(f) made public in advance;
(g) transparent and accessible.

Therefore, in order to effectively use DLT-protocol based shareholder ledgers, CC should be adapted at least with a waiver model as provided for the CSD-registered shares or alternatively by a GDPR model where the objectives or functions the ledger must meet are stipulated in regulation, but the specific measures are left up to the administrator.

Finally, on the basis of the third use case it can be concluded that currently, eIDAS regulation on electronic signatures is built around LOTL infrastructure and the PKI model. As research showed, technically, the signing processes based

on the PKI model and the one based on DLT are rather similar and, consequently, as gathered on the basis of the analysis, functionally predominantly equivalent. As described in this dissertation, DLT is a fusion of technologies that binds together cryptography, P2P networks, consensus mechanism and linked time-stamping, but does not include centralised trust structures. Differently from the existing source of trust for electronic signatures, DLT-based trust is built on a protocol-based trust that does not require a centralised authority or a central trust list such as LOTL. The auditable protocol of DLT creates decentralised trust without the need to involve LOTL-based centralised trust-based key management for electronic signing of contracts in an electronic form. Communication between parties, based on DLT protocol, is encrypted and uses linked timestamping, which is functionally equivalent to electronic signing under the eIDAS. Furthermore, the DLT-based contract uses a similar public-private key encryption cryptography algorithm, as required in the EU technical standards under the eIDAS interoperability framework.

Furthermore, such conclusion does not mean that all DLT-based smart contract signatures are functionally equivalent to the electronic signatures required under the eIDAS. However, it does mean that the electronic signature system required under the eIDAS for contracts to be qualified in an electronic form is tilted and biased towards electronic signatures that originate from the centralised system of trust. However, in line with the principle of technology neutrality and Article 9 of the Ecommerce Directive, which also calls for the same weight and value for functionally equivalent electronic signatures, DLT-based smart contracts should not be discriminated against simply because the key generation and key administration is executed differently. The author is of the opinion that none of the restrictions allowed under Article 3 (2) and (4) of the Ecommerce Directive for Member States to limit the freedom to provide information society services would be applicable in this use case and therefore, there is no justification for the non-compliance with the principle.

Nevertheless, the research showed that there are differences in functions of centralized and decentralized solutions: either the issuer of the means of payment is different, the source of trust is different, the key generation and management is different, the ledger administrator is different, and this could in some circumstances result in functional difference rather than equivalence. However, functional equivalence does not mean that the processes and institutions (parties executing the processes) must be the same, rather functional equivalence (and functional approach in comparative law) in general looks at the objectives these processes are targeted at and aims to clarify if the objectives (such as protection goals or values) are addressed equivalently. This does not mean that the difference in processes, institutions or infrastructure should be ignored, but rather that when a difference is identified, this calls for assessment of a need for difference in treatment. Finally, at times these identified differences can justify difference in treatment that is proportional to the difference in the analysed process or its inherent functions, e.g. lifting or adding certain compliance requirements. In the DLT use cases discussed in the present chapter, there were differences identified

in the functions but due to the similarity of objectives these different functions pursued, the treatment of these technical solutions called for effects equivalence with minor adjustments to. Consequently, these use cases show that rather than denying technical solutions that perform functions differently (while reaching similar or same objectives) all effects equivalence, the technology neutrality principle calls for effects equivalence to be granted (even with adjustments if needed) to address advances or risks related to the new technological solution.

V CONCLUSIONS

As existing regulation has been drafted for centralised structures and not distributed ones like DLT, this dissertation explored the existing regulation author for bias against DLT use in the EU and Estonia applied to the specific DLT use cases chosen by the. The research demonstrated different apparent and non-apparent biases against DLT use that maybe difficult to detect if no functional analysis is conducted on existing regulation. The conclusions based on the posed research questions can be summarized as follows.

5.1 Identifying bias against DLT

To identify bias, the author used the principle of technology neutrality as a benchmark. The author extends the application of the principle developed in the 1990s for the equal treatment of offline and online dimensions to test the equivalence of treatment of centralised and distributed dimensions. The principle is aimed at preventing regulators from preferring or favouring a certain technology. Although the principle was originally linked only to ICT, with the expansion of digital society to all sectors of life, the principle has become a general principle of law. The principle is not an overarching principle and certainly must be balanced against other values (rights, freedoms and justifications) that need protection by law.

As to the content of the principle, the research of the author showed that the principle consists of the components of functional equivalence and effects equivalence. In order to identify bias in regulation, these components should be used to conduct functional and effects analysis. In order to understand why existing regulation is how it is – e.g., creating dependencies on intermediaries and registrations or issuing processes – the models, processes and solutions predominantly used during the development of the existing regulation should be investigated. Such investigation provides insight into the reasons for any possible inherent bias and reveals the hidden features the regulation presumes from technology, which, in the context of new technology, often require the performance of unfit, repetitive or unnecessary formalities that have already been sufficiently addressed by the technical or organisational solution (e.g., see analysis in Article III of the hybrid smart contract use case). These requirements may become obsolete in the context of the new technology. Consequently, maintaining the regulation as is creates a disadvantage for the functionally equivalent innovative technology solutions, as these often are not granted effects equivalence without meeting the formalities stated in the existing regulation. Therefore, the objectives of these formalities must be explored in order to assess whether a waiver of the formalities is called for. A similar approach was taken for example by the European regulator in the Pilot Regime that was just recently introduced in relation to crypto-assets. The functional and effects analysis, as indicated by its title, has two parts:

(i) in order to check compliance with the sub-principle of functional equivalence, the technology and its functions need to be compared with the objectives of the requirements in the existing regulation with the aim to identify whether the solution can be considered functionally equivalent;
(ii) thereafter, the effects of the existing regulation to functionally equivalent solutions that do not comply with the specific requirements in the existing regulation should be investigated in order to understand whether effects equivalence (such effects as validity, binding effect, constitutive value, etc.) can be granted under the existing regulation to functionally equivalent solutions (solutions that meet the objectives of the requirements but not the formal requirements themselves).

In case effects analysis reveals difference of treatment of a functionally equivalent solution that is not justified by any specific difference in the specific solution, the difference of treatment can be regarded as discriminatory and consequently, considered as a bias written in the existing regulation. The detection of bias under such analysis is largely dependent on how well regulators understand the new technology, the wider context of the technology, the impact of existing regulation on the technology and the technology neutrality principle itself.

The research showed that the sub-principle of functional equivalence challenges any bias towards a certain existing solution (technical or organisational models) and requires the regulator to analyse whether an innovative solution is able to achieve the objectives of the requirements of the existing regulation functionally equivalently without necessarily meeting all of the formal requirements prescribed in the existing regulation. This idea has been successfully incorporated in the 'privacy-by-design' regulative model of the GDPR by including only the objectives of the requirements in the regulation and not the specific procedural requirements how these objectives need to be obtained.

Furthermore, based on the research presented in the dissertation, it appeared that a core aspect of the principle and one of the most cited values in relation to the neutrality principle is the sustainability goal. Regulation should be flexible and abstract enough to sustain development of new technology and, if it is technology-specific, it should grant effects equivalence to functionally equivalent solutions, similar to the way that electronic form, under certain conditions, is treated equivalently with written or physical form. Based on the sustainability goal, each piece of existing regulation must be evaluated for possible hurdles to innovation. However, as discussed in this dissertation, such sustainable regulation might be difficult to draft and maintain due to the technology advancing in unexpected directions. This means that whenever a new technology reveals its new use cases, existing regulation might need an overhaul check for compliance with the technology neutrality principle. The Digital Finance Package introduced in late 2020 clearly shows that the EU is introducing evidence-based adaptations of existing regulation and this evidence can be gathered based on this type of functional and effects analysis, as discussed in this dissertation. Based on the use cases analysed, this dissertation showed that this type of analysis should not stop

at financial sector regulation (e.g., the Digital Finance Package), but should cover all existing regulation addressing digital society.

However, the research on the application of the technology neutrality principle presented in the dissertation reveals that the courts have a hard time understanding the principle and applying it outside the scope of electronic communication regulation. Furthermore, some relevant court cases (such as *UsedSoft* and *Tom Kabinet)* separate the content layer from transport layer and identify how the transport layer can influence the content layer, the utility and rights attached to the goods or service to make it functionally different from the same goods or service in a different form and consequently, justifying also the difference in treatment. As can be seen in these court cases, technical solutions have multiple layers and the process of examination thereof might reveal a different utility of a good that is in a different form. These differences often call for different treatment, as equivalence should not restrict the use of a more advanced technology in order to achieve the advanced objectives of regulators that the new technology allows (such as the wider protection of rights of copyright holders). This means that technology's advancement can influence regulation in a way that the new product may be granted additional effects that are not granted to the physical medium, and such treatment is in compliance with the technology neutrality principle, as regulation should not limit technology from advancing different legal regimes (e.g., ownership or control of private property). The existence of the layers themselves does not necessarily justify different treatment but assists in understanding the objective regulators might have to treat these media differently despite the functional equivalence of the content layer. Considering that the principle is based on the general principles of non-discrimination, the limitation of the principle is anchored at the borders of differences in the new technical solution. The ultimate question, however, remains – is the difference substantive enough to justify difference of treatment and is the difference in treatment proportional to the difference in substance.

Such conclusions and questions are in line with the critique of the principle stating that due to the advancement of technology and the changes in the market and society, regulation is unable to maintain sustainability and is bound to become unfit for the changed context. Digital publishing, online media and OTT services are all vastly different domains than their physical infrastructure-based counterparts, and this calls for the recognition of the contextual change and the convergence of technologies and sectors that has taken place. This type of development challenges regulators' use of the technology neutrality principle, as there is no strict functional equivalence in the sense that the new technology is used for the same purpose as the old (e.g., telephone services and VoiP), but enables more functionalities and use cases, less friction, a wider reach, a global user base, etc. In such a case, the technology neutrality principle demands that regulators not extend existing regulation to the new context, but instead adapt it to consider technological development and their objective in regulating. The newly introduced Digital Finance Package is aimed at exactly that – adaptation of the existing

regulation to consider the use of DLT outputs in the form of crypto-assets in the financial sector.

However, such phenomenon makes it difficult for regulators to understand how effects equivalence should be granted to comply with technology neutrality principle and therefore, not to favour or prefer a certain technology, while at the same time still creating technology-specific regulation to enable the new technology to fulfil its use potential. This difficulty might lead regulators to create regulation that merely uses neutral terminology while still being built around certain specific existing solutions used in reality. Such outcome was identified in the third DLT use case analysed in the dissertation in relation to electronic signature regulation under the eIDAS. As revealed by the third DLT use case, technology neutral wording in regulation may still include a bias for the use of technical solutions existing at the moment of drafting the regulation. As a solution, the technology neutrality principle requires regulators to use functional analysis to diligently investigate for such bias and to aim to ensure neutrality.

5.2 Identifying bias against DLT based on use cases

In the dissertation, the author conducted three compliance checks of existing regulation with the technology neutrality principle on the basis of three different DLT use cases based on the objectives of the specific regulation. The objectives reveal why the regulator stipulated in the regulation specific functional requirements. These compliance checks allowed the author to conduct a functional and effects analysis of the existing regulation relevant to the DLT use case. Such an approach challenges any bias written into existing regulation towards a certain existing (technical or organizational) solution and makes it possible to analyse whether, in a specific use case, the DLT solution is able to achieve the objectives of the regulator functionally equivalently without necessarily meeting all the procedural or formal requirements set in the existing regulation. The described approach allows the author to assess whether the existing regulation is technology-neutral or has an innate bias for a technical or organizational solution that existed during the drafting of the regulation. The following sections provide a summary of the conclusions made on the basis of the use case analysis.

5.2.1 Bias for centralised means of payment

The first DLT use case explored whether anti-money laundering regulation and the application of it in Estonia to bitcoin and its traders in *de Voogd* case was technologically neutral. The research focused on the treatment of bitcoin and bitcoin traders under the anti-money laundering regulation that was valid from 2014–2016 in Estonia (referred to as MLPA I). Research showed that MLPA I separated the treatment of bitcoin from fiat currency under a new *sui generis* category called ‘alternative means of payment’ that was not based on AMLD and

consequently treated the traders of bitcoin differently from the traders of fiat currency. Although, AMLD allowed the EU Member States to develop more stringent rules and additional categories of obligated entities, the Member States needed to notify the Commission of such activity. Though such separation into different subject categories cannot be regarded as contrary to the principle of technology neutrality, the different treatment of these categories can be regarded as contrary to the principle (and also perhaps against the aim of the AMLD) unless the difference of treatment is based on the difference in technology.

Hence, the bias identified in the first use case was the bias for centralised means of payment and, consequently, the bias against alternative means of payment, such as decentralised or distributed. As part of the analysis the author compared *de Voogd* ruling to the application of the EU VAT regulation to bitcoin and its traders in CJEU ruling in *Hedqvist*. The conclusion on bias is largely based on the *Hedqvist* ruling. Based on the *Hedqvist,* the author argues that the difference in treatment of fiat currency and alternative means of payment under MLPA I was contrary to the principle of technology neutrality as in the *Hedqvist* case, CJEU had confirmed these categories to be functionally equivalent. Consequently, not granting these object categories (the means of payment) and subject categories (the traders) equivalent treatment with fiat currency and fiat currency traders, and subjecting the DLT-based object and trading subjects under more stringent compliance rules can be regarded as contrary to the technology neutrality principle.

In the *de Voogd* ruling of the Estonian Supreme Court, bitcoin was qualified as an alternative means of payment under MLPA I, although the court did not identify any grounds related to anti-money laundering regulation objectives that justified the difference in the treatment of these functionally equivalent categories of fiat currency and bitcoin. Furthermore, considering the statements of the Supreme Court in the respective ruling, the court was also of the opinion that the treatment of this *sui generis* category must be proportionate to and considerate of the technological and global use cases of bitcoin. Although the court clearly states these concerns in the ruling, it, nevertheless, did not apply the MLPA I to bitcoin and bitcoin traders in a functional-teleological way nor refer the interpretation of AMLD to CJEU for preliminary ruling to explore whether the introduction of an alternative means of payment category without notification and granting the subjects trading with this category different treatment is at all compliant with AMLD.

In the ruling of the *de Voogd*, the Supreme Court urged the legislative branch is: (i) to assess the effect of MLPA I on bitcoin trade, (ii) to consider adapting MLPA I considering the characteristics of bitcoin trading and (iii) to ensure sufficient flexibility in order to treat innovative technology neutrally. Nevertheless, the Supreme Court itself failed to interpret MLPA I in a functional-technological way, the way the CJEU had interpreted with the EU VAT regulation in the *Hedqvist* case.

Consequently, the research of the first DLT use case presented in this dissertation showed that the courts (and not only legislators) must also conduct a

functional analysis and, upon identifying functional equivalence, grant effects equivalence to the new technological outputs on the basis ofthe existing regulation. The analysis showed that the application of the principle of technology neutrality revealed a bias against 'alternative means of payment' and, although the in the definition of the *sui generis* category of MLPA I was meant to be sustainable, the treatment of this category failed to have a sufficient level of flexibility to allow innovation and different technologies to flourish and to compete. Given the new Digital Finance Package introduced in the EU late 2020 addressing crypto-assets and the fact that the MLPA I has been replaced with multiple different versions of MLPA since 2016 both on the basis of amendments to AMLD and also not based on it, there is no other specific recommendation or course of action suggested by the author on the basis of this analysis.

5.2.2 Bias for centralised administrator of shareholder ledger

The second DLT use case explored a bias in the shareholder ledger administration regulation of Estonian private limited companies under the Estonian Commercial Code (CC). More specifically, the author analysed whether the relevant provisions in the CC were technology-neutral and allowed for the effective use of DLT in the ledger administration of the shares not registered at the CSD (non-CSD shares). In summary, the existing CC does not restrict the use of DLT or any other technology in shareholder ledger administration. In fact, the existing CC regulation is technology-independent as it neither requires nor prohibits the use of any technological solution for ledger administration. However, the author's research showed that the entries in the ledgers maintained by either CSD or non-CSD are valued differently, and the regulation does not allow for effects equivalence to be granted in case functional equivalence with CSD ledger is established in non-CSD ledger administration through the use of any technology. Consequently, the author identified a bias in the CC for CSD maintained ledger. Consequently, the difference of treatment of ledgers, ledger entries and shares registered in these is based on who the administrator of the ledger is. Furthermore, which any non-CSD ledger maintenance solution, irrelevant how sophisticated could not resolve such bias under the existing CC.

Given that DLT is a ledger technology, maintaining shareholder ledgers using DLT, the ledger functionalities ensure trustworthiness, transparency and verification of data entries. Due to these functionalities, the DLT-based shareholder ledger could potentially equivalently perform the functions CSD performs in maintaining the ledger. Consequently, in order to be compliant with the technology neutrality principle, the Estonian regulator should either, using either the GDPR regulative model, introduce the objectives of the technical and organisational measures that need to be fulfilled for any technological solution for ledger maintenance to be considered functionally equivalent to the CSD-maintained ledger or on the basis of the waiver regulative model include flexibility in the CC to allow waivers from more stringent requirements in case of non-CSD

share ledgers in case certain trustworthiness, transparency and verification requirements for data entries are met. Such recommendation is in line with the Pilot Regime that allows exemptions from certain requirements of the CSDR and MIFID II that are "proportionate to and justified"[535] by the use of DLT. Consequently, it would be equally proportionate to expect the Estonian regulator to grant the use of DLT in the shareholder ledger maintenance of non-CSD shares also effects equivalence with the treatment of CSD shares under the CC. As long as the Estonian regulator is mute as to these flexible solutions to achieve effects equivalence, the CC regulation is based on a bias for a centralised solution.

5.2.3 Bias for centralised key management

The third DLT use case explored the certification-centric authentication technology regulation of the eIDAS, analysing whether a DLT-based smart contract signature could be regarded as functionally equivalent to an eIDAS qualified electronic signature. The author identified a bias in the electronic signatures regulation related to key management. The bias was attached to the requirement that the keys needed for electronic signing must be generated and maintained by a trust service provider. This requirement can be regarded as bias as while DLT key generation and management is independent of all service providers. This means that the eIDAS regulation stipulates requirements that have no relevance or reasoned need, in the case of DLT as in DLT-based systems it is possible to issue trustworthy signatures without the use of service providers. Consequently, the author concludes that the eIDAS needs an adaptation through either (i) waiver regulative model as was initiated in the EU with the Digital Finance Package or (i) GDPR model through the introduction of objectives without specific list of procedural requirements or (iii) through polycentric coregulation using multiple stakeholders who are well-versed with available electronic signing solutions.

The only function the DLT-based smart contract analysed in the third DLT model failed to address was the identification function. The research presented showed that the inherent identification function can be added on the smart contract solution as a separate stand-alone function or be performed based on other evidence, such as IP address, e-mail address, phone number, etc., or alternatively the EU regulator could also expand the freedom of contract of the parties and enable contracts to be concluded in an electronic form which do not require identification function to be performed at all. If regulation, such as the eIDAS, does not grant effects equivalence to functionally equivalent alternative electronic signature systems, the regulation is not in compliance with the technology neutrality principle. Such shortcoming can be considered a substantial drawback given the expected growth of electronic commerce. Any liberalisation of the regulation under investigation in the third DLT use case is much needed. This liberalisation could also be extended to the concept of anonymous or pseudo-

[535] Article 5 of the Pilot Regime.

nymous transactions in the online domain, which the author is sure is also a much-needed development given the prevalent privacy concerns of online commerce.

As self-executing smart contracts are easier to enforce than non-self-executing contracts, the balancing exercise does not necessarily create an advantage for contracts with ease of identification but often creates an advantage for contracts ensuring ease of enforcement. One is not necessarily better than the other simply because we as users and also the regulator are accustomed to it. Any preference towards one solution over the other by regulators shows that they indulge themselves to an infrastructural bias against innovative solutions that may or may not include distributed networks, ledgers and DLT.

5.3 Ensuring DLT-neutrality in regulation

The need to address infrastructural bias for centralized means of payment, centralized ledger maintenance and centralized key generation and maintenance is a in line with the technology-neutrality principle and the sub-principle of functional equivalence must be utilized to recognize the objectives different regulators desire to reach through including these biases in the regulation. Such recognition allows to conduct a functional and effects analysis of the innovative technological solution used against these objectives and conclude whether the new solution is equivalently suitable to perform the required functions of the regulation and should be granted effects equivalence. To ensure DLT-neutrality, the regulation should allow effects equivalence to all DLT-based functionally equivalent solutions.

In light of this conclusion and given that new DLT applications are constantly being developed, the author asked in the dissertation whether it is at all possible to ensure DLT-neutrality in regulation that also has a certain level of sustainability. DLT is after all an 'all-purpose technology', which means the technology can be used in multiple sectors and facets of society. This creates a need to evaluate many regulatory frameworks to identify these biases and, if necessary, resolve these. Such a task called for an exploration into the regulative models and strategies that could sustainably achieve DLT-neutrality across jurisdictions.

For this purpose, the author addressed the sustainable DLT-neutrality quest on a foundational level. This means that upon conducting such exploration into regulative strategies, not one specific DLT use case was used as an example as otherwise the research would have been fragmented to that use case, instead, the wider perspective of regulative strategies and models was considered.

This dissertation did not treat DLT regulation in any way as a separate field of study or in need of separate regulation. Nevertheless, introducing DLT-specific regulation is not in breach of the technology neutrality principle as long as effects equivalence is granted across different technologies. This means that each technology can be addressed by a separate regulation that considers its functional differences and still be technology neutral. The Digital Finance Package serves as an example here, as a DLT-specific regulation that adapts existing regulation to consider DLT functionalities while maintaining protection interests similar to

those addressed for existing technology. Consequently, in this dissertation, the author discussed the different regulative strategies in relation to DLT, aiming to identify alternative paths sustainably to ensure DLT-neutrality across regulatory frameworks.

As research showed, these regulative strategies can be expressed in different regulative models. For example, in the case of the Digital Finance Package, the impact assessment showed that although the Commission identified similar regulative strategies for the Pilot Regime and the MiCA Proposal, the models chosen for adapting existing regulation were different. Among the alternative options discussed in the Pilot Regime were issuing interpretation in the form of guidance on the applicability of EU regulation to crypto-assets or adapting existing EU regulatory framework through either a more comprehensive regulation change or a temporary and iterative option chosen by the regulator in the Pilot Regime.

On the other hand, the MiCA Proposal identified an even wider selection of alternative models (full harmonisation or an opt-in licensing regime coupled with a separate regime for stablecoins) under these same regulative strategies, which all focused on adapting existing regulation. The compromise of the MiCA Proposal is a selection of these alternative options all in one.

Therefore, in this dissertation, the author addressed alternative models of regulation as part of these regulative strategies that as research showed are able to ensure DLT neutrality in a sustainable way. The models discussed in the dissertation include functional-teleological interpretation and the waiver solution as part of the strategy to apply existing regulation and the UNCITRAL and the GDPR model along with either self-regulation or polycentric coregulation as models for adaptation of existing regulation. Furthermore, the author concluded that these regulative strategies and models are often adopted in parallel (wait-and-see, along with the application of existing regulation) or coupled with temporary additional exploration techniques (such as the sandbox regime).

As the research presented in this dissertation showed, both the subsidiarity principle-based model used in the GDPR and the strategy of polycentric coregulation (which includes the constantly evolving amorphous soft law, multiple sources of regulation and reliance on stakeholders, etc.) enable a certain level of sustainability and flexibility, allowing the iteration of regulatory responses to the fast-paced change brought about by DLT.

To exemplify this, the Digital Finance Package, with the example of the Pilot Regime, is a revolutionary regulative approach employing constantly iterative functionalities in respect of the subsidiarity principle, targeting the sustainability goal through the waiver regime and reaching for neutrality through allowing a directly applicable list of exemptions from compliance requirements to be customised to specific DLT applications. The referred Pilot Regime shows that the EU regulator is without a doubt able to revolutionise with regulatory strategy by adapting to the needs of distributed infrastructure in order to promote competition and innovation.

Nevertheless, the Digital Finance Package merely addresses the financial sector and its regulation; however, DLT has an array of other use cases across

multiple sectors, and regulative strategies and models securing neutrality in a sustainable way should also be a priority in these other regulatory frameworks. DLT challenging substantive law is not the only challenge, as DLT can also be used in the delivery of regulation and in complying with the regulation. As discussed in the final section of chapter 3, DLT enables the delivery of regulation to its subjects in the form of a code and allows compliance with the requirements of regulation also be executed through the use of the built-in code. Therefore, as the financial sector is allowing use of DLT in fulfilling financial compliance requirements, regulators should also explore the use of DLT for any other type of regulatory compliance. Consequently, the challenge posed by DLT to regulators should no longer be limited to the content layer (the content of the provisions of regulation themselves), but also expanded to the transport layer (the delivery tool of the content of the provisions), paving the way for code-based regulation that allows compliance through the use of the same code (DLT used as regulatory compliance tool).

Unfortunately, neutrality as a goal can also be used to create an advantage (as the EU Digital Finance Package proposal shows) to the use of one technology (e.g., DLT) and could therefore, be also considered as technology-partial as it promotes one technology over another. DLT neutrality might not necessarily be technology-neutral to all other technologies unless effects equivalence of the DLT-specific regulation is secured to other functionally equivalent technologies. Consequently, the challenge to be sustainably technology-neutral is considerably more difficult than being merely sustainably DLT-neutral.

Finally, the research presented in this dissertation established that regulators (including legislative, executive and judiciary branch), not only the innovator, needs to be active in learning about DLT and its wider context in order to ensure DLT-neutrality and identify infrastructural bias in regulation, but it should be the aim of regulators themselves to interpret and implement existing regulation in a technologically neutral way, issue guidelines that explain compliance objectives (rather than enforce existing unfit requirements) and promote market-led polycentric coregulation efforts. All of these activities are creating and sharing knowledge, and through such cooperation activities the regulator is supporting innovation and promoting regulation compliant behaviour without putting the burden of obtaining legal clarity and certainty on any single early-adopter.In this dissertation, the author was exploring biases written into existing regulation using the principle of technology neutrality as a benchmark and consequently, the aim of the dissertation was not to explore the specific adaptations needed to the existing regulation applicable and relevant in the analysed DLT use cases. Such analysis of specific adaptations needed or justifications for not making these adaptations in all three DLT use cases needs to be addressed in future work. Furthermore, any limitations and challenges raised in this dissertation similarly provide opportunities for future research. Not to mention, the use of DLT in corporate applications, the wider use of smart contracts and cryptocurrencies, crypto-assets and non-fungible tokens calls for similar explorations into the biases of the relevant existing regulation that may lead to adaptations of far more

sources of existing regulation than this dissertation addressed. The code-based or algorithmic regulation is a topic that certainly is gaining momentum and should be further explored also in the context of the challenges raised in this dissertation – specifically how to address the fast pace change of technology in relation to self-executing contracts, self-driving cars and self-operating machines with a dynamic and adaptive regulation. Lastly, given the popularity of online commerce and rivalry desire for privacy and security while conversing and trading in the digital domain, the identification and authentication technology along with the domain of smart contracts needs the attention of legal scholars to address anonymous and pseudonymous online contracts and self-sovereign identity administration.

The focus of technology neutrality principle has certainly moved from the comparison of online-offline dimensions to a highly developed virtual world available on multiple different infrastructures – centralized, decentralized and distributed, with primary and subset levels of interactions with communities, platforms, peers (P2P) and machines. From the time the principle was discussed in the writings of Koops and Reed in the context of equal treatment of offline-online domains, the relevance of digital technology has grown exponentially and consequently, the relevance of the neutrality principle has multiplied. However, due to the complexities introduced with such development of the digital domain, the functional and effects analysis are of utmost importance as both the regulator and the legal scholar should be exploring these realities as comparative legal theorists are exploring foreign legal systems – on the basis of functional approach and free of assumptions. The author's findings in the dissertation concur with those of Reyes, Finck, de Filippi and Wright that the regulatory challenges specific to DLT and blockchain need regulators to expand their traditional regulatory strategies recognizing endogenous, code-based and self- or co-regulation alternatives to respond to these challenges. Finally, all of the enumerated challenges of infrastructural paradigm shift presented in this dissertation and biases the onlookers have when observing this transformation from one paradigm to the next can be recognized already in the work of Lessig and consequently, the findings in this dissertation merely build on his work while exploring a new dimension.

REFERENCES

Literature and publications

1. **Abbott, Kenneth W**., Marchant, Gary E., Corley, Elizabeth A. 'Soft law oversight mechanisms for nanotechnology' (2012) 52 Jurimetrics J., p. 279–312.
2. **Al-Bassam, M.** SCPKI: a smart contract-based PKI and identity system (in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts ACM, April 2017), <http://www0.cs.ucl.ac.uk/staff/M.AlBassam/publications/scpki-bcc17.pdf> accessed 3 July 2019.
3. **Alekand, A.** 'Osaühingu osanikeregistri pidamine' (2015) Juridica I, p. 13, <https://www.juridica.ee/article_full.php?uri=2015_1_osa_hingu_osanikeregistri_pidamine&pdf=1> accessed 4 January 2019.
4. **Anderlini L., Felli L., and Riboni A**. "Statute Law or Case Law?" LSE STICERD Research Paper No. TE/2008/528 (August 2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401783>.
5. **Antonopoulos, Andreas M.** Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014.
6. **Armitage A., Cordova A. and Siegel R.** 'Design-Thinking: The Answer to the Impasse Between Innovation and Regulation', UC Hastings Research Paper No. 250, 15, https://repository.uchastings.edu/cgi/viewcontent.cgi?article=2568&context=faculty_scholarship> accessed 5 April 2020.
7. **Armitage A., Cordova A. and Siegel R.** 'Design-Thinking: The Answer to the Impasse Between Innovation and Regulation' (2017) 250 UC Hastings Research Paper, p. 15, Available at: <https://repository.uchastings.edu/cgi/viewcontent.cgi?article=2568&context=faculty_scholarship> accessed 5 April 2020.
8. **Bennett Moses, L.** 'Understanding legal responses to technological change: the example of in vitro fertilization' (2005) 6 (2), Art. 4., *Minnesota Journal of Law, Science and Technology*, <https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1337&context=mjlst> accessed 28 November 2018.
9. **Berarducci, P.** 'Collaborative Approaches to Blockchain Regulation: The Brooklyn Project Example' (2019) 69 Cleveland State Law Review 23.
10. **Berman, Harold J.** 'Law and Revolution: The Formation of the Legal Tradition' (1983) Harvard University Press, p. 10;
11. **Bernstein, L.** 'Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry' (1992) 21 (1) *The Journal of Legal Studies*, pp. 115–57, <https://www.jstor.org/stable/724403?seq=1> accessed 30 May 2020.
12. **Bijker, W.** *Of Bicycles, Bakelites and Bulbs: Toward a theory of Sociotechnical Change* (MIT Press., 1995).
13. **Black, J.** 'Constitutionalising Self-Regulation', (1996) 59 24 Modern Law Review, p. 27.
14. **Bodó B., Gervais D. and Quintais, J. P.** 'Blockchain and smart contracts: the missing link in copyright licensing?' (2018) 26 (4) International Journal of Law and Information Technology, pp. 311–312, DOI: <https://doi.org/10.1093/ijlit/eay014> accessed 31 July 2019.

15. **Borgsten, E. and Jiang, O.** 'Authentication using Smart Contracts in a Blockchain' (MA thesis in Computer Systems and Networks, University of Gothenburg and Chalmers University of Technology, 2018), p. 15 <http://publications.lib.chalmers.se/records/fulltext/256254/256254.pdf> accessed 10 July 2019.
16. **Borgsten, E. and Jiang, O.** 'Authentication using Smart Contracts in a Blockchain' (MA thesis in Computer Systems and Networks, University of Gothenburg and Chalmers University of Technology, 2018), p. 15 <http://publications.lib.chalmers.se/records/fulltext/256254/256254.pdf> accessed 10 July 2019.
17. **Brynjolfsson, E. and McAfee, A.** *The Second Machine Age* (W.W. Norton: New York, London, 2016), p. 90.
18. **Busch, De Franceschi**, Algorithmic Regulation and Personalized Law. A Handbook (forthcoming 2021 Beck Hart Sowon).
19. **Butenko, A. and Larouche, P.** 'Regulation for innovativeness or regulation of innovation?', (2015) 7 (1), Law, Innovation and Technology, pp. 52–82. DOI: <10.1080/17579961.2015.1052643> accessed 20 November 2018.
20. **Cantero Gamito, M.** 'Regulation.com Self-Regulation and Contract Governance in the Platform Economy: A Research Agenda' (2017) 9 (2) European Journal of Legal Studies, p. 53, <https://ejls.eui.eu/wp-content/uploads/sites/32/pdfs/Spring2017/REGULATION.COM._SELF-REGULATION_AND_CONTRACT_GOVERNANCE_%20IN_THE_PLATFORM_ECONOMY_A_RESEARCH_AGENDA.pdf>.
21. **Cantero Gamito, M.** 'Regulation.com Self-Regulation and Contract Governance in the Platform Economy: A Research Agenda' (2017) 9 European Journal of Legal Studies 53.
22. **Cantero Gamito, M.** 'The Legitimacy of Standardisation as a Regulatory Technique in Telecommunications' (2020), in Eliantonio, Mariolina, Caufmann, Caroline (ed), *The Legitimacy of Standardization as a Regulatory Technique A Cross-disciplinary and Multi-level Analysis* (Edward Elgar Publishing, 2020), pp. 222–242.
23. **Comandé G., Ebers M., Zou M.** (eds.) 'Machine Intelligence, and Law. Data Science, Machine Intelligence, and Law' (Springer 2020).
24. **Craig, CJ**. "Technological Neutrality: (Pre)Serving the Purposes of Copyright Law." Osgoode Legal Studies Research Paper Series 45 (2014): 275–276 https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1044&context=olsrps.
25. **Cerf, V.** 'Keep the Internet Open' (*New York Times*, 24 May 2012), <www..nytimes.com/2012705/25/opinion/keep-the-internet-open.html>; **Hamblen, D.** 'Only the Limits of Our Imagination: An Exclusive Interview with RADM Grace M. Hopper' (*Ships Ahoy*, July 1986), <http://web.archive.org/web/20090114165606/http://www.chips.navy.mil/archives/86_jul/interview.html>.
26. **Chang, S.** "Here's all the money in the world, in one chart." MarketWatch.com (28 November 2017) <https://www.marketwatch.com/story/this-is-how-much-money-exists-in-the-entire-world-in-one-chart-2015-12-18>.

27. **Christidis, K. and Devetsikiotis, M.** *Blockchains and Smart Contracts for the Internet of* Things (Special section on the plethora of research in the internet of things (IoT), 3 June 2016), DOI: <10.1109/ACCESS.2016.2566339> or <http://people.cs.pitt.edu/~mosse/courses/cs3720/blockchain-iot.pdf> accessed 1 June 2019.
28. **Christidis, K. and Devetsikiotis, M.** *Blockchains and Smart Contracts for the Internet of* Things (Special section on the plethora of research in the internet of things (IoT), 3 June 2016), DOI: <10.1109/ACCESS.2016.2566339> or <http://people.cs.pitt.edu/~mosse/courses/cs3720/blockchain-iot.pdf> accessed 1 June 2019.
29. **Clinton, W.J. and Gore, Al Jr.** 'Framework for Global Electronic Commerce', White House (1 July 1997), <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html> accessed 12 November 2018.
30. **Coleman, L.** *Tezos Investors Forced to Undergo KYC Nearly 1 Year after ICO* (12 June 2018), <https://www.ccn.com/tezos-investors-forced-to-undergo-kyc-nearly-1-year-after-ico/> accessed 24 June 2019.
31. **Collingridge, D.** *The Social Control of Technology* (St Martin's Press, New York, 1980).
32. **Crews, C. W.** *Mapping Washington's Lawlessness: An Inventory of Regulatory Dark Matter* 2017 Edition 20, p. 49, <https://cei.org/ sites/default/files/Wayne%20Crews%20-%20Map> accessed 30 March 2020.
33. **Cuccuru, P.** 'Beyond bitcoin: an early overview on smart contracts', 25 (3) 2017 International Journal of Law and Information Technology, p. 180. DOI: <https://doi.org/10.1093/ijlit/eax003> accessed 19 October 2020.
34. **Daniel J. Gervais.** 'Towards a new core international copyright norm: the reverse three-step test' (2005) 9 Marquette International Property Law Review, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=499924> accessed 27 November 2019.
35. **David, G.** 'How the Internet is making jurisdiction sexy (again)', 25 (4) 2017 International Journal of Law and Information Technology, pp. 249–258, DOI: <https://doi.org/10.1093/ijlit/eax019> accessed 22 March 2020.
36. **Davidson, Sinclair, De Filippi P., and Potts J.** "Economics of Blockchain" (March 8, 2016) http://dx.doi.org/10.2139/ssrn.2744751.
37. **De Filippi, P. and Wright, A.** *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018), p. 80.
38. **De Filippi and Hassan, S.** 'Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code' (2016) 21(12) First Monday.
39. **Downes, L.** *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age* (Basic Books, 2009).
40. **Downes, L.** 'Take Note Republic and and Democrats, This is What Pro-innovation Platform Looks Like' (*Washington Post,* 7 January 2015), <www.washingtonpost.com/news/innovations/wp/2015/0107/take-note-republicans-and-democrats-this-is-what-a-pro-innovation-platform-looks-like>.

41. **Ebers, M., Cantero Gamito, M**. 'Algorithmic Governance and Governance of Algorithms: An Introduction' in Martin Ebers; Marta Cantero Gamito (eds.). Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges. (Cham: Springer Nature 2020).
42. **Eenmaa-Dimitrieva, H., Schmidt-Kessen, M. J.**, 'Creating Markets in No-trust Environments: The Law and Economics of Smart Contracts' 35 Computer Law & Security Review 69 (2019).
43. **Epstein, R.** 'Can Technological Innovation Survive Government Regulation?' (2013) 36 Harvard Journal of Law and Public Policy pp. 87–88, <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=4977&context=journal_articles> accessed 04 April 2020.
44. **Fenwick M., McCahery J. and Vermeulen, E.** 'The End of 'Corporate' Governance: Hello 'Platform' Governance' (2019) 20 European Business Organization Law Review.
45. **Finck, M.** *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 2019) pp. 153–181.
46. **Furrer, A. and Müller, L.** 'Functional equivalence of digital legal transactions A fundamental principle for assessing the legal validity of legal institutions and legal transactions under Swiss law', Jusletter (18 June 2018), p. 15, <https://www.mme.ch/fileadmin/files/documents/MME_Compact/2018/180619_Funktionale_AEquivalenz.pdf> accessed 12 November 2020.
47. **Gervais, D.J.** "Towards a new core international copyright norm: the reverse three-step test." Marquette International Property Law Review 9 (2005) // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=499924.
48. **Greenberg, B. A.** 'Rethinking Technology Neutrality', (2016) 100 Minnesota Law Review, p.1495.
49. **Gudkov, A.** 'Control on Blockchain Network' (2018) 42 Nova Law Review.
50. **Hacker P., Lianos I., Dimitropoulos G. and Eich, S.** 'An Introduction', in Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich, eds., *Regulating Blockchain Techno-Social and Legal Challenges* (Oxford University Press, 2019), p. 2.
51. **Hagermann R., Huddleston Skees J. and Thierer A.** 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (5 February 2018), Colorado Technology Law Journal, p. 59, SSNR: <https://ssrn.com/abstract=3118539> accessed 20 August 2020.
52. **Harvey, D. J.** *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (Bloomsbury Publishing 2017), pp. 59–60.
53. **Harlev, et al.** *Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning,* (Proceedings of the 51st Hawaii International Conference on System Sciences, 2018) <https://core.ac.uk/download/pdf/143481278.pdf> accessed 8 July 2019.
54. **Herian, R.** *Legal Recognition of Blockchain Registries and Smart Contracts.* (EU Blockchain Observatory and Forum 2018) < http://oro.open.ac.uk/59481/> accessed 1 May 2019.
55. **Hildebrandt, M.** *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015), p.140–218.
56. **Hildebrandt, M. and Tielemans, L.** 'Data protection by design and technology neutral law' (2013) 29 Computer Law & Security Review, p. 516.

57. **Hogg, M.** 'Secrecy and Signatures – Turning the Legal Spotlight on Encryption and Electronic Signatures', in Edwards, Lilian, Waelde, Charlotte, *Law & the Internet. A framework for electronic commerce* (Hart Publishing, 2000), p. 37.
58. **Holder, C. et al.** 'Robotics and Law: Key Legal and Regulatory Implications of the Robotics Age', 2016 Computer Law & Security Review 32/3, p. 383. DOI: <https://doi.org/10.2478/bjlp-2019-0011> accessed 3 June 2020.
59. **Hojnik, J.** 'Technology neutral EU law: digital goods within the traditional good/ services distinction', (2017) International Journal of Law and Information Technology 25, pp. 63–84 and p. 71, DOI: <10.1093/ijlit/eaw009> accessed 29 April 2020.
60. **Hörnle, J.** 'Book Reviews. Making Laws for Cyberspace' (2012) 20 (4) IJLT, p. 373.
61. **Ilves, E.** 'Polütsentriline õigus: riik ja õigus ei ole lahutamatud' [Polycentric law (1999) 3 Juridica, pp. 106–109.
62. **Inselberg, K.** 'Tavid kaalub Bitcoiniga kauplemise alustamist' [*Tavid is considering trading bitcoins*] (23 January 2014), Postimees.ee, <https://majandus24.postimees.ee/2671592/tavid-kaalubbitcoiniga-kauplemise-alustamist> accessed 02 May 2020.
63. **Jovanović, B.** 'Browser statistics: Catching the best surf on the Web' (*DataProt*, 2 December 2019), <https://dataprot.net/statistics/browser-statistics/> accessed 03 October 2020.
64. **Jürgen, L.**, Die elektronische Signatur nach europa¨ischem, deutschem und estnischem Recht (Westfälische Wilhelms-Universität Münster 2015).
65. **Kaaru, S**. 'Germany passes law legalizing electronic securities on blockchain' (Business Coingeek 21 December 2020) <https://coingeek.com/germany-passes-law-legalizing-electronic-securities-on-blockchain/> accesssed 27 December 2020.
66. **Kamecke, U. and Körber, T.** 'Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood. Technological Neutrality in the EC Regulatory Framework' (2008), p. 331, <http://www.unigoettingen.de/de/document/download/65b9d0d841b831596888f8fb208e838b.pdf/KameckeKoerber_ECLR08_29%285%29_330-339.pdf> accessed 30 April 2020.
67. **Kiršienė, J., Kelley, C., Kiršys, D., and Žymančius, J.** 'Rethinking the Implications of Transformative Economic Innovations: Mapping Challenges of Private Law', 12 (2) 2018 Baltic Journal of Law & Politics, p. 50, DOI: <https://doi.org/10.2478/bjlp-2019-0011> accessed 18 March 2020.
68. **Klaris, E. and Bedat, A.** 'Copyright liability for linking and embedding: an E.U. versus U.S. comparison and guide' (12 March 2018) <https://klarislaw.com/wp-content/uploads/klarislaw-copyright-liability-for-linking-and-embedding.pdf> accessed 10 December 2019.
69. **Kmia, O.** '*Why Kodak Died and Fujifilm Thrived: A Tale of Two Film Companies*' (*PetaPixel blog*, 2018) <https://petapixel.com/2018/10/19/why-kodak-died-and-fujifilm-thrived-a-tale-of-two-film-companies/>.
70. **Koopman C., Mitchell M. and Thierer A.** 'The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change' (2015) Journal of Business Entrepreneurship and Law 8.

71. **Koops, B.-J.** 'Should ICT Regulation be Technology-Neutral?', in Bert-Jaap Koops et al. *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, 9 IT & Law Series., p. 7 (The Hague: T.M.C. Asser Press 2006), <https://ssrn.com/abstract=918746> accessed 01 December 2019.
72. **Kõve, V.** (2013) 'Kas kinnistusraamatu ja teiste kohtulike registrite korraldus vajab reformi?' *Juridica* VII 2013, p. 461. <https://www.juridica.ee/article_full.php?uri=2013_7_kas_kinnistusraamatu_ja_teiste_kohtulike_registrite_korraldus_vajab_reformi_&pdf=1> accessed 1 January 2018.
73. **Krämera, J. and Schnurr, D.** 'Is there a need for platform neutrality regulation in the EU?', 42 (7) 2018 Telecommunications Policy, pp. 514–529. DOI: <https://doi.org/10.1016/j.telpol.2018.06.004> accessed 9 May 2020.
74. **Lafarre, A. and Van der Elst, C.** 'Blockchain Technology for Corporate Governance and Shareholder Activism', European Corporate Governance Institute (ECGI) – Law Working Paper No. 390/2018 (Tilburg Law School Research Paper No. 2018-7), SSRN: <https://ssrn.com/abstract=3135209> or <http://dx.doi.org/10.2139/ssrn.3135209> accessed 20 October 2020.
75. **Lawrence, L**. Code version 2.0. 2nd Revised Edition. (Basic Books, 2006) <http://codev2.cc/>.
76. **Lielacher, A**. "An Introduction to Cryptoeconomics." BTCMANAGER (June 14, 2017) <https://btcmanager.com/an-introduction-to-cryptoeconomics/>.
77. **Lucking, D.** Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares. Allen & Overy publications, 26 September 2017. [online] <http://www.allenovery.com/publications/en-gb/Pages/Delaware-Passes-Law-Permitting-Companies-to-Use-Blockchain-Technology-to-Issue-and-Track-Shares-.aspx> accessed 05 May 2019.
78. **Maher, I.** 'Competition Law and Transnational Private Regulatory Regimes: Marking the Cartel Boundary' (2011) 38 Journal of Law and Society, p. 119, <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6478.2011.00537.x> accessed 4 April 2020.
79. **Maume, P. and Fromberger, M.** 'Initial Coin Offerings: Are Tokens Securities under EU Law?' (University of Oxford, Faculty of Law blog, 7 September 2018), <https://www.law.ox.ac.uk/business-law-blog/blog/2018/09/initial-coin-offerings-are-tokens-securities-under-eu-law> accessed 01 December 2019.
80. **Maume, P. and Fromberger, M.** 'Regulation of Initial Coin Offerings: Reconciling US and EU Securities Laws' (2019) 19.2 Chicago Journal of International Law, pp. 548–585. SSRN: <https://ssrn.com/abstract=3200037 or http://dx.doi.org/10.2139/ssrn.3200037> accessed 01 December 2019.
81. **Mayer-Schönberger, V.** Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press, 2009.
82. **Maxwell, W. and Bourreau, M.** 'Technology Neutrality in Internet, Telecoms and Data Protection Regulation' (January 2015) 21 (1) Computer and Telecommunications Law Review, SSRN: <https://ssrn.com/abstract=2529680> or <http://dx.doi.org/10.2139/ssrn.2529680>.
83. **McCorry, P., Hicks, A., and Meikeljohn, S.,** Smart contracts for bribing miners. Conference Proceedings The 5th Workshop on Bitcoin and Blockchain Research, 2nd March 2018. Available from: https://fc18.ifca.ai/bitcoin/schedule.html [Accessed 03 May 2018].

84. **Metjahic, L.** 'Deconstructing the DAO: The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations' (2018) 39 Cardozo Law Review.
85. **Minárik, T., and Osula, A.** 'Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law' (2016) 32 (1) Computer Law and Security Review, <111−127.10.1016/j.clsr.2015.12.002>.
86. **Mik, E.** 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity (2017) 9 Law, Innovation and Technology.
87. **Murray, A.** The Regulation of Cyberspace. 1st edition. Routledge-Cavendish, 2006.
88. **Möslein, F**. 'Blockchain Applications and Company Law' (2020) Legal Technology Transformation in Practice (October 27). <https://ssrn.com/abstract=> accessed 26 December 2020.
89. **Nakamoto, S.** *Bitcoin: Peer-to-peer Electronic Cash System* (2008), <https://bitcoin.org/bitcoin.pdf> accessed 12 April 2018.
90. **Nordén, A.** 'Electronic signatures in a legal context', in Magnusson Sjöberg, Cecilia (ed), *IT Law for IT Professionals – an introduction* (Studentlitteratur 2005), p. 173.
91. **Norta, A., Matulevĭcius, R., and Leiding, B.** 'Safeguarding a Formalized Blockchain-Enabled Identity-Authentication Protocol by Applying Security Risk – Oriented Patterns' (2019), Computers & Security, <https://www.sciencedirect.com/science/article/pii/S0167404818302670?dgcid=author> accessed 10 July 2019.
92. **Olivier, G. and Jaccard, B.** 'Smart Contracts and the Role of Law', 23 November 2017 Jusletter IT, p. 10, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885 > accessed 31 July 2017.
93. **Oren, O.** 'ICO's, DAO'S, and the SEC: A Partnership Solution' (2018) 617 Columbia Business Law Review.
94. **Osula, A.** *The Global Rush in Standards in Blockchain. Directions [commentary] EU Institute for Security Studies*, 9 April 2020, <https://directionsblog.eu/the-global-rush-for-standards-in-blockchain/> accessed 03 October 2020.
95. **O'Toole, M. J., Reilly, M. K.** The First Block in the Chain: Proposed Amendments to the DGCL Pave the Way for Distributed Ledgers and Beyond. Harvard Law School Forum on Corporate Governance and Financial Regulation, 16 March 2017. Available from: https://corpgov.law.harvard.edu/2017/03/16/the-first-block-in-the-chain-proposedamendments-to-the-dgcl-pave-the-way-for-distributed-ledgers-and-beyond/#3 [Accessed 30 April 2017].
96. **Papadaki, E.** 'Hyperlinking, making available and copyright infringement: lessons from European national courts' (2017) 8(1) European Journal of Law and Technology, accessed 10 December 2019.
97. **Parker, Geoffrey G., Van Alstyne, Marshall W. and Choudary, Sangeet P.** *Platform Revolution: How Networked Markets Are Transforming the Economy – and How to Make Them Work For You* (W.W. Norton & Company, 2016).
98. **Partz, H.** 'Korean Blockchain Association Reveals Self-regulatory Rules for 14 Member Exchanges' (*Cointelegraph*, 17 April 2018), <https://cointelegraph.com/news/korean-blockchain-association-reveals-self-regulatory-rules-for-14-member-exchanges> accessed 4 April 2020.
99. **Perez, C**. *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages* (Edward Elgar Publishing, Cheltenham, UK), 26 April 2003, ISBN: 978 1 84064 922 2.

100. **Polner, G. et al.**, Delaware Approves Use of Blockchain in New DGCL Amendments. Gibson Dunn Securities Regulation and Corporate Governance Monitor. 31 July 2017. [online] <http://securitiesregulationmonitor.com/Lists/Posts/Post.aspx?ID=299> accessed 07 May 2018.
101. **Ranchordas, S. and van 't Schip, M.** 'Future-Proofing Legislation for the Digital Age' (8 August 2019), in S. Ranchordas and Y. Roznai (eds), *Time, Law, and Change* (Hart, 2020, Forthcoming) (University of Groningen Faculty of Law Research Paper No. 36/2019), SSRN: <https://ssrn.com/abstract=3466161> or <http://dx.doi.org/10.2139/ssrn.3466161>.
102. **Reed, C.** 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 (3) International Journal of Law and Information Technology, p. 248, DOI:<https://doi.org/10.1093/ijlit/eaq006> accessed 9 May 2020.
103. **Reed, C.** 'Taking Sides on Technology Neutrality', SCRIPTed 263 4 (3) (September 2007), p. 264, <http://heinonline.org/HOL/P?h=hein.journals/scripted4&i=281> accessed 20 November 2018.
104. **Reed, C**. 'The Law of Unintended Consequences – embedded business models in IT regulation' (2007) The Journal of Information and Technology Law 1, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/ accessed 22 November 2020
105. **Reed, E.** 'Equity Tokens vs. Security Tokens: What's the Difference?' (13 February 13, 2019), Bitcoin Market Journal, <https://www.bitcoinmarketjournal.com/equity-token/> accessed 23 July 2019.
106. **Reyes, C. L.** "Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal." 61 Vill. L. Rev. 191 (2016)
107. **Rhue, L.** 'Trust is All You Need: An Empirical Exploration of Initial Coin Offerings (ICOs) and ICO Reputation Scores' (16 May 16, 2018), p. 14. SSRN: <https://ssrn.com/abstract=3179723> or <http://dx.doi.org/10.2139/ssrn.3179723> accessed 24 July 2019.
108. **Rodrigues, U.** 'Law and the Blockchain' (2019) 104 Iowa Law Review.
109. **Ryan, M.J. and Efatmaneshnik, M.** 'Future Proofing Process' (27th Annual INCOSE International Symposium, 2017), DOI: <10.1002/j.2334-5837.2017.00403.x> accessed 22 March 2020.
110. **Saad, R.** 'Mida arvab Eesti Pank bitcoinist?' (What does the Bank of Estonia think of bitcoin?), Äripäev (18 December 2013), <https://www.aripaev.ee/uudised/2013-12-18/mida_arvab_eesti_pank_bitcoinist> accessed 02 May 2020.
111. **Saare, K. et al.** *Ühinguõigus I*, Juura, 2015, pp. 53–54.
112. **Salami, I.** 'Why unregulated cryptocurrencies could trigger another financial crisis' (The Conversation blog, 10 January 2018), <https://theconversation.com/why-unregulated-cryptocurrencies-could-trigger-another-financial-crisis-89808>.
113. **Sardá, T., Natale, S., Sotirakopoulos, N. and Monaghan, M.** 'Understanding online anonymity' (2019) 41(4) *Media Culture & Society*, DOI: <10.1177/0163443719842074> accessed 3 October 2020.
114. **Savin, A.** 'Rule Making in the Digital Economy: Overcoming Functional Equivalence As a Regulatory Principle in the EU' (Copenhagen Business School, CBS LAW Research Paper 19–10, 24 February 2019), 22 (8) Journal of Internet Law, SSRN: <https://ssrn.com/abstract=3340886> accessed 28 November 2019.

115. **Savin, A**. 'EU Regulatory Models for Platforms on the Content and Carrier Layers: Convergence and Changing Policy Patterns' (November 14, 2018). The Nordic Journal of Commercial law, 1/2018, Copenhagen Business School, CBS LAW Research Paper No. 19–08, <https://ssrn.com/abstract=3284434> accessed 14 November 2020.
116. **Schwarcz, S. L**. 'Regulating Financial Change: A Functional Approach', 100 Minnesota Law Review 1441–1494 (2016). <https://scholarship.law.duke.edu/faculty_scholarship/3309> accessed 8 March 2021.
117. **Seipel, P.** 'IT Law in the Framework of Legal Informatics', Scandinavian Studies in Law (Stockholm Institute for Scandianvian Law), 2004, p. 46. ISSN 0085-5944, <https://www.scandinavianlaw.se/pdf/47-2.pdf>.
118. **Sein, K.**, Tehingu vorminõuded ja nende järgimata jätmise tagajärjed, Juridica VII (2010).
119. **Sklaroff, J.M**. 'Smart Contracts and the Cost of Inflexibility' (2018) 166 University of Pennsylvania Law Review.
120. **Shaan, R.** The Difference Between Blockchains & Distributed Ledger Technology. [blog entry] Medium Blog Towards Data Science (2018). Available from: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 [Accessed 01 May 2018].
121. **Shaw, S.R.** 'There is no silver bullet: solutions to Internet jurisdiction', 25 (4) 2017 International Journal of Law and Information Technology, pp. 283–308. DOI: <https://doi.org/10.1093/ijlit/eax017> 22 March 2020.
122. **Song, W.**, Bullish on blockchain: examining Delaware's approach to distributed ledger technology in corporate governance law and beyond. Harvard Law Review (2018). Available from: http://www.hblr.org/2018/01/bullish-on-blockchain-examiningdelawares-approach-to-distributed-ledger-technology-in-corporate-governance-law-andbeyond/ [Accessed 07 May 2018].
123. **Stromberg G. T. et al.** Are Headwinds Hampering Delaware's Blockchain Initiative? Law 360, 23 March 2018. Available from: https://jenner.com/system/assets/publications/17844/original/stromberg%20Law360%20March%2023%202018.pdf?1521837416 [Accessed 14 January 2019].
124. **Stuart Minor, B.** 'Evaluating E-Rulemaking: Public Participation and Political Institutions' (2006), Duke Law Journal, <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1283&context=dlj> accessed 5 April 2020.
125. **Svantesson, D.** 'The holy trinity of legal fictions undermining the application of law to the global Internet', 23 (3) 2015 International Journal of Law and Information Technology, pp. 219–234, DOI: <https://doi.org/10.1093/ijlit/eav007> accessed 22 March 2020.
126. **Taekema, S.** *Relative Autonomy. A Characterisation of the Discipline of Law*, in van Klink, Bart, *Law and Method. Interdisciplinary Research into Law*, p. 41.
127. **Thierer, A.** *Permissionless innovation. The Continuing Case for Comprehensive Technological Freedom*, Revised and Expanded Edition (Mercatus Center, George Mason University), 2016.
128. **Tusikov, N.** *Chokepoints. Global Private Regulation on the Internet.* (University of California Press, 2017), p. 8.

129. **Van der Haar, I. M.** *The principle technological neutrality: connecting EC network and content regulation* (2008), <https://pure.uvt.nl/ws/portalfiles/portal/1063437/3240352.pdf> accessed March 2019.
130. **Veerpalu, A.** 'Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De Voogd and Hedqvist', 11 (2) Baltic Journal of Law & Politics, p. 78. DOI: <https://doi.org/10.2478/bjlp-2018-0011> accessed 15 April 2020.
131. **Veerpalu, A.** 'Shareholder ledger using distributed ledger technology: the Estonian perspective', 13 (2) Masaryk University Journal of Law and Technology, <277−310.10.5817/MUJLT2019-2-6>.
132. **Veerpalu, A.** 'Functional Equivalence: An Exploration Through Shortcomings to Solutions' (2019) 12 (2) Baltic Journal of Law & Politics, pp. 134–162, DOI: <https://doi.org/10.2478/bjlp-2019-0015> accessed 7 June 2020.
133. **Veerpalu, A.** 'Computational Law & Blockchain Festival DISCUSS Symposium Reports: Tartu Nod', 24 June 2018, Stanford Journal of Blockchain Law & Policy, <https://stanford-jblp.pubpub.org/pub/tartu> accessed 15 July 2019.
134. **Veerpalu A., Jürgen L., da Cruz Rodrigues e Silva E. and Norta A.** 'The hybrid smart-contract agreement challenge to European electronic signature regulation' (2020) 28 (1) International Journal of Law and Information Technology, DOI: <eaaa005, https://doi.org/10.1093/ijlit/eaaa005> accessed 31 May 2020.
135. **Walden, I.** "Press regulation in a converging environment": 61–82. In: L. Gillies and D. Mangan, eds. Mapping the rule of law for the Internet. Edward Elgar Publishing, 2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2717734>.
136. **Wheatley, A.** "Cash Is Dead, Long Live Cash." Finance & Development Vol. 54, No. 2 (June 2017) <https://www.imf.org/external/pubs/ft/fandd/2017/06/wheatley.htm>.
137. **Zetzsche D. A., Buckley R. and Arner D.** 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) *University of Illinois Law Review,* p. 1361.

Normative documents and official commentary

Estonian legislation

1. Administrative Procedure Act [*haldusmenetluse seadus*] – RT I 2001, 58, 354; RT I, 13.03.2019, 55.
2. Code of Administrative Court Procedure [*halduskohtumenetluse seadustik*] – RT I, 13.03.2019, 54; RT I, 23.02.2011, 3.
3. Commercial Code [*äriseadustik*] – RT I 1995, 26, 355; versions RT I, 10.07.2020, 35, RT I, 17.03.2020, 1; RT I, 28.02.2019, 10; RT I, 17.11.2017, 22.
4. Constitution of the Republic of Estonia [*Eesti Vabariigi Põhiseadus]* – RT I, 15.05.2015, 2.
5. Decree of the Minister of Justice no 60 (2012), Statute of the registry department of the court [*kohtu registriosakonna kodukord*] – RT I, 28.12.2012, 10.
6. Electronic Communication Act *[elektroonilise side seadus]* – RT I 2004, 87, 593; RT I, 20.05.2020, 34.
7. Electronic Identification and Trust Services for Electronic Transactions Act, [e-*identimise ja e-tehingute usaldusteenuste seadus*] – RT I, 25.10.2016, 1.

8. Estonian Central Register of Securities Act [*Eesti väärtpaberite keskregistri seadus*] – RT 2000, 57, 373; RT I, 13.03.2019, 201.
9. Family Law Act [perekonnaseadus]. RT I 2009, 60, 395, RT I, 09.05.2017, 29.
10. General Part of the Civil Code Act (GPCCA) [*tsiviilseadustiku üldosa seadus*] – RT I 2002, 35, 216; versions RT I, 06.12.2018, 3; RT I, 23.05.2020, 4.
11. Law of Obligations Act [*võlaõigusseadus*] – RT I 2001, 81, 487, RT I, 20.02.2019, 8.
12. Money Laundering and Terrorist Financing Prevention Act of Estonia [*rahapesu ja terrorismi rahastamise tõkestamise seadus*] – RT I 2008, 3, 21 (MLPA I).
13. Money Laundering and Terrorist Financing Prevention Act of Estonia, [*rahapesu ja terrorismi rahastamise tõkestamise seadus*] – RT I 06.07.2016, 13 (MLPA II).
14. Money Laundering and Terrorist Financing Prevention Act of Estonia, [*rahapesu ja terrorismi rahastamise tõkestamise seadus*] – RT I, 17.11.2017, 2 (MLPA III).
15. Notarisation Act [tõestamisseadus] – RT I 2001, 93, 564; RT I, 22.02.2019, 3.
16. Personal Data Protection Act [*isikuandmete kaitse seadus]* – RT I, 04.01.2019, 11.
17. Product Conformity Act [*toote nõuetele vastavuse seadus*) – RT I 2010, 31, 157; RT I, 30.06.2020, 23.
18. Public Information Act [*avaliku teabe seadus*] – RT I 2000, 92, 597; RT I, 14.11.2018, 5.
19. Public Procurement Act [*riigihangete seadus]* – RT I, 01.07.2017, 1; RT I, 08.07.2020, 8.
20. Securities Register Maintenance Act [v*äärtpaberite registri pidamise seadus*] – RT I 2000, 57, 373; RT I, 26.06.2017, 1.

Other countries legislation

1. Innovative Technology Arrangements and Services Act (2018) of Malta, ACT No. XXXIII of 2018, <https://mdia.gov.mt/wp-content/uploads/2018/10/ITAS.pdf> accessed 31 May 2020.
2. Delaware State Senate 149th General Assembly Senate Bill No. 69 An act to amend title 8 of the Delaware Code Relating to the General Corporation Law. [online] <https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId= 25730& legislationTypeId=1&docTypeId=2&legislationName=SB69> ccessed 07 May 2018].
3. Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés) published in JORF n°0121 du 23 mai 2017 texte n° 20. <https://www.legifrance.gouv.fr/ affichTexte.do?cidTexte=JORFTEXT000034795042&categorieLien=id> accessed 1 May 2018].

EU legislation

1. Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 47–390.
2. Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax OJ L 347, 11.12.2006, p. 1–118 (VAT Directive).

3. Commission Implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.
4. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16.
5. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Copyright or InfoSoc Directive). Official Journal of the European Union, L 167, 22.6.2001.
6. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). OJ L 108, 24.4.2002, p. 33–50.
7. Directive (EU) 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) (Text with EEA relevance), Official Journal of the European Union, L 111, 5.5.2009, p. 16–22.
8. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance) OJ L 267, 10.10.2009, p. 7–17.
9. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Better Regulation Directive, Text with EEA relevance). OJ L 337, 18.12.2009, p. 37–69.
10. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance, the 4th AML Directive or AMLD), OJ L 141, 5.6.2015, p. 73–117.
11. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016, p. 1–30.
12. Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
13. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the

financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance, the 5th AML Directive or AMLD) PE/72/2017/REV/1, OJ L 156, 19.6.2018
14. Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax OJ L 347, 11.12.2006, p. 1–118 (VAT Directive).
15. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) PE/52/2018/REV/1 OJ L 321
16. Regulation (EU) 2014/910 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
17. Regulation (EU) 2014/909 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 Text with EEA relevance OJ L 257, 28.8.2014, p. 1–72.
18. 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 the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.
19. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance) PE/56/2019/REV/1 OJ L 186, 11.7.2019, p. 57–79.
20. 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 the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.
21. Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of tele-communications infrastructure and repealing Decision No 1336/97/EC Text with EEA relevance OJ L 86, 21.3.2014, p. 14–26.

Conventions, charters, declarations, guidelines, green papers and model laws

1. Charter of Fundamental Rights of the European Union, Official Journal of the European Communities (26.10.2012) C 326:391–407, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf> accessed 26 November 2018.
2. ENISA. *Security guidelines on the appropriate use of qualified electronic signatures.* Guidance for users, December 2016, <https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures/at_download/fullReport> accessed 11 May 2020.
3. ENISA. *Standardisation in the field of Electronic Identities and Trust Service Providers. Inventory of activities*, December 2014, <https://www.enisa.europa.eu/publications/standards-eidas/at_download/fullReport> accessed 11 May 2020.
4. European Commission. Directorate-General for the Information Society and Media. Declarations. Global information networks: Realising the potential. European ministerial Conference. Bonn, 6 to 8 July 1997, <https://op.europa.eu/en/publication-detail/-/publication/0d76a85c-e66a-41af-91c2-28cd29a85094> accessed 29 April 2020.
5. THE EUROPEAN PARLIAMENT, THE COUNCIL OF THE EUROPEAN UNION AND THE EUROPEAN COMMISSION 2016, Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making *OJ L 123, 12.5.2016, p. 1–14*
6. European Commission, Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union'COM (2017) 495 final, 8.
7. Okinawa Charter on Global Information Society, <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> accessed 29 April 2020.
8. Opinion of the Economic and Social Committee on the "Green Paper on European Union Consumer Protection" (COM(2001) 531 final) 27.5.2002, OJ C 125, p. 1–5.
9. UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998, 12 June 1996, <https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce> accessed 2 May 2020.
10. UNCITRAL Model Law on Electronic Signatures (2001), 5 July 2001, <https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures> accessed 2 May 2020.
11. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, <http://www.uncitral.org/pdf/english/texts/electcom/V1504118_Ebook.pdf> accessed 28 November 2019.
12. World Summit on the Information Society. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium. Document WSIS-03/GENEVA/DOC/4, 12 December 2003 , <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> accessed 29 April 2020.

Reports, working documents, proposals, policies, communications and programmes

1. 137 SE Eelnõu seletuskiri, Seletuskiri rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu juurde (Explanatory Memorandum of Draft Law 137 SE on Money Laundering and Terrorism Financing Prevention Act 2007), <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/046802d9-335d-415b-c4a1-650aa487eb33/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus> accessed 2 May 2020.
2. 232 SE Eelnõu seletuskiri Isikut tõendavate dokumentide seaduse, krediidiasutuste seaduse ning rahapesu ja terrorismi rahastamise tõkestamise seaduse muutmise seaduse juurde (Explanatory Memorandum of Draft law 232 SE on the Act Amending Identification Documents Act, Credit Institutions Act and Money Laundering and Terrorism Financing Prevention Act 2016) // <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/954a096c-722d-4e9a-8000-e292026f8156/Isikut%20t%C3%B5endavate%20dokumentide%20seaduse,%20krediidiasutuste%20seaduse%20ning%20rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seaduse%20muutmise%20seadus>.
3. *A testproject by Lantmäteriet* (The Swedish Mapping, Cadastre and Land Registration Authority), ChromaWay, Landshypotek Bank, SBAB, Telia company and foresight company Kairos Future Report, March 2017, <https://static1.squarespace.com/static/5e26f18cd5824c7138a9118b/t/5e3c35451c2cbb6170caa19e/1581004119677/Blockchain_Landregistry_Report_2017.pdf> accessed 20 October 2020.
4. Center for Media Transition. *The Impact of Digital Platforms on News and Journalistic Content* (2018). <https://www.accc.gov.au/system/files/ACCC%20commissioned%20report%20-%20The%20impact%20of%20digital%20platforms%20on%20news%20and%20journalistic%20content%2C%20Centre%20for%20Media%20Transition%20%282%29.pdf > accessed 22 November 2020
5. Chamber of Notaries. *Notarite Koja arvamus ühinguõiguse revisjoni muudatusettepanekute kohta.* Opinion on the analysis-concept paper of company law revision working group, 17 December 2018, p. 2, <https://www.just.ee/> accessed 12 January 2019.
6. Commission Communication. *A Digital Single Market Strategy for Europe*, 6.5.2015
7. COM(2015) 192, <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final> accessed 20 October 2020.
8. Communication from the Commission, A Digital Single Market Strategy for Europe, COM (2015) 192 final.
9. Communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of the Regions, "Better Regulation for Better Results – An EU Agenda", COM (2015) 215.
10. Commission communication of 2016 as one of the principles to develop the legal framework for online platforms (European Commission, Online Platforms, and the Digital Single Market, Communication, 25.5.2016) COM (2016) 288, p. 5, <https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.PDF> accessed 22 July 2019.

11. EBA. Report with advice for the European Commission, 9 January 2019, p. 7, <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf> accessed 9 December 2019.
12. Ernst & Young Baltic AS. *Study Report SUMMARY OF THE STUDY: "USAGE OF QUALIFIED ELECTRONIC SIGNATURE WITHIN EUROPE UNION"* (2015), p. 2,
13. <https://mkm.ee/sites/default/files/summary_of_the_study_usage_of_qualified_electronic_signature_within_europe_union.pdf> accessed 21 July 2019.
14. EU Blockchain Observatory and Forum. *Legal and regulatory framework of blockchains and smart contracts. A thematic report prepared by the EU Blockchain Observatory and Forum*, 27 September 2019, p. 14, <https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf > accessed 26 January 2020.
15. European Commission. Directorate-General Taxation and Customs Union, VAT Committee (Article 398 of Directive 2006/112/EC), Working Paper No 892, Question concerning the application of EU VAT provisions, Subject: CJEU Case C-264/14: Bitcoin, 4 February 2016.
16. European Commission. Directorate-General Taxation and Customs Union, VAT Committee (Article 398 of Directive 2006/112/EC), Working Paper No 811, Question concerning the application of EU VAT provisions, Subject: VAT treatment of Bitcoin, 23 October 2014, p. 5.
17. European Commission. Commission staff working document Brussels, 26.6.2017 SWD(2017) 241 final PART 2/2 Accompanying the document to Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations {COM(2017) 340 final}, p. 234 <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en>.
18. European Commission. *European Multi Stakeholder Platform on ICT Standardisation*, 7 August 2020, <https://ec.europa.eu/digital-single-market/en/european-multi-stakeholder-platform-ict-standardisation> accessed 3 October 2020.
19. European Commission. *Study on blockchains: legal, governance and legal interoperability aspects* (SMART 2018/0038), A Study prepared for the European Commission DG Communications Networks, Content & Technology by Spark Legal Network, Michèle Finck, Tech4i2, Datarella. Luxembourg: Publications Office of the European Union, 2020, p. 48, <https://media-exp1.licdn.com/dms/document/C4D1FAQFJzr8AaugNJg/feedshare-document-pdf-analyzed/0?e=1582790400&v=beta&t=-SjoR4XelczLwddmhTMffXf9jftdvjhq1QGZ0z2U1dk> accessed 26 February 2020.
20. European Commission. *Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union*, COM (2017) 495, 8.
21. European Commission. *Rolling plan of ICT standardisation*, 5 August 2020, <https://ec.europa.eu/digital-single-market/en/rolling-plan-ict-standardisation> accessed 03 October 2020.

22. European Parliament. *Blockchain for supply chains and international trade. STUDY Panel for the Future of Science and Technology. EPRS*, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE 641.544 – May 2020, p. 66, DOI: <10.2861/957600> or <https://www.europarl.europa.eu/stoa/en/indexsearch?query=supply+chain> accessed 11 October 2020.
23. European Parliament, Policy Department A: Economic and Scientific Policy. *Online Platforms: How to Adapt Regulatory Framework to the Digital Age?* Briefing, 2017, DOI: <10.2861/645636>.
24. European Securities and Markets Authority. *Advice Initial Coin Offerings and Crypto-Assets* (9 January 2019) p.11, <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> accessed 21 July 2017.
25. ESMA. "Initial Coin Offerings and Crypto-Assets." Advice (9 January 2019) https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
26. Explanatory Memorandum for the draft law 148 SE to amend Commercial Code, Notarisation Act and Notary Fees Act (Explanatory Memorandum 148 SE). *Seletuskiri äriseadustiku, tõestamisseaduse ja notari tasu seaduse muutmise seaduse 148 SE eelnõu juurde,* <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/a771f589-ef25-4298-802b-2532822eb4b9/%C3%84riseadustiku%20muutmise%20seadus%20(osa%20v%C3%B5%C3%B5randamine)> accessed 9 May 2020.
27. FATF. FATF *Report: Virtual Currencies Key Definitions and Potential AML/CFT Risks*, June 2014, <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 1 December 2019.
28. FINAL REPORT OF THE COMMITTEE OF WISE MEN ON THE REGULATION OF EUROPEAN SECURITIES MARKETS, Brussels, 15 February 2001 <https://www.esma.europa.eu/sites/default/files/library/2015/11/lamfalussy_report.pdf> accessed 8 March 2021.
29. Government Office For Science (2016). *Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser*, p. 53, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf accessed 19> October 2020.
30. Innovative Technology Arrangements and Services Act (2018) of Malta, ACT No. XXXIII of 2018, <https://mdia.gov.mt/wp-content/uploads/2018/10/ITAS.pdf> accessed 31 May 2020.
31. ITU TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU Focus Group on Application of Distributed Ledger Technology (FG DLT). *Technical Report FG DLT D 2.1. Distributed ledger technology use cases*, 1 August 2019, pp. 21–22, <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf> accessed 20 October 2020.
32. OECD. *Directorate For Financial and Enterprise Affairs Committee on Financial Markets. Draft Recommendation of the Council on Blockchain*, 5 March 2020 p. 9.
33. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the

financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC COM/2016/0450 final – 2016/0208 (COD).
34. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.
35. Proposal HB0185 named Corporate stock-certificate tokens. [online] <www.wyoleg.gov/Legislation/2019/HB0185> accessed 23 January 2019]. 37 Report to the President of the Republic relating to Ordinance No. 2017–1674 of 8 December 2017 on the use of a shared electronic registration device for the representation and transmission of financial securities,
36. Rapport au Président de la République relatif à l'ordonnance n° 2017–1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers. Published in JORF n°0287 du 9 décembre 2017 texte n° 23. [online] <https://www.legifrance.gouv. fr/eli/rapport/2017/12/9/ECOT1729053P/jo/texte> accessed 01 May 2018].
37. Summary of Regulation (EU) No 283/2014 – guidelines for trans-European networks in the area of telecommunications infrastructure titled Supporting telecommunications networks and digital service infrastructures across Europe <https://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32014R0283> accessed 1 March 2021.

Case law and official commentary

CJEU

1. Case C-267/99 *Adam* [2001] ECR I-7467.
2. Case C-419/13 *Art & Allposters International BV v Stichting Pictoright* Request for a preliminary ruling from the Hoge Raad der Nederlanden [2015] ECLI:EU:C:2015:27.
3. Case C-375/11 *Belgacom SA and Others v État belge* [2013] ECLI:EU:C:2013:185.
4. Case C 109/02 *Commission of the European Communities v Federal Republic of Germany* [2003] ECLI:EU:C:2003:586
5. Cases C-509/09 and C-161/10 *eDate Advertising GmbH and Others v X and Société MGN Limited* [2011] ECLI:EU:C:2011:685.
6. Case C-114/12 *European Commission, European Parliament v Council of the European Union* [2014] ECLI:EU:C:2014:224.
7. Case C-479/13 *European Commission v French Republic* ECLI:EU:C:2015:141 [2015],
8. Case C-502/13 *European Commission v Grand Duchy of Luxembourg* [2015]. ECLI:EU:C:2015:143
9. Case C 480/10 *European Commission v Kingdom of Sweden* [2013] ECLI:EU:C:2013:263
10. Case C-461/12 *Granton Advertising BV versus Inspecteur van de Belastingdienst Haaglanden/kantoor Den Haag* [2014] ECLI:EU:C:2014:1745.
11. Case C-455/05 *Velvet & Steel Immobilien* [2007] EU:C:2007:232, par. 16, Case C-189/11 *Commission* v *Spain* [2013] EU:C:2013:587

12. Case C 128-11 *UsedSoft GmbH v Oracle International Corp* [2012] ECLI:EU:C:2012:407.
13. Case C-117/13 *Technische Universität Darmstadt v Eugen Ulmer KG,* 11 September [2014] ECLI:EU:C:2014:2196.
14. Case C-264/14 *Skatteverket V David Hedqvist* [2015] ECLI:EU:C:2015:718.
15. Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECLI:EU:C:2015:498, Opinion of Advocate General Kokott
16. Case C-67/16 P *Comunidad Autónoma de Cataluña, Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI)* [2016].
17. Case C-68/16 P *Navarra de Servicios y Tecnologías SA* [2016].
18. Case C-174/15 *Vereniging Openbare Bibliotheken v Stichting Leenrecht* Request for a preliminary ruling from the Rechtbank Den Haag [2016] ECLI:EU:C:2014:2214 Advocate General's Opinion.
19. Case C-66/16 P to C-69/16 P and Case C-70/16 P and C-81/16 P *Cellnex Telecom SA, formerly Abertis Telecom SA, Retevisión I SA (C69/16 P) v European Commission, SES Astra SA* [2017] ECLI:EU:C:2017:999.
20. Case C-66/16 P *Comunidad Autónoma del País Vasco, Itelazpi SA* [2017] ECLI:EU:C:2017:999.
21. Case C-255/16 *Criminal proceedings against Bent Falbert and Others Request for a preliminary ruling from the Københavns Byret* [2017] ECLI:EU:C:2017:983.
22. Case C-255/16 *Anklagemyndigheden v Bent Falbert, Poul Madsen, JP/Politikens Hus A/S* [2017] ECLI:EU:C:2017:983 Opinion of Advocate General Bobek.
23. Case C-5/16 *Republic of Poland v European Parliament and Council of the European Union* [2018] ECLI:EU:C:2018:483.
24. Case C-263/18 *Nederlands Uitgeversverbond, Groep Algemene Uitgevers v Tom Kabinet Internet BV, Tom Kabinet Holding BV, Tom Kabinet Uitgeverij BV* [2019] ECLI:EU:C:2019:1111.
25. Case C-194/16 *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB.* [2017] ECLI:EU:C:2017:766.
26. Cases C-453/02 and C-462/02 *Finanzamt Gladbeck v Edith Linneweber and Finanzamt Herne-West v Savvas Akritidis*. [2005] ECLI:EU:C:2005:92.
27. Case C-466/12 *Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd v Retriever Sverige AB* [2014] OJ C 379/31.
28. Case C-160/15GS *Media BV v Sanoma Media Netherlands BV and Others.,* Request for a preliminary ruling from the Hoge Raad der Nederlanden (Netherlands) [2015].
29. Case C-306/05 *Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA*. [2006] ECR I-11519.
30. Case C-461/08, *Don Bosco Onroerend Goed*, [2008] EU:C:2009:722.
31. Case C-259/11, *DTZ, Zadelhoff*, [2011] EU:C:2012:423.
32. Case C-326/11, *J.J. Komen en Zonen Beheer Heerhugowaard*, [2011] EU:C:2012:461.
33. Case C 368/10, *Commission v Netherlands*, [2010] EU:C:2012:284.
34. Case C-413/17, *Roche Lietuva' UAB v Kauno Dainavos poliklinika VšĮ*, [2017] EU:C:309:29.

Estonian court case law

1. SCALC judgment, 5th November 2020, case 3-20-718/28.
2. SCALC judgment, 4th November 2020, case 3-20-924/24.
3. SCALC judgment, 6th March 2014, case 3-3-1-13-12.
4. SCALC judgment 12th October 2011, case 3-3-1-31-11.
5. SCALC judgment, 27th October 2010, case 3-3-1-66-10.
6. SCALC judgment, 11th April 2016, case 3-3-1-75-15.
7. Estonian Supreme Court Civil Law Chamber (SCCLC) judgment, 22nd February 2012, case no 3-2-1-163-11 (2012).
8. SCCLC judgment, 14th December 2011, case no 3-2-1-133-11.
9. Estonian Supreme Court Constitutional Review Chamber (SCCRC) judgment, 6th July 2012, case no 3-4-1-3-12.
10. SCCLC judgment, 28th January 2015, case no 3-2-1-141-14.
11. SCALC judgment, 17th February 2003, case no 3-4-1-1-03.
12. SCCLC judgment, 14th December 2011, case no 3-2-1-133-11.
13. SCCLC judgment, 28th January 2015, case no 3-2-1-141-14.

Electronic resources

1. Allison, I. Smart securities issuer Symbiont fires shots in the private blockchain arms race. International Business Times, 28 September 2015. <https://www.ibtimes.co.uk/smart-securities-issuer-symbiont-fires-shots-private-blockchain-arms-race-1521449> accessed 08 May 2018].
2. Authcoin website: <https://authcoin.com/>.
3. BTC.ee site: http://btc.ee/appeal.html accessed 02 May 2020.
4. Civic KYC service page: https://www.civic.com/solutions/kyc-services/ accessed: 25 July 2019.
5. Clifford Chance (2017). France pioneers blockchain legal framework for unlisted
6. Securities, Briefing Note. [online] <https://www.cliffordchance.com/content/dam/cliffordchance/PDFDocuments/Client%20Briefing%20-%20France%20-%20Blockchain%20for%20unlisted%20securities%20180750-4-2....pdf> accessed 08 May 2018].
7. David John Harvey is a former district court judge from Auckland, New Zealand and currently serves as a director of the New Zealand Center for ICT Law and lecturers on Law and Information Technology at the University of Auckland, see more here https://www.bloomsburyprofessional.com/author/david-j-harvey/ accessed 19 April 2020.
8. European Commission. Call for tender page. Tender press release 12 December 2018. <https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects> accessed 06 November 2020
9. Finance Estonia, *Ühisrahastuse platvormid muutuvad läbipaistvamaks.* <http://www.financeestonia.eu/news/uhisrahastuse-platvormid-muutuvad-labipaistvamaks/ accessed 4 April 2020.

10. Financial Supervisory Authority, *Virtuaalraha pakkujad ei kuulu järelevalve alla* (Providers of virtual currency do not fall under supervision), Website of Financial Supervisory Authority (05 February 2014). Website of Financial Supervisory Authority (05 February 2014). <http://www.fi.ee/index.php?id=21561> accessed 2 May 2020.
11. FINMA page, <https://www.finma.ch/en/authorisation/self-regulatory-organisations-sros/> accessed 4 April 2020.
12. Encyclopaedia Britannica, <https://www.britannica.com/topic/cyberspace>.
13. Ethereum website: <https://www.ethereum.org/terms-of-use/> accessed 1 May 2019.
14. Ethereum website <https://ethereum.org/en/> 30 September 2020.
15. 'Euroopa Kohus: bitcoinidega kauplemine on maksuvaba' [*European Court: trading with bitcoins is tax free*]. Äripäev.ee (23 October 2015) <https://www.aripaev.ee/uudised/2015/10/23/euroopa-kohus-bitcoinidega-kauplemine-on-maksuvaba>
16. European Union Agency for Cybersecurity, *Glossary*, <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/public-key-infrastructure-pki> accessed 10 May 2020.
17. European Union Agency for Cybersecurity, *Glossary*, <https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/public-key-infrastructure-pki> accessed 10 May 2020.
18. HM Treasury. *A new regulator for the new millennium*, 1 June 1998, <https://webarchive.nationalarchives.gov.uk/20100512163629/http://www.hm-treasury.gov.uk/press_84_98.htm> accessed 29 April 2020.
19. ISO 22739:2020 Blockchain and distributed ledger technologies – Vocabulary, ISO/TR 23244:2020 Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations and ISO/TR 23455:2019 Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems. Available on Standards by ISO/TC 307 website: https://www.iso.org/committee/6266604/x/catalogue/p/1/u/0/w/0/d/0 October 2020].
20. Lätt, Priit. "Complaint of de Voogd's representative" (21 April 2014) // <http://btc.ee/documents.html>.
21. MyCrypto support page, <https://support.mycrypto.com/how-to/getting-started/how-to-create-a-wallet> accessed 9 July 2019.
22. Polyswarm. *Blockchain in Cyber Security: Who is Who.* 10 January 2018, <https://medium.com/polyswarm/blockchain-in-cyber-security-who-is-who-269d89feadc1> accessed 10 July 2019.
23. PwC. *PwC's Global Blockchain Survey 2018*, <https://www.pwc.com/gx/en/industries/technology/blockchain/blockchain-in-business.html and https://www.pwccn.com/en/research-and-insights/publications/global-blockchain-survey-2018/global-blockchain-survey-2018-report.pdf>.
24. SEC. *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities* (U.S. Securities and Exchange Commission Press Release, 25 July, 2017), <https://www.sec.gov/news/press-release/2017-131 accessed 01 December 2019.
25. See more at IEEE Blockchain site <https://blockchain.ieee.org/> accessed 03 October 2020.

26. See more on the relevant International Telecommunication Union (ITU), <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx> accessed 03 October 2020.
27. Speech delivered by Vice President of the European Commission Neelie Kroes at the European Commission and European Parliament Summit on "The Open Internet and Net Neutrality in Europe" in Brussels, 11 November 2010, <https://ec.europa.eu/digital-single-market/en/news/net-neutrality-%E2%80%93-way-forward> accessed 9 May 2020.
28. Terms and Conditions of the Ethereum Genesis Sale, 21 July 2014, <https://web.archive.org/web/20140723212709/https://www.ethereum.org/pdfs/TermsAndConditionsOfTheEthereumGenesisSale.pdf> accessed 1 May 2019.
29. Tezos KYC procedure, <https://www.civic.com/blog/4-key-takeaways-decentralized-kyc-for-icos-and-token-sales/> accessed 24 July 2019.
30. Trusted List Browser under eIDAS, <https://webgate.ec.europa.eu/tl-browser/#/> accessed 10 May 2020.
31. UNIDROIT Commercial Contracts' Principles, <https://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2016> accessed 23 July 2018.
32. U.S. Securities and Exchange Commission SRO page for such commenting rounds, <https://www.sec.gov/rules/sro.shtml>.
33. U.S. Securities and Exchange Commission. *SEC Orders Blockchain Company to Pay $24 Million Penalty for Unregistered ICO* (Press Release September 30, 2019), <https://www.sec.gov/news/press-release/2019-202> accessed 01 December 2019. <https://www.fbo.gov/index?s=opportunity&mode=form&id=c18a03f93cf06df47dab8a1c1a7f87a9&tab=core&_cview=0> accessed 8 July 2019.
34. German Ministry of Finance site: <https://www.bundesfinanzministerium.de/Content/EN/Pressemitteilungen/2019/2019-18-09-joint-release-with-bmwi.html> accessed 26 December 2020.
35. The Ministry of Finance site of the new law on electronic securities, 'Gesetz zur Einführung von elektronischen Wertpapieren' [*Law on the introduction of electronic securities*] <https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2020/12/2020-12-16-gesetz-zur-einfuehrung-von-elektronischen-wertpapieren.html> accessed 26 December 2020.

ACKNOWLEDGEMENTS

I am thankful for this experience, this challenge I took on upon the invitation of the first director of the IT Law Master's Programme Helen Eenmaa-Dimitrieva to apply to the IT law specific doctoral programme. It has been a privilege to take on a fast-developing subject related to technology and explore it from the point of view of law. I am forever grateful to my supervisors: Associate Professor Martin Ebers and previous supervisor Professor Jaan Ginter from the University of Tartu and Dr Anna-Maria Osula and Associate Professor Alex Norta from TalTech. I could not have finished this dissertation without your invaluable support, belief in me and honest but constructive feedback. I also thank Associate Professor Marta Cantero Gamito from the University of Tartu for being a great inspiration to me and PhD Programme Director Merike Ristikivi and assistant Katri Holst for support in the PhD Programme.

I am particularly indebted to my fellow PhD students who participated in the same PhD program at the University of Tartu: Kärt Pormeister, Liliia Oprysk, Taivo Liivak, Kristjan Kikerpill and Tõnu Mets. Thank you for leading by example, being there during the difficult times and finding your own path in this struggle.

I was fortunate enough to have the opportunity to research part of my dissertation as a visiting researcher at welcoming universities. I thank University College London along with Professor of Computing and Director of the Financial Computing Centre Philip Treleaven and Vice Dean of Innovation for the Faculty of Laws Anna Donovan, but most of all visiting researcher at Imperial College Centre for Cryptocurrency Research and Engineering Catherine Mulligan for the invitation. My sincere appreciation also goes to the Swedish Law and Informatics Research Institute of the University of Stockholm for making me feel at home in the historical place where many have struggled with similar research on a topic intersecting law and IT. During my visit, several discussions over lunch were granted to me by Professor Peter Wahlgren out of his vacation period that shaped much of my approach to my research topic and choice of methods. Thank you also to Cyril Holm for all the administrative support during my visit. I also thank Archimedes and the University of Tartu for the resources to go on these visits.

During my doctoral studies, I crossed paths and had the pleasure to discuss my research with many inspiring people. I would like to thank the inspirational scholars and scientists Primavera de Filippi and Lawrence Lessig for all your books and articles and for that one day in Berlin where I got to meet you and share my thoughts with you. I am forever indebted to fellow PhD candidate Florian Glatz from the University of Bayreuth and my colleague Eduardo da Cruz Rodrigues e Silva for always finding the time to discuss, read and assist me in all topics related to blockchain and law. Furthermore, my fellow legal hackers Jameson Dempsey, Steven Nam, Risto Hübner, Nikolay (Mykola) Demchuk and Evert Nõlv – thank you for being with me on this journey into an interdisciplinary domain.

I thank also the inspiring staff of the writing retreats of MIDOK – Djuddah Arthur Joost Leijen, Anni Jürine and organizer Katrin Tamm – and am thankful for the invaluable courage and confidence boost from Professor Andra Siibak from the Institute of Social Studies at the University of Tartu. Special gratitude goes to Djuddah Arthur Joost Leijen for the Zoom writing sessions during the first corona lockdown organized in spring 2020.

I would not have been successful in this struggle without the support of my husband, my kids, my colleagues and clients, who granted me these moments to work on my research. Not to mention my mentors Signe Viimsalu (Dr iur. of the University of Tartu) for always believing in me and being there for the last mile; Lorraine Weekes (PhD of Stanford University) for inspiring me and Associate Professor Innar Liiv from TalTech for inviting me to Berlin to meet my heroes and lending an ear during the tougher times.

Lastly, I thank Aaron Swartz, the 'Internet's Own Boy', who fought for the liberation of knowledge and Satoshi Nakamoto, whoever (s)he is for introducing the revolutionary technology.

SUMMARY IN ESTONIAN

Hajusraamatutehnoloogia kasutuselevõtu õiguslikud takistused: tehnoloogia neutraalsuse ja funktsionaalse samaväärsuse põhimõtetele tuginev analüüs

Väitekirja uurimisese on hajusraamatutehnoloogia (*distributed ledger technology*), sh plokiahelatehnoloogia (*blockchain technology*) kasutamisel esinevad õiguslikud takistused, mis tulenevad õigusraamistikku sisse kirjutatud taristuslikest eelarvamustest. Viidatud eelarvamusi ning nendega seotud tagajärgi uuritakse väitekirjas tehnoloogianeutraalsuse põhimõtte ja funktsionaalse samaväärsuse alampõhimõtte alusel. Kuigi need põhimõtted on olulised laiemas tehnoloogia reguleerimise kontekstis, mitte pelgalt hajusraamatutehnoloogia kasutamisel, piirdutakse väitekirjas põhimõtete kohaldamisega autori poolt valitud hajusraamatutehnoloogia konkreetsetel kasutusjuhtudel kohalduvatele õigusnormidele. Olukorras, kus ilmneb õigusnormi mittevastavus tehnoloogianeutraalsuse põhimõttele, uurib autor selle mittevastavuse põhjuseid ja tagajärgi ning püüab leida mittevastavusele lahendusi kasutades tehnoloogianeutraalsuse alampõhimõtte – funktsionaalse samaväärsuse – abi.

Hajusraamatutehnoloogia all peetakse silmas andmestruktuuri, mis kajastab algoritmis sätestatud loogika kohaselt kodeeritud arvestusraamatu (*ledger*) andmetest, mida saab vahetada ja millel võib olla õiguslik tähendus. Andmete terviklikkust kaitseb iteratiivne räsimine (*hashing*). Räside endi terviklikkust kaitsevad krüptograafia (*cryptography*) ja ajatembeldus (*timestamping*) funktsioonid. Kõige tuntum hajusraamatutehnoloogia andmestruktuur on plokiahel, mida kasutatakse ka krüptoraha (*cryptocurrency*) andmestruktuurides. Sellistes andmestruktuurides esitab arvestusraamat krüptoraha kasutajate rahakottide kohta andmeid ning nende rahakottide vahelisi makseid ühikutes, mis on käibel arvestusraamatu oma taristu sees ja enamasti võimaldab teha vahetustehinguid ka andmestruktuuriga seotud turgudel. Kõige tuntum krüptoraha on tänini bitimünt (*bitcoin*) ja sellest väiksem sama vääringu ühik *satoshi* (sajamiljondik bitimündist). Plokiahela andmestruktuuri iseloomustab see, et andmestruktuur koosneb andmeplokkidest ja iga järgnev andmeplokk on räsi kaudu eelneva andmeplokiga ühenduses. Arvestusraamatuid hoitakse hajusraamatutehnoloogia puhul (nagu ka selle nimetus ütleb) hajutatult, s.t ei ole nii, et on üks arvestusraamatu originaal ja teised vaid koopiad, vaid mitu osalist hoiab arvestusraamatu identset originaali algoritmi sissekirjutatud konsensusprotokolli alusel, mille põhjal lepivad hajusraamatu kasutajad (kes üksteist enamasti ei tunne) kokku, mis on arvestusraamatusse tehtud kannete tegelik seis. Kuna plokiahel on vaid üks hajusraamatutehnoloogia andmestruktuure, käsitletakse väitekirjas plokiahela andmestruktuuri kui näidet, mis ilmestab õigusraamistikust tulenevaid takistusi sh normidesse sissekirjutatud eelarvamusi hajusraamatutehnoloogia kasutusele võtmisele.

Transformatiivne ehk murranguline innovatsioon mõjutab eri ühiskonnakihte ning kuna hajusraamatutehnoloogiat peetakse just selliseks transformatiivseks

ehk murranguliseks innovatsiooniks, mis mõjutab ühiskonda suureulatuslikult ja selle mõju ühiskonnas on mitmedimensiooniline. Kuigi finantsteenused (sh krüptoraha) on hajusraamatutehnoloogia üks levinumaid rakendusi, seisneb hajusraamatutehnoloogia murrangulisus asjaolus, et sellel tehnoloogial võib olla palju laiem mõju kui vaid finantssektoris, näiteks valdkondades nagu isikusamasuse haldamine, turvalisuse haldamine ja andmete haldamine. Hajusraamatutehnoloogia murrangulist mõju saab täheldada mitmes sektoris ning selle rakendused on kasutusel lisaks finantssektori rakendustele ka rahvusvahelises kaubanduses, väärtpaberitehingute talletamises ja kajastamises, ravimite väljakirjutamises ja selle protsessi seires, organidoonorluse seires, energiaressursside jaotuses ja ümberjaotuses ning igasuguste andmete talletamises ja vahetamises paljudes sektorites, nagu tarneahela juhtimine, tervishoid, avalikud teenused, intellektuaalomandiõiguste haldus, e-kaubandus, jms. Kuna hajusraamatutehnoloogia on üldotstarbeline tehnoloogia, millel on hulk võimalikke rakendusi ja väljundeid ning mida saab kasutada eri teenuste osutamisel ja protsesside rakendamisel, prognoositakse, et hajusraamatutehnoloogia mõju äritegevusele ja ühiskonnale suureneb ajas oluliselt. Sellist järeldust toetab ka septembris 2020.a. avaldatud EL-i digitaalse finantspaketi projekt, mille eesmärk on tehnoloogianeutraalselt toetada hajusraamatutehnoloogia kasutuselevõttu EL-is finantssektoris krüptovarade reguleerimise kaudu.

Õigusraamistikku sissekirjutatud taristuslike eelarvamuste uurimisel tuleb arvestada ka tempoprobleemi (*pacing problem*), mis tähendab seda, et tehnoloogia ja selle kasutuspraktika muutuvad ajas kiiresti ning eksponentsiaalselt, kuid õigusraamistik samas muutub vähehaaval ning aeglaselt. Lisaks tuleb arvesse võtta ka Collingridge'i dilemmat, mille kohaselt tunneb seadusandja vajadust sekkuda iga uue tehnoloogia saabumisega tekkinud mõjudesse üsna varakult, olgugi et uue tehnoloogia kasutuselevõtu tagajärjed on tihti veel varajases etapis ning seega üpris ebaselged. Sekkumise põhjus on tihtipeale hirm, et selleks ajaks, kui kasutuselevõtu mõju ja tagajärjed on selged, on tehnoloogia sageli nii olulisel määral osa majandusest või ühiskonnast, et seda on raske ohjata. Seega on Collingridge'i dilemma kohaselt lihtsam kehtestada uued õigusnormid pigem võimalikult varakult – ajal, mil tehnoloogia ei ole veel täielikult välja kujunenud. Samas kuna uue regulatsiooni mõju on varakult sekkudes veel arenemata tehnoloogia osas ebaselge võivad uued õigusnormid osutuda tehnoloogia laiemale kasutuselevõtule piiravaks või hukatuslikuks.

Oluline on tuvastada õigusraamistikku sissekirjutatud taristuslikud eelarvamused hajusraamatutehnoloogia osas ka põhjusel, et Euroopa Komisjoni endise presidendi Junckeri sõnul on ühtse digitaalse turu loomisel vaja luua võrdsed võimalused nii turgu valitsevatele ettevõtjatele kui ka tehnoloogia, taristu, kasutusjuhtude uuendajatele, kehtestades võrdsed mängureeglid kõigele, mis on digitaalne. Sarnane soov väljendub ka EL-i 2020. a septembris avaldatud digitaalse finantspaketi projektidokumentides, mille eesmärk on kooskõlas tehnoloogianeutraalsuse põhimõttega toetada hajusraamatutehnoloogia kasutuselevõttu EL-is ning autori arvates ka kõrvaldada olemasolevasse finantsturge puudutavasse õigusraamistikku sissekirjutatud taristust lähtuvad eelarvamused. Paraku püüel-

dakse võrdsete mängureeglite kehtestamise eesmärgi poole sageli viisil, mis on ajendatud hirmust, et murranguline innovatsioon tekitab juba olemasoleval ja toimival turul kaose ja ebaselguse. Sel põhjusel on seadusandja tihti motiveeritud allutama turul asetleidvad uuendused olemasolevatele õigusnormidele ilma norme uuenenud tehnoloogilisele lahendusele kohandamata. Seda isegi juhul, kui innovatsioon selle tegevuse tulemusel kannatab.

Väitekirja üldine eesmärk on välja selgitada, kas Eesti ja Euroopa Liidu õigus, mida kohaldatakse või kohaldati autori poolt välja valitud konkreetsetel hajusraamatutehnoloogia kasutusjuhtudel, on tehnoloogianeutraalne. Kui konkreetsel juhul kohalduv õigus ei vasta tehnoloogianeutraalsuse põhimõttele, uurib autor, mis ulatuses ja kuidas on vaja õigusraamistikku muuta, et saavutada tehnoloogianeutraalsus. Et saavutada väitekirja üldine eesmärk, püstitas autor alltoodud uurimisküsimused:

1. Kuidas tuvastada olemasolevatesse õigusnormidesse sisse kirjutatud eelarvamused hajusraamatutehnoloogia suhtes?
2. Kuidas jätkusuutlikult tagada õigusnormide tehnoloogianeutraalsus hajusraamatutehnoloogia suhtes?
3. Kas autori poolt valitud hajusraamatutehnoloogia kasutusjuhtudele kohaldatavad õigusnormid on kooskõlas tehnoloogianeutraalsuse põhimõttega või sisaldab eelarvamusi hajusraamatutehnoloogia suhtes? Täpsemad uurimisküsimused iga hajusraamatutehnoloogia kasutusjuhu kohta on järgnevad:

    a) Kas rahapesutõkestamise regulatsioon Eestis ja selle rakendamine olid bitimündi ja selle kauplejate suhtes tehnoloogianeutraalsed (*de Voogd* näitel) nagu käibemaksu regulatsiooni rakendamine bitimündi ja selle kauplejate osas EL-is (*Hedqvist*'i näitel)?
    b) Kas Eesti äriseadustiku alusel osaühingu osanike nimekirja pidamine juhatuse poolt võimaldab seda pidada hajusraamatutehnoloogia baasil funktsionaalselt samaväärsena keskregistri poolt peetava nimekirjaga ja kas seadus tagab sellisele osanike nimekirja pidamisele tehnoloogianeutraalsuse põhimõttest lähtuvalt võrdse kohtlemise?
    c) Kas hajusraamatutehnoloogial põhinevat allkirja targal lepingul saab lugeda funktsionaalselt samaväärseks eIDAS-e kvalifitseeritud elektroonilise allkirjaga ning kas eIDAS võimaldab seda allkirja tehnoloogianeutraalsuse põhimõttest lähtuvalt võrdselt kohelda PKI mudelil põhineva allkirjaga?

Autori poolt valitud hajusraamatutehnoloogia kasutusjuhud illustreerivad erinevaid viise, kuidas õigusnormid võivad mõjuda hajusraamatutehnoloogia kasutusele diskrimineerivalt. Näited annavad tunnistust sellest, et kehtiv õigus on mitmeti tehnoloogiliselt erapoolik või konkreetse taristu keskne. Eespool toodud uurimisküsimusi käsitletakse lisaks käesolevas väitekirjas toodule ka alljärgnevas neljas õigusteadusartiklis, mille on avaldanud autor või autor koos kaasautoritega:

- Artikkel I: „Decentralised technology and technology neutrality in legal rules: an analysis of De Voogd and Hedqvist“, milles analüüsitakse bitimündile kui maksevahendile ja bitimündiga kauplejale kohaldatavaid õigusnorme Eesti rahapesutõkestamise seaduse ja Euroopa käibemaksu regulatsiooni alusel. Artiklis uuritakse, kas tehnoloogianeutraalsuse põhimõte sobib tsentraalsel-detsentraalsel skaalal tekkiva diskrimineerimise lahendamiseks sarnaselt tehnoloogianeutraalsuse põhimõtte rakendamisega füüsilise ja digimaailma (*offline-online*) reguleerimise vastuolude puhul. Artiklis käsitletakse kahte kohtuasja, millest üht lahendas Eesti Vabariigi Riigikohus (de Voogd) ja teises võttis seisukoha Euroopa Liidu Kohus (Hedqvist). Seejuures võrreldakse kohtuasjade pinnal kahte eri lähenemisviisi bitimüntidele ja nendega kauplemisele olemasolevate õigusnormide alusel. Võrdluse põhjal uurib autor, kas õigusraamistik ja selle rakendamine Eestis oli tehnoloogianeutraalne või sisaldas regulatsioon ja selle kohaldamine taristupõhiseid eelarvamusi. Artiklis antakse ka põgus ülevaade tehnoloogianeutraalsuse põhimõttest.
- Artikkel II: „Shareholder ledger using distributed ledger technology: the Estonian perspective“, milles analüüsitakse hajusraamatutehnoloogia kasutamist osanike nimekirja pidamisel Eesti õiguse näitel. Analüüsi fookuses on küsimus, kas osanike nimekirja pidamisele kohaldatavad õigusnormid vastavad tehnoloogianeutraalsuse põhimõttele. Autor analüüsib, kas olemasolev õigusraamistik annab eeliseid osanike nimekirja pidamisele tsentraliseeritud taristu (väärtpaberite keskregister) poolt ning seega kas kohalduvad õigusnormid sisaldavad eelarvamusi detsentraliseeritud innovaatiliste tehnoloogiliste lahenduste (nt hajusraamatutehnoloogia) kasutuse vastu osanike nimekirja pidamise, mis suudab keskregistriga funktsionaalselt samaväärselt nimekirja käitada ilma keskse vahendajata.
- Artikkel III: „Hybrid smart contract challenge to European electronic signature regulation“ (kaasautorid Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva ja Alex Norta), milles uuritakse Eesti ja EL-i õiguse näitel, kas määrus 910/2014 (eIDAS) võimaldab hajusraamatutehnoloogial põhinevat hübriidset tarka lepingut, mida kasutatakse müntide esmaemissioonil (Initial Coin Offering (ICO)), lugeda sellele lisatud e-allkirja alusel elektroonilises vormis sõlmitud lepinguks. Artiklis nimetatakse tarka lepingut hübriidseks targaks lepinguks põhjusel, et selle moodustavad eri komponendid, mis ei koosne üksnes koodist, vaid ka lepingu kasutajatele mõeldud kirjalikust tekstist. Artikli keskmes on eIDAS-e vastavuse analüüs tehnoloogianeutraalsuse põhimõttele hajusraamatutehnoloogia baasil sõlmitud lepingute kasutusjuhu puhul. Lisaks analüüsitakse artiklis funktsionaalse samaväärsuse alampõhimõtte alusel, kas hübriidse targa lepingu allkiri kvalifitseeruks funktsionaalselt samaväärseks eIDAS-e kvalifitseeritud e-allkirjaga isegi juhul, kui see ei vasta kõigile sellise allkirja vorminõuetele, kuid täidab nende nõuete eesmärke.
- Artikkel IV: „Functional equivalence – an exploration through shortcomings to solutions“, milles uuritakse tehnoloogianeutraalsuse ja funktsionaalse

samaväärsuse põhimõtete alusel hajusraamatutehnoloogianeutraalse regulatsiooni kujundamisalternatiive, et lahendada eelnevates artiklites toodud näidete alusel tuvastatud tsentraliseeritud taristu eelistamisest tulenevat diskrimineerimist detsentraliseeritud ja hajustehnoloogiatel põhinevate rakenduste vastu. Artiklis analüüsitakse üksikasjalikumalt funktsionaalse samaväärsuse alampõhimõtet ning selle kasutamist EL-i õiguse tõlgendamisel ja kohandamisel. Artiklis uuritakse funktsionaalse samaväärsuse alampõhimõttele tuginevat regulatsioonimudelit võttes eeskujuks isikuandmete kaitse üldmääruses (GDPR) kasutatud „lõimitud andmekaitse reguleerimismudel". Viimane pigem kirjeldab oma regulatsioonis väärtusi ja eesmärke, selle asemel et keskenduda konkreetsele tehnilisele või korralduslikule taristukesksele lahendusele ning seeläbi diskrimineerides kõiki teisi alternatiivseid lahendusi.

Väitekirjas kasutatavad uurimismeetodid koosnevad õiguse uurimise meetoditest ja proaktiivsest meetodist, mille aluseks on Peter Seipeli pakutud lähenemisviisid infotehnoloogiaõigusele. Õiguse uurimise meetoditest kasutatakse esiteks kvalitatiivset süsteemse analüüsi meetodit, et kaardistada tehnoloogianeutraalsuse põhimõtte ja funktsionaalse samaväärsuse alampõhimõtte sisu ja ulatus, võttes aluseks õigusaktid, kohtupraktika, õigusteooria ning muud teisesed allikad. Teiseks kasutatakse õigusdogmaatikat, et uurida positiivset õigust, tuvastamaks olemasolevad õigusnormid, mis kohalduvad valitud hajusraamatutehnoloogia kasutusjuhtudele. Dogmaatilist meetodit kombineeritakse kirjeldava (väline perspektiiv), hermeneutilise ja normatiivse (sisemine perspektiiv) uurimusega, s.t autor mitte üksnes ei kirjelda positiivset õigust, vaid tõlgendab selle teksti ning hindab seda. Ehkki autor ei kasuta väitekirjas võrdlevat meetodit, kasutab ta võrdlusi kui meetodit, võrreldes eri jurisdiktsioonide kohtupraktikat ja esitades mitmete jurisdiktsioonide õigusnorme, mille fookus on reguleerida hajusraamatutehnoloogia kasutamist.

Kuna hajusraamatutehnoloogia on uus ja arenev tehnoloogia, kasutatakse väitekirjas ka proaktiivset uurimismetoodikat uurimaks infotehnoloogiaõigusele omaselt takistusi klastrikeskselt ja kohaldades Peter Seipel'i eriteooria lähenemisviisi. Klastrikeskne lähenemisviis võimaldab uurimuses süveneda vaid nendesse aspektidesse, mis tulenevad vaid konkreetse tehnoloogia kasutusjuhu puhul kohalduvast õigusest. Lähenemisviisi raames analüüsitakse eri õigusinstrumente, et tuvastada kasutusjuhule kohalduvad õigusnormid ning seejärel lahendada õigusnormide kohaldamisest tulenev tehnoloogia kasutusega seotud probleem, mis käesolevas väitekirjas on väljendatud õigusnormi sissekirjutatud eelarvamusena hajusraamatutehnoloogia vastu. Seipel leiab, et viidatud lähenemisviis on funktsionaalne ning selle eesmärk on tuvastada õigusnormide lüngad ja puudused, pidades silmas konkreetset tehnoloogia kasutusjuhtu. Hajusraamatutehnoloogia konkreetsed kasutusjuhud määretlevad probleemide klastri, mis võib hõlmata nii regulatsiooni lünki, sissekirjutatud eelarvamusi kui ka puudusi, mis takistavad fookuses oleva tehnoloogia kasutuselevõttu.

Lõpetuseks käsitletakse klastri osas eriteooriale tuginevat lähenemisviisi. Sellesse käsitlusse kuuluvad teemad nõuavad õigusnormide ja nn. tööriistade ehk tehnoloogia kokkupuutepunktide analüüse ning see lähenemisviis ei rahuldu pelgalt olemasolevate õigusnormide analüüsiga, vaid nõuab ka nn. Tööriistade ehk tehnoloogia enda uurimist (inglise keeles „tools“ ehk tehnoloogiat ennast, jne). Autor kasutab eriteooria lähenemisviisi funktsionaalse samaväärsuse alampõhimõtte rakendamiseks hajusraamatutehnoloogia kasutusjuhtudele. Eriteooria lähenemisviis hõlmab hajusraamatutehnoloogia funktsioonide analüüsi koos õigusnormidest tulenevate tööriista-kesksete nõuete analüüsiga. Selle analüüsi eesmärk on püüda mõista, kas hajusraamatutehnoloogia täidab või on suuteline täitma õigusnormides püstitatud eesmärke nii õigusnormides toodud tehnoloogiakeskseid vorminõudeid täites või neid vorminõudeid täitmata. Seega kontrollib autor eriteooriale tugineva lähenemisviisi rakendamise abil hajusraamatutehnoloogial põhineva lahenduse funktsionaalset samaväärsust õigusnormi loomisel arvestatud ja õigusnormides väljendatud tööriistakeskse lahenduse eesmärkide ning vorminõuetega. Selleks süveneb autor väitekirjas konkreetsel kasutusjuhul kohalduvate õigusnormidega kehtestatud nõuete eesmärkidesse ja kehtestatud vorminõuete põhjustesse. Eriteooriale tuginev lähenemisviis võimaldab tuvastada kohalduvates õigusaktides sisalduvad taristulikud eelarvamused olemasoleva lahenduse suhtes ning seda seetõttu ka eelistades. Selline tagajärg aga ei ole kooskõlas tehnoloogianeutraalsuse põhimõttega.

Väitekirjas kasutatavad peamised allikad olid tehnoloogianeutraalsuse põhimõtte kaardistamisel EL-i õiguse pinnal raamdirektiiv, NIS, isikuandmete kaitse üldmäärus, eIDAS ja EL-i uus digitaalse finantspaketi projekt koos EL-i kohtupraktika ning õigusteadusteostega. Sama põhimõtte kaardistamisel Eesti õiguse pinnal oli primaarne allikas elektroonilise side seadus. Lisaks dogmaatilise õigusalase uurimuse allikatena kasutas autor hajusraamatutehnoloogia kasutusjuhtude keskseid kohalduvaid õigusnormikogumeid nii era- kui ka avalike õigusallikate hulgast. Näiteks bitimüntide kasutusjuhuga seoses uuritakse käibemaksu ja rahapesu tõkestamist puudutavaid õigusnorme rahapesu ja terrorismi rahastamise tõkestamise seaduse, rahapesu tõkestamise 5. direktiivi ja käibemaksudirektiivi alusel. Osanike nimekirja kasutusjuhuga seoses uuritakse ühinguõigust, eelkõige Eesti Vabariigi äriseadustikku. Protokollipõhiste tarkade hübriidlepingute kasutusjuhuga seoses uuritakse primaarselt elektroonilist allkirja reguleerivaid õigusnorme eIDAS-e alusel.

Käesolevaga esitab autor kokkuvõtte uurimisprobleemidest ja väitekirjas toodud analüüsi pinnal tehtud järeldustest.

1. Kuidas tuvastada olemasolevatesse õigusnormidesse sissekirjutatud eelarvamused hajusraamatutehnoloogia suhtes?

Digimaailma loomisel tuvastas seadusandja võimaliku diskrimineerimisohu seoses digivormiga. Nimelt selgus, et digivormi koheldi ebavõrdselt võrreldes tollal harjumuspärase analoogvormiga, kuna digivormi suhtes oldi eelarvamustega,

mida kajastas ka regulatsioon. Selleks, et maandada nimetatud ebavõrdse kohtlemise riski ja eelarvamusi, peeti vajalikuks võtta kasutusele tehnoloogianeutraalsuse põhimõte, mille eesmärk oli neutraliseerida analoogmaailma eelistamine riigivõimu poolt ning tagada digivormi võrdne kohtlemine regulatsiooni kaudu. Sellest kasvas välja üldine tehnoloogianeutraalsuse põhimõte.

1.1. Tehnoloogianeutraalsuse põhimõte

Arvestades tehnoloogianeutraalsuse põhimõtte eesmärki, on selle põhimõtte kohaldamine hajusraamatutehnoloogia kontekstis sama asjakohane kui transformatiivse innovatsiooni kontekstis, mille tingisid digimaailm ja interneti kasutuselevõtt. Sarnane diskrimineerimisoht peitub ka hajusraamatutehnoloogia kasutuselevõtu puhul. Et selle ohuga tegeleda ja võtta kasutusele ohtu minimeerivad meetmed, on esmalt vaja tuvastada asjaolud, mille tulemusena tekivad takistused innovatsioonile, ning seetõttu tuleb luua tingimused, mis maandavad tehnoloogia kasutuselevõttu takistavaid tegureid. Seega peab hajusraamatutehnoloogia põhjustatud transformatiivse innovatsiooni tõttu kontrollima olemasolevaid õigusnorme tehnoloogianeutraalsuse põhimõtte alusel, et tuvastada, kas kehtiv õigus sisaldab eelarvamusi ja diskrimineerib hajusraamatutehnoloogiat.

Tehnoloogianeutraalsus on põhimõte, mida peetakse info- ja kommunikatsioonitehnoloogiaõiguse (IKT-õiguse) ning ka tänapäevasema infotehnoloogiaõiguse (IT-õiguse) lähtepunktiks. Tehnoloogianeutraalsuse põhimõtte eesmärk on kaitsta innovatsiooni ja konkurentsi. Tehnoloogianeutraalsuse põhimõte sarnaneb paljuski soolise ja rassilise neutraalsuse põhimõttega ning selle eesmärk on tagada ühtlasi iga uue tehnoloogiaga arvestamine. Arvestamine väljendub siinkohal pigem selles, et seadusandja ei eelista ühtegi varasemat tehnoloogiat, võimaldades tehnoloogia kasutajal vabalt valida tehnoloogia ega diskrimineeri ühegi konkreetse tehnoloogia kasutust.

See põhimõte pärineb 1990-ndatest ning on esindatud EL-i telekommunikatsiooni direktiivides, nagu raamdirektiiv, juurdepääsu direktiiv, loadirektiiv, parema õigusloome direktiiv ja NIS-i direktiiv. Samas on põhimõtte eesmärk, kohelda erinevaid intellektuaalomandiõiguse väljendusvorme võrdselt, väljendatud ka InfoSoc direktiivis ja tarkvaradirektiivis ning elektroonilise lepinguvormi diskrimineerimiskeeld on väljendatud ka elektroonilise kaubanduse direktiivis. Nii põhimõte kui ka funktsionaalse samaväärsuse alampõhimõte on äratuntavad ka riigihanke direktiivi põhjenduses 74 ning sama direktiivi võrdse kohtlemise, mittediskrimineerimise ja läbipaistvuse põhimõtetes – see on arusaadav, sest mingi konkreetse tehnoloogia eelistamise keeld riigihankemenetluses on kooskõlas tehnoloogianeutraalsuse põhimõttega. Väitekirjas esitatud analüüs näitas, et põhimõtet mainitakse EL-i kohtukaasustes harva ja enamasti siiski ilma viiteta konkreetsele õigusallikale. Samas viitavad nii isikuandmete kaitse üldmääruse (GDPR) kui ka veel trükimustad EL-i digitaalse finantspaketi määruste projektid tehnoloogianeutraalsusele kui oma eesmärgile ja suunisele. Selline

areng näitab, et põhimõtet ei saa enam seostada vaid IT-õigusega või IKT-sektoriga, vaid see mõjutab kõiki valdkondi, kus on digitaalne element.

Väitekirjas uuriti ka põhimõtte kajastamist Eesti õiguses ning autor tuvastas, et põhimõtet mainitakse vaid elektroonilise side seaduses (ESS). Samas jätab seadusandja isegi ESS-is põhimõtte defineerimata ning seletab seda teiste väärtuste kirjelduste kaudu eraldiseisvates sätetes. Nii nagu EL-i õiguses on ka põhimõtte komponendid äratuntavad riigihangete seaduses ning selle pinnalt on põhimõtet käsitletud ka Eesti kohtulahendites.

Uurides täpsemalt põhimõtte sisu, saab väitekirjas esitatu alusel järeldada, et põhimõte koosneb funktsionaalse samaväärsuse ja mõju samaväärsuse alampõhimõtetest ning jätkusuutlikkuse eesmärgist. Väitekirjas süveneb autor pigem funktsionaalse samaväärsuse alampõhimõtte tähendusse ja käsitleb mõju samaväärsust vaid funktsionaalse samaväärsuspõhimõtte nõutud tagajärjena.

1.2. Funktsionaalse samaväärsuse alampõhimõte

Funktsionaalne samaväärsus on infotehnoloogia üks peamisi reguleerimismeetodeid. Seda alampõhimõtet kasutatakse õigusloomes sageli õigustusena, et laiendada kehtivaid õigusnorme uuele tehnoloogiale ilma uue tehnoloogia ja selle erinevuste piisava analüüsita. Väitekirjas esitatud analüüs aga kinnitas vastupidiselt, et funktsionaalse samaväärsuse alampõhimõtte eesmärk on hoopis suunata seadusandjat tuvastama õigusnormis sisalduvate nõuete eesmärke ning hindama, kas neid eesmärke on võimalik saavutada kasutades tehnoloogia enda omadusi . Et mõista, miks kehtiv õigus on selline, nagu see on (nt nõudes vahendaja olemasolu, registreerimist või keskregistrit), tuleks uurida konkreetsete nõuete seadustamise ajal kasutatud mudeleid, protsesse ja lahendusi, et mõista, miks olid need nõuded vajalikud konkreetse õigusnormi eesmärgi täitmiseks. Selline analüüs aitab mõista õigusnormidesse sisseehitatud kallutatusi ja eelarvamusi ning paljastab selged ja varjatud tunnused või funktsioonid, mille olemasolu õigusnormid eeldavad ja mis tihtipeale nõuavad uuele tehnoloogiale sobimatuid, korduvaid või ebavajalikke formaalsusi. Selliste formaalsuste täitmise jätkuv nõudmine võib uuendajat piirata innovaatilise tehnoloogia peamiste eeliste kasutamiselning takistada uue tehnoloogia kasutamist. Lisaks tuleb funktsionaalse samaväärsuse alampõhimõtte alusel seadusandjal veenduda, et formaalsuste nõudmine ei oleks diskrimineeriv ka tehnoloogia kasutajate harjumuste ja käitumise suhtes (nt tarkade lepingute kasutajad võivad soovida sõlmida elektroonilises vormis lepinguid ka anonüümselt).

Väitekirjas esitatud kasutusjuhtude analüüsi põhjal jõudis autor järeldusele, et funktsionaalne samaväärsus nõuab näiteks ka seda, et riigivõim nii seadusandja kui ka täidesaatva ja kohtuvõimu rollis aktsepteeriks eri tehnoloogiakasutusjuhtudel õigusnormis nõutust teistsugust lahendust, juhul kui selle teistsuguse lahenduse eesmärk on samaväärne normis nõutuga. Näiteks kolmanda hajusraamatutehnoloogia kasutusjuhu puhul tuvastas autor, et elektrooniliste allkirjade osas vajaliku isikutuvastus nõude täitmiseks võiks aktsepteerida nii hajus-

raamatutehnoloogias endas sisalduvaid kui ka sellest eraldiseisvaid funktsioone, sh võimaldades isikut tuvastada muude tõendite alusel, nagu IP-aadress, e-posti aadress, telefoninumber jne, või hoopis laiendades valiku- ja lepinguvabadust, võimaldades isikutuvastusest loobuda elektroonilises vormis lepingute puhul (anonüümsed elektroonilised lepingud jne).

Autor leidis väitekirjas, et mõned õigusnormidest tulenevad nõuded (nt PKI-mudelile tuginev isikusamasuse tuvastamise süsteem, mis on sätestatud eIDAS-e nõuetes) on tegelikkuses pelgalt „riskijuhtimise viis", mille eesmärk on lepingu osapoolelt kõrvaldada isiku tuvastamise koorem, kuna see võib osutuda lepingu täitmise nõudmisel koormavaks. Siinkohal võib küsida, kas sellise riskijuhtimise eesmärk õigustab formaliseeritud õigusraamistikku, mis ei anna seda riskijuhtimise valikuvabadust lepingupooltele. Arvestades tarkade hübriidlepingute kasutusjuhtu, on seadusandjal alati võimalus lubada lepingupooltel kasutada funktsionaalselt samaväärseid elektrooniliste lepingute sõlmimise tööriistu, tagades mõju samaväärsuse ka juhul, kui kasutajad ise soovivad võtta riske, mis tulenevad puuduvast isikusamasuse tuvastamise funktsioonist (nt elektroonilises vormis anonüümsed lepingud).

Siinkohal tuleb arvestada, et isetäitva (*self-executing*) lepingu täitmisele pööramine on lihtsam kui mitteisetäitva (*non-self-executing*) lepingu täitmisele pööramine, isegi kui sellise lepingu puhul on täidetud isiku tuvastamise funktsioon. Üks ei pruugi olla ilmtingimata parem alternatiiv kui teine pelgalt seetõttu, et kasutajad või seadusandja on selle alternatiiviga harjunud. Kui seadusandja eelistab üht lahendust teisele, tähendab see seda, et ta lubab enesele innovaatiliste lahenduste diskrimineerimist valikute põhjal, mis võivad kitsendada isiku valikuvabadust.

Kõnealune alampõhimõte seab kahtluse alla igasuguse diskrimineerimise teatud olemasoleva lahenduse alusel ja nõuab, et seadusandja analüüsiks, kas uuenduslik lahendus suudab saavutada kehtiva õiguse nõuete eesmärgid funktsionaalselt samaväärselt, ilma et see lahendust täidaks kõiki vorminõudeid, mida kehtiv õigus ette näeb.

Kuigi analüüs näitas, et seadusandjal ja kohtuvõimul on raskusi funktsionaalse samaväärsuse põhimõtte kohaldamisega, võib selle kohaldamine olla edukas, kui kaasata tehnoloogia ja selle funktsioonide hindamisse tehnikaeksperte. Lisaks saavad oma teadmisi jagada turuosalised, uuendajad ja huvirühmad, koostades eneseregulatsiooni standardeid, suuniseid või muid polütsentrilise koosreguleerimise väljendusi, mida saab esitada kirjaliku tekstina või lõimida koodipõhise lahendusena tarkvarasse (koodipõhine reguleerimine).

Siinkohal uuris autor lähemalt, kuidas tehnoloogianeutraalsuse põhimõtet ja selle alampõhimõtteid praktikas rakendada.

1.3. Põhimõtte rakendamine funktsioonide analüüsi teel

Selleks, et tehnoloogianeutraalsuse põhimõtet rakendada, on vaja teha nii funktsioonide kui ka mõjude analüüs ning hinnata nõnda uue tehnoloogia kohtlemist olemasolevate õigusnormide alusel. Seega on tehtavas analüüsis kaks osa:

(iii) et hinnata funktsionaalset samaväärsust, tuleb kõigepealt kaardistada uue tehnoloogia funktsioonid ning ka olemasolevate õigusnormide alusel nõutud funktsioonid ning nende nõuete ja funktsioonide eesmärgid;
(iv) teiseks tuleb hinnata mõjude samaväärsust ehk seda, kas olemasolevates õigusnormides toodud nõuetele vastavus või nõuete eesmärkidele vastavus toob kaasa samaväärse mõju nii varasemale kui ka uuele tehnoloogiale, mis pruugib täita osa õigusnormides toodud nõudeid uuele tehnoloogiale omasel viisil. Mõju all peetakse siinkohal silmas nii instrumendi kehtivust, siduvust, heauskse omandamise võimalikkust, registrikande usaldusväärsust, tehingu vorminõuet, jms.

Analüüsi raames kallutatuse või eelarvamuse tuvastamine sõltub sellest, kas analüüsija mõistab uut tehnoloogiat, selle toimimist, selle funktsioone ning nende funktsioonide eesmärke, olemasolevate õigusnormide mõju ning ka tehnoloogianeutraalsuse põhimõtet. Seega on olemasolevate õigusnormide puhul oluline, et kehtiv õigus oleks läbipaistev ja neutraalne ka uue tehnoloogia ja taristu suhtes. Kohtuasja Hedqvist analüüs näitas, et isegi kui õigusnormid ei ole koostatud tehnoloogianeutraalselt, saab neid tehnoloogianeutraalselt rakendada, kui seadusandja analüüsib tehnoloogia funktsioone, kasutab funktsionaalset tõlgendamist ning eraldab aega, et uurida tehnoloogia mõju, kehtiva õiguse eesmärke ja kehtiva õiguse mõju uuenduslikule lahendusele. See tähendab, et isegi „ootame-vaatame“ ja „kehtiva õiguse rakendamise“ regulatiivstrateegiat (mis ei pruugi olla tehnoloogianeutraalne) saab rakendada tehnoloogianeutraalsel viisil juhul kui seadusandja võtab enda kanda uurimistöö koorma ega ole innovaatiliste kasutusjuhtude uurimises passiivne.

2. Kuidas jätkusuutlikult tagada õigusnormide tehnoloogianeutraalsus hajusraamatutehnoloogia suhtes?

Tehnoloogianeutraalsuse põhimõtte oluline omadus on ühtlasi tagada õigusnormide jätkusuutlikkus ja paindlikkus. Jätkusuutlikkust nimetatakse ka õigusaktide tulevikukindlaks muutmiseks või „pikaealisuse tagatiseks“. Sel põhjusel peaks tehnoloogia suhtes kohalduv õigusnorm olema piisavalt paindlik, et mitte takistada uue tehnoloogia kasutust või sama tehnoloogia uusi kasutusvõimalusi. Samal ajal tuleb arvestada, et mida abstraktsem on õigusnorm, seda ebakindlamad on selle adressaadid normi sisu ja sellest tulenevate kohustuste osas. Subsidiaarsuspõhimõttest tuleneb, et mida kõrgemal tasandil konkreetne õigusaktide hierarhias on, seda abstraktsemad ja jätkusuutlikumad peavad selle õigusnormid

olema, samas kui madalam tasand õigusaktide hierarhias koosneb vähem kestlikest ja lünkade täitmiseks mõeldud suunistest, standarditest jms.

Eelneva põhjal saab järeldada, et tehnoloogia neutraalsus peaks olema kehtiva õiguse tõlgendamist suunav meetod, sest see on osa teleoloogilisest meetodist. Ainus erinevus seisneb selles, et tõlgendamine peaks olema funktsionaal-teleoloogiline. Tõlgendaja peaks püüdma mõista kehtivas õiguses nõutud rakenduste või lahenduste funktsioone ja tõlgendama kehtivat õigust viisil, mis ei hinda funktsioone kui tööriistu, vaid peab suutma mõista nende funktsioonide eesmärke ning hindama, kas uus tehnoloogia suudab saavutada neid eesmärke samaväärselt. Sarnane lahendus on lisatud isikuandmete kaitse üldmäärusesse lõimitud andmekaitse või lõimprivaatsuse ('*privacy-by-design*') regulatsiooni, mille kohaselt on sõnastatud küll andmekaitse eesmärgid, kuid tehnilised ja korralduslikud meetmed selle kaitse tagamiseks on jäetud kohustatud isikute endi valida. Selles lahenduses väljendubki tehnoloogianeutraalsuse põhimõte. Lõimprivaatsus kui regulatsiooni kujundusviis on n-ö avatud lahendus, mis ei omista asendamatut väärtust varasemale tehnoloogiale, ärimudelile või taristule, sest „sobivate tehniliste või korralduslike meetmete" valik on selle olemasoleva turuosalise või uuendaja enda teha, kes peab pakkuma nõutud kaitset isikuandmete kaitse üldmääruse alusel.

Tehnoloogia neutraalsuse põhimõttest saadakse sageli valesti aru. Põhimõtte eesmärk on piirata õigusnormide mõju tehnoloogia, tööriista või vormi valikule, rõhutades, et riigi asemel peab otsustama turg seda, milline tehnoloogia on turul edukas. Lisaks nimetatud põhimõte vaikimisi pigem piirab varasemat tehnoloogiat silmas pidades väljatöötatud õigusnormide kohaldamist uuele tehnoloogiale, isegi kui uuel tehnoloogial on sama otstarve või sarnased funktsioonid. Seega nimetatud põhimõte pigem pooldab eneseregulatsiooni kui sobimatu kehtiva regulatsiooni kohaldamist uutele tehnoloogiatele või olemasoleva tehnoloogia uutele kasutusjuhtudele.

Arvestades tehnoloogia kiiret arengut, tempoprobleemi (*pacing problem*) ja Collingridge'i dilemmat, saab vastuolu tehnoloogianeutraalsuse põhimõttega lahendada, kaaludes alternatiivseid regulatiivstrateegiaid, sh funktsionaalse samaväärsuse alampõhimõtte kasutamist ilma regulatsiooni ennast muutmata. Väitekirjas käsitleb autor sellist alternatiivi kui erandi mudelit (*waiver model*). Erandi mudelit kasutatakse pisut muudetud kujul ka digitaalse finantspaketi projektides, milles luuakse MIFID II ja Euroopa keskdepositooriumite määrusega (CSDR) määrustes toodud nõuetest hajusraamatutehnoloogia suhtes hulk erandeid, kuid seda vaid regulatiivse muudatuse teel.

Autor järeldab, et arvestades tehnoloogiliste muudatuste kiirust, jätkub tehniliste lahenduste erinev de- ja rekonstrueerimine, mistõttu ei suuda tehnoloogiaspetsiifiline staatiline õigus iialgi olla piisavalt paindlik kõigi uute tehnoloogiate suhtes. Seega on vaja üldisemat lähenemisviisi, mille puhul kasutatakse turul väljakujunenud või riigi kehtestatud standardeid (koosreguleerimine) või eneseregulatsiooni suuniseid kõigi uudsete lahenduste puhul, et oleks tagatud nende õiglane kohtlemine.

Kui aga kasutada funktsionaalse samaväärsuse alampõhimõtet korrektselt, siis on võimalik tagada õigusraamistiku piisav paindlikkus, mis võimaldab regulatsioonil kohaneda uuest rakendusest või tehnoloogiast tulenevate probleemidega, mida innovatsioon tekitab ja millele saab kiiresti reageerida, kasutades reageerimisprotsessis eri huvirühmade abi. Alampõhimõttest lähtudes peab seadusandja normi luues läbi mõtlema ka selle, kuidas oleks võimalik tagada õigusnormi mõju samaväärsus juhul, kui funktsionaalne analüüs tuvastab rakenduse, mis on olemasolevate õigusnormide nõuete eesmärgiga samaväärne. Väitekirja kohaselt saab selle eesmärgi saavutamisse kaasata tehnoloogilise innovatsiooni eesliini osalisi ehk siis uuendajad endid, et kiiremini hinnata, mis lahendust saab pidada funktsionaalselt samaväärseks alternatiiviks ja millist mitte. Selline hindamisprotsess võib toimuda nn liivakasti (*sandbox*) menetluse kaudu või ka polütsentrilise koosreguleerimise mudeli kasutamise teel, mida väitekirjas ka põgusalt tutvustatakse. Samas ei saa siin rääkida ühestki konkreetsest toimivast reguleerimismudelist, vaid pigem alternatiividest, mille vahel seadusandjal on võimalik valida, adresseerides tehnoloogianeutraalsusest tulenevaid nõudeid.

Tehnoloogianeutraalsuse tagamine õigusnormides nõuab innovaatorite endi aktiivsust, et selgitada seadusandjale õigusnormide mõju samaväärsuse puuduseid või normides sisalduvaid eelarvamusi võimalike lahenduste kohta. Samuti nõuab põhimõte avatust, turuosalejate endi kehtestatud eneseregulatsiooni aktsepteerimist, standardite kehtestamist, eeskuju näitamist, mis võib olla esindatud ka hajusraamatutehnoloogiale omaselt protokollis endas või konsensusmehhanismis või võrgustiku valitsemisreeglites. Selliseid laiapõhjalisi reguleerimisstrateegiate alternatiive peab seadusandja kaaluma ka seepärast, et hajusraamatutehnoloogia on mitmeotstarbeline tehnoloogia (*all-purpose technology*), mida saab kasutada paljudes sektorites, rakendustes ja lahendustes ning mis toob kaasa vajaduse muuta õigusnorme paljudes õigusaktides ja võimaldada selle tehnoloogia kasutamist samaväärse mõjuga. See tähendab, et väitekirjas lähenetakse regulatsiooni muutmise alternatiivsetele strateegiatele pigem fundamentaalsel tasandil ja ei laskuta teatava normi või õigusakti muutmise konkreetsetesse detailidesse eraldiseisvalt seega vältides fragmenteeritust. Selline valik on õigustatud, et mõista hajusraamatutehnoloogia eripära ja suuremat pilti olemasolevate õigusnormide mõjust, millega seadusandja peaks uurima, et tagada tehnoloogianeutraalsus. See ei tähenda, et konkreetse õigusnormi või -akti funktsionaalne analüüs konkreetse kasutusjuhu puhul ei päädi konkreetsete muudatusettepanekutega, vaid pigem, et selle väitekirja eesmärk ei ole teha muudatusettepanekuid normi tasandil, mida rakendatakse kasutusjuhu puhul, vaid pakkuda alternatiive, kuidas oleks võimalik tagada õiguses hajusraamatutehnoloogia suhtes jätkusuutlik neutraalsus, arvestades seda, mis tulemusi väitekirjas käsitletud kasutusjuhtude analüüsid näitasid. Nagu öeldud, ei ole ka väitekirjas hajusraamatutehnoloogia kasutusjuhtude osas kohalduv õigus mingi eraldi valdkond ja see tehnoloogia ei ole eraldi reguleerimisobjekt. Samuti ei ole üksnes hajusraamatutehnoloogia rakendustele suunatud õigusnormid või õigusakt otseselt tehnoloogianeutraalsuse põhimõttega vastuolus ja selle kinnituseks on ka EL-i digitaalse finantspaketi projektdokumentatsioon.

Sellest lähtuvalt käsitletakse väitekirjas varasemates hajusraamatutehnoloogia uurimustes käsitletud regulatiivsete strateegiate kogumit, mille hulgas on kolm peamist kategooriat:

(i) oota-ja-vaata;
(ii) olemasolevate õigusnormide kohaldamine;
(iii) olemasolevate õigusnormide muutmine.

Need strateegiad võivad olla väljendatud eri mudelites, mida väitekirjas käsitletakse hajusraamatutehnoloogia kontekstis. Mudelite hulgas on nt erandi mudel, mida kohaldatakse siis kui funktsionaalne analüüs on tuvastanud, et uus tehnoloogia suudab funktsionaalselt samaväärselt normi eesmärke saavutada ning peaks seega olema tagatud mõju samaväärsus isegi kui uus tehnoloogia kõiki õigusakti nõudeid ei täida . Kuid mudelite hulgas on ka GDPR-i lõimprivaatsuse mudel, funktsionaal-teleoloogiline tõlgendamismudel, UNCITRAL-i mudel ning olemasolevate õigusnormide muutmine eneseregulatsiooni ja polütsentrilise koosreguleerimise teel. Igal mudelil võivad olla oma puudused ja eelised nii neutraalsuse kui ka jätkusuutlikkuse osas, kuid nagu autor väitekirjas tuvastas, on vaata-ja-oota strateegia pigem olemasolevate õigusnormide kohaldamine, mitte eraldi strateegia, ning mudelid ise ei ole eksklusiivsed seega seadusandja pruugib kasutada mitut mudelit või strateegiat samaaegselt, leides sobiliku alternatiivi lähtuvalt tehnoloogia rakendus- ja kasutusjuhtudele.

3. Kas autori valitud hajusraamatutehnoloogia kasutusjuhtude suhtes kohalduvad õigusnormid on kooskõlas tehnoloogianeutraalsuse põhimõttega?

Väitekirjas analüüsitakse kolme hajusraamatutehnoloogia kasutusjuhtu, et kontrollida, kas kehtivad õigusnormid on kooskõlas tehnoloogianeutraalsuse põhimõttega või valitseb hajusraamatutehnoloogia suhtes tehnoloogiline või taristust lähtuv kallutatus ehk eelarvamus. Kasutusjuhu analüüsis kasutab autor probleemikogumi lähenemisviisi ja käsitleb kasutusjuhule kohalduvat kehtivat regulatsiooni, et kontrollida, kas see vastab tehnoloogianeutraalsuse põhimõttele. Täpsemad uurimisküsimused iga hajusraamatutehnoloogia kasutusjuhu kohta on toodud allpool.

3.1 Kas rahapesutõkestamise regulatsioon Eestis ja selle rakendamine olid bitimündi ja selle kauplejate suhtes tehnoloogianeutraalne (*de Voogd* näitel) sarnaselt EL käibemaksu regulatsiooni rakendamisele bitimündi ja selle kauplejate osas (*Hedqvist*'i näitel)?

Esimese vaadeldava kasutusjuhu puhul uurib autor bitimündi ja bitimüntide vahetusteenuse pakkujate kohtlemist võrreldes kehtiva vääringu ning selle vahetusteenuse pakkujate kohtlemisega analüüsides *de Voogd* ja *Hedqvist*

kohtuasju. Riigikohtu lahend *de Voogd*'i kohtuasjas tehti 2016. aasta 11. aprillil ja Euroopa Liidu Kohtu otsus *Hedqvist*'i kohtuasjas 2015. aasta 22. oktoobril (sh kohtujuristi arvamus samas kohtuasjas avaldati 2015. aasta 16. juulil). Seega analüüsib autor esimese kasutusjuhu raames 2015.–2016. aastal kehtinud rahapesu ja terrorismi rahastamise tõkestamise seaduse (RahaPTS) eri redaktsioone, rahapesu tõkestamise direktiivi eri redaktsioone ja EL käibemaksudirektiivi piiratud ulatuses.

Hedqvist'i kohtuasjas järeldas Euroopa Liidu Kohus käibemaksudirektiivi artikli 135 lõike 1 punkti e alusel, et bitimünte ja nendega tehtud tehinguid tuleb kohelda käibemaksuga maksustamise mõttes võrdselt muude kehtiva vääringuga tehtud finantstehingutega, kuna kehtiv vääring ja bitimünt on nende kasutajatele funktsionaalselt samaväärsed. Lahend on seega kooskõlas tehnoloogianeutraalsuse põhimõttega, sh selle põhimõtte funktsionaalse samaväärsuse alampõhimõttega.

Samas erines *Hedqvist*' is toodud kohtu järeldus oluliselt järeldusest, milleni vaid aasta varem jõudis Euroopa Komisjoni käibemaksukomitee. Selleks et võtta *Hedqvist*'i asjas seisukoht, uurisid Euroopa Liidu Kohus, kohtujurist Kokott ja varem ka käibemaksukomitee põhjalikult bitimündi funktsioone ning võrdlesid neid kehtiva vääringu ehk riikliku valuuta funktsioonidega ja kohaldamisele kuuluva normi eesmärgiga. Kohtujurist Kokott järeldas, et vääringutel, mida kasutatakse maksevahendina, „ei ole põhimõtteliselt muud praktilise kasutamise võimalust kui maksevahendina kasutamine" ja seepärast peaks „see, mis kehtib seaduslike maksevahendite kohta, kehtima ka muude maksevahendite kohta, mille funktsioon sellega ammendub", sest „nad täidavad käibemaksu seisukohast sama ülesannet".

Hedqvist'ile eelnevates bitimündile kohalduva regulatsiooni analüüsides lähtus Euroopa Komisjoni käibemaksukomitee käibemaksudirektiivi artikli 135 lõike 1 punkti e sõnastuse grammatilisest tõlgendusest, lubades terminoloogial piirata käibemaksudirektiivi mõju funktsionaalselt samaväärsete maksevahendite osas ja jättes selle tulemusel bitimündid normi kohaldamisulatusest välja. Toodud lähenemisega jättis käibemaksukomitee kõrvale vastavate normide funktsionaalse ja teleoloogilise tõlgenduse ning tõlgendas maksevahendi erinevuste tõttu õigusnormi bitimüntide suhtes diskrimineerival viisil. Samas liigitas *Hedqvist*'i otsuses toodud vastava normi tõlgendus bitimündid seaduslike maksevahenditega samaväärsete objektide hulka, mille tulemusena laiendas kohus tehnoloogianeutraalsuse põhimõttega kooskõlas käibemaksudirektiivi artikli 135 lõike 1 punkti e kohaldamisala. Nagu juba ülal toodud, kinnitab ka käsitletud lahend, et seadusandlik, täitev- ja kohtuvõim peavad tegema tehnoloogia funktsioonide analüüsi, et kehtivat õigust tehnoloogianeutraalselt tõlgendada, ning liikuma õigusnormi grammatilisest tõlgendamisest ka funktsionaalse ja teleoloogilise tõlgendamise poole, hinnates ühtlasi õigusnormi kohaldamise mõju uue tehnoloogia ja bitimüntide kasutusele.

Kohtuasjas *de Voogd* leidis Riigikohus sel ajal kehtinud RahaPTS-i alusel, et „õigusnormi sõnastuse alusel loetakse krüptoraha vahetusteenuse pakkujaid kehtiva õiguse kohaselt alternatiivsete maksevahendite teenuse pakkujateks".

Sellisele järeldusele jõudmiseks tuvastas Riigikohus mõned bitimündi omadused, näiteks i) bitimünte saab vahetada kehtiva vääringu vastu, ii) bitimüntide kauplemiskeskkondades tekib neil rahaliselt mõõdetav kurss ning iii) neid saab kasutada kehtiva valuuta asemel ka tehingute eest tasumiseks. Seega, samamoodi nagu Euroopa Liidu Kohus *Hedqvist*'i asjas, leidis ka Riigikohus, et bitimüntide ainus funktsioon on nende kasutamine maksevahendina. Samas ei viidanud Riigikohus *de Voogd*'i kohtuasjas *Hedqvist*'i lahendile ega selle lahendi kohtujuristi arvamusele ega põhjendanud ka, miks see lahend ei ole asjakohane või miks selles toodud samaväärsust ei saa de Voogdis kohaldada. Funktsionaalne analüüs bitimündi ja riikliku valuuta erinevuste kohta, mis võiks olla alus nende erinevale kohtlemisele, *de Voogd*'i lahendis puudub. Samuti ei kasutatud Riigikohtu lahendis konkreetse õigusnormi funktsionaalset ja teleoloogilist tõlgendamist, et hinnata, kas enne hajusraamatutehnoloogia loomist jõustunud vastav RahaPTS-i norm on diskrimineeriv bitimüntide osas või hajusraamatutehnoloogia rakenduste suhtes.

Seega, olenemata asjaolust, et Riigikohus jõudis *de Voogd*'is bitimündi kasutusotstarbe osas samale järeldusele nagu Euroopa Liidu Kohus *Hedqvist*'is – et bitimünte saab kasutada kehtiva valuuta asemel ka tehingute eest tasumiseks –, ei järeldanud kohus *de Voogd*'i kaasuses sarnaselt *Hedqvist*'iga, et bitimündid on funktsionaalselt samaväärsed kehtiva vääringuga ning nende kohtlemine peab seega olema kooskõlas kehtiva vääringu kohtlemisega. Selle asemel luges nii Politsei- ja Piirivalveameti Rahapesu Andmebüroo (RAB) kui ka Riigikohus, et bitimünt tuleb liigitada *sui generis*-kategooria „alternatiivne maksevahend" alla ning seda tuleb kohelda teisiti kui kehtivat vääringut.

Lahendi ajal kehtinud RahaPTS-is oli nimetatud kategooria sõnastatud väga üldiselt, defineerides RahaPTS-i § 6 lg 4 kohaselt alternatiivseid maksevahendeid kui „rahalise väärtusega vahendeid, mille abil on võimalik täita rahalisi kohustusi või mida saab vahetada kehtiva vääringu vastu". Bitimüntide lugemine alternatiivsete maksevahendite hulka võimaldas kohelda nii neid ühikuid kui ka nendega kauplejaid teisiti kui riiklikku valuutat või sellega kauplejaid. Seega tõi selline kvalifikatsioon kaasa RahaPTS-i § 15 lg 8 alusel bitimüntidega kauplejate suhtes tunduvalt karmimate vastavusmeetmete (eelkõige näost näkku isikutuvastamise nõue väga väikse tehinguväärtuse pealt) kohaldamise kui riikliku valuuta kauplejate suhtes. Seetõttu piiras bitimüntide liigitamine alternatiivseteks maksevahenditeks oluliselt bitimüntidega kauplejaid, mis bitimüntide kauplemise eripärasid arvestades (tegu on globaalselt kasutatava digivormis maksevahendiga, mis võimaldab kaubelda pseudoanonüümselt) ajutiselt seiskas kogu sellega seotud äritegevuse Eesti turul.

Tehnoloogianeutraalsuse põhimõtte alusel tuleb kriitiliselt hinnata selliste uute *sui generis*-kategooriate teisiti kohtlemist kehtivast vääringust ja tuvastada, mis on teisiti kohtlemise eesmärk. Nagu eespool märgitud, tuleb sellesuunalise analüüsi tegemiseks tutvuda uue tehnoloogia funktsioonidega ning ühtlasi seadusandja eesmärgiga õigusnormi loomisel, et mõista, kas õigusnormi funktsionaal-teleoloogilise tõlgendamise tagajärjel on erinev kohtlemine põhjendatud, täitmaks seadusandja püstitatud eesmärki. Autorile jääb ebaselgeks ja *de Voogd*'i

lahendi alusel põhjendamatuks, miks Riigikohus eiras Euroopa Liidu Kohtu järeldust kehtiva vääringu ja bitimüntide funktsionaalse samaväärsuse kohta ning ei pidanud vajalikuks *Hedqvist*'i lahendit ega selles toodud järeldusi uurida ega hinnata. Lahendist jääb selgusetuks, kas Riigikohus leidis, et RahaPTS-ist ja selle § 15 lg-st 8 tulenev alternatiivsete maksevahendite kehtivast vääringust erinev kohtlemine on Riigikohtu arvates kooskõlas *Hedqvist*'i lahendiga või mitte. Autori arvates oleks *Hedqvist*'i lahendist lähtudes saanud aktsepteerida bitimünte funktsionaalselt samaväärsena kehtiva vääringuna. Ühtlasi oleks pidanud tehnoloogianeutraalselt põhjendama RahaPTS-i § 15 lg 8 alusel kehtiva vääringuga kauplejate suhtes oluliselt karmimate vastavusmeetmete kohaldamist, lähtudes seadusandja eesmärgist ja bitimüntidega seotud erinevustest. Tehnoloogianeutraalsus tähendab siinjuures seda, et bitimüntide teisiti kohtlemisel tuleb tagada, et erinevus ei tooks kaasa ebavõrdset kohtlemist, eelarvamusi uue tehnoloogia suhtes ega bitimüntide suhtes diskrimineerivat kohtlemist, kui see kohtlemiserinevus pole kooskõlas seadusandja eesmärgiga. Siinkohal on oluline rõhutada, et tehnoloogianeutraalsuse põhimõtte järgi ei saa seadusandja seada eesmärgiks soodustada bitimüntidega kauplemise asemel kehtiva valuutaga kauplemist ja sel põhjusel luua viimastele soodsamad tingimused.

de Voogd'i lahendi ajal kehtinud rahapesu tõkestamise direktiiv ei käsitlenud bitimünte ega olnud ka aluseks RahaPTS-i alternatiivse maksevahendi kategooriale. Samas oli sel ajal kehtinud rahapesu tõkestamise direktiiv minimaalse harmoniseerimise direktiiv ning lubas liikmesriikidel kehtestada rangemad reeglid, et tegeleda suurte ohtudega, mida liikmesriigid peavad maandama riigisiseselt. Seega oli liikmesriikidel rahapesu tõkestamise direktiivi artikli 4 alusel õigus laiendada direktiivi kohaldamisala uute kohustatud isikute kategooriatega, teavitades sellest komisjoni. Nagu autor tuvastas *de Voogd*'i lahendis, ei olnud ka Riigikohus Eesti Vabariigi nimel teavitanud komisjoni uuest *sui generis*-kategooriast. Samas leidis kohus, et mitteteavitamine „ei oma selle regulatsiooni kehtivuse ja kohaldatavuse aspektist tähendust". Riigikohus pigem rõhutas, et sama direktiivi artikli 5 alusel võivad liikmesriigid „direktiiviga reguleeritud valdkonnas rahapesu ja terrorismi rahastamise tõkestamiseks vastu võtta või kehtima jätta käesoleva direktiivi sätetest rangemad sätted". Siinkohal pidas Riigikohus vajalikuks nentida, et „direktiivi artiklid 4 ja 5 on üheselt mõistetavad ning piisavalt selged. Seega esineb *acte clair*-olukord ning puudub alus ja vajadus küsida Euroopa Kohtult eelotsust." Selline järeldus tundub väitekirja autorile ootamatu olukorras, kus riigivõimu eri asutused kuulutasid avalikult, et bitimüntidele ei kohaldu ühtegi normi; kus kohustatud isikute laiendamise aluses (artikkel 4) toodud teavitamiskohustust ei olnud järgitud; kus rangemad nõuded artikli 5 alusel olid kehtestatud vaid teatud rühmale (alternatiivne maksevahendiga kaupleja), tuues seega kaasa selle rühma ebavõrdse kohtlemise. Arvestades halduskohtumenetluse mittediskrimineerimise põhimõtet, proportsionaalsuse põhimõtet ja tehnoloogianeutraalsuse põhimõtet, oleks *de Voogd*'i lahendis Euroopa Kohtult eelotsuse küsimine artiklite 4 ja 5 kohta olnud kooskõlas halduskohtumenetluse peamise eesmärgiga, milleks on isikute õiguste kaitse õigusvastase tegevuse eest täidesaatva võimu teostamisel.

Nagu öeldud, ei tuginenud alternatiivse maksevahendi erinev kohtlemine *de Voogd*'i menetlemise ajal kehtinud EL-i õigusele ega olnud kooskõlas ka rahapesu tõkestamise 5. direktiivi ettepaneku eesmärkidega, mis avalikustati 5. juulil 2016. Autori hinnangul on oluline, et rahapesu tõkestamise 5. direktiivi ettepanekus kinnitasid selle koostajad, et mitte ükski Euroopa Liidu liikmesriik ei ole kehtestanud bitimüntide ega üldisemalt virtuaalvääringute kohta õigusakte, mis reguleeriks rahapesu tõkestamist. See tähendab, et kuigi *de Voogd*'i kohtuasjas leidis Riigikohus laiendavalt tõlgendades, et rahapesu tõkestamise nõuded reguleerivad *sui generis*-kategooriat „alternatiivne maksevahend", mis hõlmab ka bitimünte, ei peetud „alternatiivse maksevahendi" kohta kehtestatud norme bitimüntidele või üldisemalt virtuaalvääringutele suunatud normideks.

Bitimündi riigisisese õiguse *sui generis*-kategooriasse paigutamise negatiivne mõju isikule seisneb seega rangemate vastavusnõuete kohaldamises. Arvestades kohtu pädevust selles asjas, jääb ebaselgeks, miks halduskohus ei nõustunud *Hedqvist*'i lahendist lähtuvalt selles toodud järeldusega funktsionaalse samaväärsuse kohta ja pidas seda ebaoluliseks ning miks jättis kohus *Hedqvist*'i lahendi järeldused tähelepanuta, kvalifitseerides bitimündid *sui generis*-kategooria alla.

Kuigi Riigikohus leidis, et RahaPTS-is toodud alternatiivse maksevahendi kauplejate suhtes kohalduvate vastavusmeetmete tegelik mõju on ebaselge ja et seadusandja peaks põhjalikumalt hindama kõnealuste vastavusnõuete mõju, jättis Riigikohus autori hinnangul oma lahendis isiku õigused kaitsmata, eirates oma kohustust ise hinnata sätte mõju uuele tehnoloogiale ning kohaldada sätet tehnoloogianeutraalselt ja kooskõlas EL-i kohtupraktikaga.

3.2. Kas Eesti äriseadustiku alusel osaühingu osanike nimekirja pidamine juhatuse poolt võimaldab seda pidada hajusraamatutehnoloogia baasil funktsionaalselt samaväärsena keskregistri poolt peetava nimekirjaga ja kas seadus tagab sellisele osanike nimekirja pidamisele tehnoloogianeutraalsuse põhimõttest lähtuvalt võrdse kohtlemise?

Teine väitekirjas vaadeldav hajusraamatutehnoloogia kasutusjuht, mida käsitletakse põhjalikumalt artiklis II, keskendub osaühingu osanike nimekirja pidamisele Eestis. Hajusraamatutehnoloogia on olemuslikult arvestusraamatu tehnoloogia ja seega võiks eeldada, et seda sobiks kasutada ka igasuguste registrite ja nimekirjade pidamiseks, kus on oluline andmete terviklikkus ja muudatuste läbipaistvus. Seega on põhjendatud uurida, kas seda hajusraamatutehnoloogiat saaks kasutada osaühingute (OÜ) osanike nimekirjade pidamiseks. Eesti osaühingu osanike nimekirja pidamiseks on ÄS-is väitekirja kirjutamise seisuga ette nähtud kaks võimalust:

(i) osad registreeritakse väärtpaberite keskregistris (EVK-s) – EVK-s registreeritud osad – või
(ii) osanike nimekirja peab osaühingu juhatus – EVK-s registreerimata osad.

EVK-s on registreerinud osad vähem kui 5% OÜ-dest, mis tähendab, et 95% OÜ-del peab osanike nimekirja juhatus. Sarnane süsteem, et osanike nimekirja peab juhatus, on ka ÜK-s, Soomes, Rootsis, Taanis, Lätis, Saksamaal ja Hollandis. ÄS ei nõua juhatuselt mingi tehnoloogia kasutamist osanike nimekirja pidamiseks. Kehtivad normid ei näi ka kohustavat juhatust täitma mingeid erifunktsioone selle nimekirja pidamiseks, muutes omakorda vastavad normid tehnoloogiast sõltumatuks.

Samas sõltuvad osade võõrandamise nõuded osanike nimekirja pidajast. EVK-s registreerimata osade võõrandamise kohta kehtivad rangemad nõuded kui EVK-s registreeritud osade võõrandamise kohta. ÄS-i § 149 (4) alusel saab EVK-s registreerimata osi võõrandada üksnes notariaalselt tõestatud tehinguga, samas kui ÄS-i § 149 (5) alusel saab EVK-s registreeritud osi võõrandada mis tahes vormis tehinguga. Nimetatud nõudeid muudeti hiljuti riskikapitalisektori algatusel ning need jõustusid 01. augustil 2020 ja tõid kaasa teatud muudatused ka ÄS-i viidatud regulatsioonis. Muudatuste tulemusel nõutakse ÄS-i §-ga 149 (4) vaid käsutustehingu notariaalset tõestamist ning kohustustehingud on vormivabad. Lisaks saab OÜ ÄS-i § 149 (6) alusel teatud tingimuste täitmisel ka käsutustehingu vorminõuet oluliselt muuta, nimelt juhul, kui:

(i) osakapital on vähemalt 10 000 eurot;
(ii) osakapital on täies ulatuses sisse makstud;
(iii) põhikirjaga loobutakse notariaalse tõestamise vorminõudest;
(iv) põhikirja sellise kinnitamis- või muutmisotsuse poolt, millega loobutakse vorminõudest, peavad olema kõik osaühingu osanikud.

Selliste tingimuste täitmisel kohaldub osa võõrandamise käsutustehingule vaid kirjalikku taasesitamist võimaldav vorm. Kuna ainult 9,6% OÜ-dest täidab praegu 10 000 euro suurust osakapitali nõuet, on see muudatus hetkeseisuga oluline üksnes nendele ning 85% OÜ-dest peab muutma nii kapitali kui ka põhikirja, et saada muudatuse mõjust osa. Seega on kasutusjuhu kirjelduses toodud erinevused siiski relevantsed.

Seega nõuab kehtiv õigus teatud funktsioonide täitmist, mida seadusandja hinnangul saab teha vaid inimvahendaja (nt notar), tulenevalt sellest, kes on osanike nimekirja pidaja. Kehtiva õiguse alusel ei ole need funktsioonid ega notarist vahendaja vajalikud, kui osanike nimekirja peab EVK. Üksnes EVK kasutamise korral eeldatakse, et osanike nimekiri täidab teatud funktsioone, mis võimaldavad vormivabadust osa võõrandamisel. Kokkuvõttes tuleb nentida, et kehtiv õigus nõuab lisafunktsioonide täitmist, kui osanike nimekirja peab OÜ juhatus. Vorminõude mõju samaväärsus on seega seotud subjektiga, kes osanike nimekirja peab, mitte pidamisviisiga, sh sellega, mis funktsioone nimekirja pidamisel täidetakse või mis eesmärgid neil funktsioonidel on või mis väärtusi need funktsioonid kaitsevad. See omakorda tähendab, et kehtiv õigus on kallutatud kesksete vahendajate (EVK, notarid) poole.

Siinkohal on oluline nentida, et võõrandamise vorminõuded ei ole ainsad, mis nende kahe osanike nimekirja pidamisel erinevad. Väärtpaberite registri pidamise

seaduse § 9 (2) alusel saab registrile tuginedes heauskselt EVK-s registreeritud osi omandada. Sama heauskse omandamise võimalust EVK-s registreerimata osadele seadus ei võimalda. Nagu väitekirjas toodud näitab analüüs, et mõju samaväärsuse osanike nimekirja kannete konstitutiivse väärtuse mõistes tagab kehtiv õigus üksnes juhul, kui osanike nimekirja peab EVK, ning mõju samaväärsust ei omistata funktsionaalselt samaväärsele osanike nimekirja pidamise protsessile olukorras, kus selle pidaja ei ole taaskord EVK. Sellest tuleneb, et kehtiv õigus ei ole selle regulatsiooniga jätkusuutlik, kuna ÄS ei võimalda praegu innovatsiooni EVK-s registreerimata osanike nimekirja pidamise osas.Nagu öeldud, on hajusraamatutehnoloogia arvestusraamatu tehnoloogia ning sellel on teoreetiliselt funktsionaalsus, mis tagab usalduse, läbipaistvuse ja andmete kontrollimise võimaluse. See tähendab, et igal hajustehnoloogial põhineval osanike nimekirjal võivad olla olemas kõik funktsioonid, mida täidab EKV-s peetav osanike nimekiri. Kehtiv õigus ei piira juhatusel hajus- ega muu tehnoloogia kasutamist osanike nimekirja pidamiseks. Samas on kehtiv õigus tehnoloogiast sõltumatu ja ei nõua ega keela mis tahes tehnilise lahenduse kasutamist. Isegi juhul kui osanike nimekirja pidamisel kasutatakse tehnoloogiaid nagu nt. hajusraamatutehnoloogia siis olenemata selle pidamisel toimivatest funktsioonidest mõju samaväärsust ÄS ei taga. Kehtiv õigus ei tee vahet sellel, kuidas juhatus osanike nimekirja peab, kuna mõju samaväärsus on pelgalt subjektipõhine. Kehtiv õigus ei võimalda mõju samaväärsust.

Juhatus saab küll valida tehnilised ja korralduslikud meetmed nimekirja pidamiseks, ent seadusandja ei taga võrdset kohtlemist EVK-s registreeritud osadega olenemata neist meetmetest. Autor leiab, et kehtiv õigus ja ÄS-i hiljutised muudatused ei anna osanikule võimalust valida võrdsete alternatiivide vahel, isegi kui kasutatakse hajusraamatutehnoloogiat või muu tehnoloogia põhist osanike nimekirja pidamise lahendust, mille funktsioone peetakse samaväärseks EVK-s registreeritud osade osanike nimekirja pidamisega.

Seega viimastest muudatustest hoolimata oleks kehtiv õigus kooskõlas tehnoloogianeutraalsuse põhimõttega vaid juhul, kui see sätestaks eesmärgid, mida osanike nimekiri peab saavutama, et olla EVK-s registreeritud osa suhtes peetava osanike nimekirjaga samaväärne.

3.3. Kas hajusraamatutehnoloogial põhinevat allkirja targal lepingul saab lugeda funktsionaalselt samaväärseks eIDAS-e kvalifitseeritud elektroonilise allkirjaga ning kas eIDAS võimaldab seda allkirja tehnoloogianeutraalsuse põhimõttest lähtuvalt võrdselt kohelda?

Kolmas hajusraamatu kasutusjuht, mida autor väitekirjas analüüsis, on seotud targa lepinguga, mis sõlmitakse esmasel mündipakkumisel (*initial coin offering* ehk *ICO*). Vastutasuks võõrandatud virtuaalvääringu eest emiteerib korraldaja tavaliselt münte (*token*) otse füüsilistele isikutele, kes pakkumises osalevad, ja kasutab selleks isetäitvat protokolli, mida nimetatakse targaks lepinguks. Väitekirjas uuris autor targaks lepinguks nimetatava koodi ja esmase mündipakkumise

muude tüüpelementide (esmase mündipakkumise korraldajalt avalikkusele tehtud pakkumus, pakkumusega nõustumus kasutaja poolt, vahendite ülekandmine pakkumise korraldajale; autor nimetab neid targaks hübriidlepinguks) kvalifitseerimist kehtiva õiguse alusel elektroonilist vormi lepinguks.

Lepingu vorm on oluline, sest teatud vara või õiguste võõrandamiseks võidakse riigisisese õiguse järgi nõuda teatavat lepinguvormi. Esmase mündipakkumise korral emiteeritakse või võõrandatakse erinevaid õigusi väljendavaid münte. Maksimeerimaks võimalust, et neid lepinguid loetakse kehtivaks, on vaja aru saada, kas leping on sõlmitud korrektses vormis.

Käesolevas doktoritöös uuris autor seda, kas esmase mündipakkumise raames sõlmitud tarku lepinguid saab Euroopa Liidu õiguse mõistes lugeda elektroonilises vormis sõlmitud lepinguteks. Tarkade lepingute vastavat kvalifitseerimist lepinguvormide tüpoloogia alusel on nimetatud oluliseks õigusküsimuseks ka Euroopa Liidu plokiahela uuringus. Selleks, et lugeda lepingut elektroonilises vormis sõlmitud lepinguks, peab esmalt kontrollima, mis nõuded peavad olema selleks täidetud kehtiva riigisisese õiguse kohaselt, sest seda küsimust Euroopa Liidu õigus ei reguleeri. Selle kvalifikatsiooni seisukohast on oluline mitte üksnes lepinguõigus, vaid ka õigusnormid, mis reguleerivad elektroonilisi allkirju, kuna elektroonilised allkirjad peavad vastama teatud usaldustasemele (kvalifitseeritud elektrooniline allkiri), et lepinguvormi saaks kvalifitseerida elektrooniliseks. Seepärast keskendub autor selle kasutusjuhu puhul Euroopa Liidu elektroonilise allkirja määruse eIDAS kohaldamisele, pidades silmas elektroonilist allkirja, mis on lisatud esmases mündipakkumises kasutatavale targale hübriidlepingule.

Nagu ka väitekirjas toodud analüüs näitas, on eIDAS-e eesmärk harmoneerida elektrooniliste allkirjade regulatsiooni, et neid allkirju saaks usaldada piiriüleselt ning selle tulemusel võimaldada elektroonilisi tehinguid ja elektroonilist kaubandust. Lisaks on eIDAS-e eesmärk kohaldada tehnoloogianeutraalsuse põhimõtet tagamaks, et elektroonilisi tehinguid peetakse funktsionaalselt samaväärseks paberkandjal tehingutega. Iga kehtiv õigusakt on koostatud olemasoleva tehnoloogia põhjal ja ka eIDAS on välja töötatud selleks, et seadustada protsess, kuidas elektrooniline allkirjastamine sel ajal praktikas toimis, ehk avaliku võtme taristu (Public Key Infrastructure (PKI)) mudelil. See tähendab, et kuigi eIDAS-t peetakse tehnoloogianeutraalseks, on see siiski rajatud PKI-mudelile ja määruse vastav regulatsioon pelgalt peidab PKI-mudeli terminoloogiliselt neutraalsemate terminite varju.

Avaliku võtme taristu sõltub kontrollitud, s.o Euroopa usaldusnimekirja (European List of Trusted Lists (LOTL)) kantud allikate väljastatud digisertifikaatidest ja krüptograafilistest võtmetest. Neid usaldusteenuse pakkujaid on vaja usaldada, sest nad väljastavad sertifikaate ja privaatvõtmeid kasutajatele, et kasutajaid oleks võimalik seostada elektroonilise allkirjaga. See protsess on vajalik, et allkirja saaks pidada kvalifitseeritud elektrooniliseks allkirjaks, mis omakorda on vajalik selleks, et lepingut saaks lugeda elektroonilises vormis lepinguks.

Võrreldes PKI-taristuga on targas hübriidlepingus kasutatava hajusraamatutehnoloogia alus teistmoodi usaldustaristu – selline, mis on ehitatud protokolli endasse ja selle valitsemise reeglitesse. Väitekirjas autori poolt esitatud

funktsionaalne analüüs näitas, et hajusraamatutehnoloogia põhiste elektrooniliste allkirjade usaldusväärsus ei sõltu usaldussertifikaatidest ega usaldusteenuse pakkuja väljastatud privaatvõtmetest just seepärast, et võtmed, mida kasutatakse hajusraamatutehnoloogiale tuginevas allkirjastamisprotsessis (olenevalt kasutaja eelistustest), väljastab protokoll otse kasutajale. Seega, erinevalt PKI-mudelist puudub hajusraamatutehnoloogia puhul vajadus usaldusväärse vahendaja või ametiasutuse järele, kes neid allkirjastamiseks vajalikke võtmeid keskselt väljastaks ja haldaks.

Nagu väitekirjas kirjeldatud, on PKI-mudel ja hajusraamatutehnoloogial põhinevaid süsteeme kasutavad allkirjastamisprotsessid tehniliselt üsna sarnased. Hajusraamatutehnoloogia kätkeb eri tehnoloogiaid, nagu krüptograafia, P2P-võrgustikud, konsensusmehhanism ja lingitud ajatempliteenus, kasutamata sealjuures tsentraliseeritud usaldusstruktuure, ent kasutades siiski paljuski sama tehnoloogiat kui PKI-mudelgi. Seda konteksti arvestades loob hajusraamatutehnoloogia tehniline seadistus detsentraliseeritud usalduse ja kontrollitava protokolli ilma, et oleks vaja kasutada LOTL-põhist tsentraliseeritud usaldusteenuse pakkujate süsteemi. See siiski ei tähenda, et kõikidele hajusraamatutehnoloogiat kasutavatele tarkade lepingute kasutajatele saaks kinnitada, et see protokoll on funktsionaalselt samaväärne eIDAS-e elektroonilise allkirja protokolli ja usaldussüsteemiga. See tähendab vaid seda, et eIDAS-e süsteem on kallutatud omistama kehtivust ja tunnustust vaid elektroonilistele allkirjadele, mis pärinevad usaldusteenuse pakkujatega seotud usaldussüsteemist ning seega vastavad eIDAS-es toodud nõuetele ja standarditele.

Väitekirjas toodud analüüs näitas, et ainus funktsioon, mida hajusraamatutehnoloogiale tuginevad targad hübriidlepingud ei täida, on allkirjaandja isikutuvastus. Samas puudub eIDAS-es nõue, et isikusamasuse seostamine allkirjaõigusliku isikuga peab olema allkirjastamistehnoloogia sisene võimekus ja et seda ei saa asendada lahendusega, mis suudab küll täita isikusamasuse tuvastamise funktsiooni, kuid on allkirjastamistehnoloogiast eraldiseisev. Alternatiivina kirjeldatud lahendusele võiks seadusandja kaaluda tehinguvormi ajutisi staatusi ehk tehinguvormi fluiidsust, mille alusel vorm muutub, kui allkirja seos isikuga on tekkinud. Selline liberaliseerimine tuleks heaks kiita ka seetõttu, et mudelid, mis sõltuvad tsentraliseeritud isikusamasuse tuvastamise funktsioonist, on sisemiselt haavatavad ühe sisemise tõrkepunkti (nt LOTL) olemasolu tõttu. Arvestades et analoogmaailmas lubatakse isikutevahelistes tehingutes anonüümseid või pseudonüümseid tehinguid, oleks ehk aeg võrdsustada need võimalused ka digimaailmas, muutes kehtivat õigust nii, et see võimaldaks esmaste mündipakkumiste tarkade lepingute kasutajatel jääda anonüümseks või kasutada pseudonüümi, ent siiski sõlmida elektroonilises vormis lepinguid.

Ülaltoodut arvestades leiab autor, et tehnoloogianeutraalsuse põhimõttega on vastuolus igasugune õigusakt, mis ei taga mõju samaväärsust funktsionaalselt samaväärsetele alternatiivsetele süsteemidele.

4. Tuvastatud eelarvamused

Kokkuvõtteks näitavad hajusraamatutehnoloogia kasutusjuhud, et kehtiv õigus võib diskrimineerida innovaatilisi lahendusi ootamatutel viisidel: kohelda tehnoloogia väljundit (bitimünti) diskrimineerivalt väljaandmisprotsessi tõttu (tsentraliseeritud *vs.* hajutatud), mitte omistada mõju samaväärsust funktsionaalselt samaväärsele tehnoloogilisele lahendusele põhjusel, et puudub tsentraliseeritud vahendaja või et usaldusallikas on midagi muud kui LOTL-i nimekirjas olevad usaldusteenuse pakkujad. Seetõttu, niikaua kui riigivõim ei püüa välja selgitada kehtiva õiguse negatiivset mõju uuele tehnoloogiale, ei ole selline diskrimineerimine, kallutatus ega eelarvamused nähtavad, sest õigusnormi tekst võib olla tehnoloogiast sõltumatu (osanike nimekirja kasutusjuht) või grammatiliselt tehnoloogianeutraalne (eIDAS), ent neutraalse terminoloogia taga peituvad tegelikkuses nõuded, mis on koostatud spetsiifilise tehnoloogia kujundatud tegelikkuse alusel (avaliku võtme taristu mudel) ja mis ei taga mõju samaväärsust funktsionaalselt samaväärsetele tehnoloogiatele, kuna need ei kasuta keskset vahendajat (notar, väärtpaberite keskregister, LOTL-i usaldusteenuse pakkuja).

Seadusandjad, kes kasutavad uue tehnoloogia saabumisel „ootame-vaatame“ või „kehtiva õiguse kohaldamise“ strateegiat, peaksid võtma seda järeldust hoiatusena, sest tehnoloogianeutraalsuse põhimõtte järgi peavad nad tegema märkimisväärseid jõupingutusi, et püüda mõista seda uut tehnoloogiat ja selle laiemat konteksti, ning kohandama vähemasti kehtiva õiguse tõlgenduse selliseks, et see oleks kooskõlas tehnoloogianeutraalsuse põhimõttega.

PUBLICATIONS

CURRICULUM VITAE IN ENGLISH

Name: Anne Veerpalu
Date of birth: 3 May 1977
E-mail: anne.veerpalu@techxlegal.com

Career

2020–present	attorney-at-law and partner of TECH x LEGAL Law Firm
2015–present	visiting lecturer of the IT Law Master's programme at the University of Tartu
2001–2020	numerous positions as a practicing lawyer and attorney in law firms and consulting companies

Education

2016–present	Doctoral studies, Information Technology Law, School of Law, University of Tartu, Estonia
2015–2016	MA in Information Technology Law, School of Law, University of Tartu, Estonia
2001–2006	MA in Business Administration, Estonian Business School, Estonia
1998–2000	MA in Public International Law, Faculty of Law, Helsinki University, Finland
1995–1998	BA in Social Sciences (Law), Faculty of Law, University of Tartu, Estonia

Publications

Article I	Anne Veerpalu, 'Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of *De Voogd* and *Hedqvist*' (2018) 11/2 Baltic Journal of Law & Politics, pp. 61–94.
Article II	Anne Veerpalu, 'Shareholder ledger using distributed ledger technology: the Estonian perspective' (2019) 13/2, Masaryk University Journal of Law and Technology, pp. 277−310.
Article III	Anne Veerpalu, Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva, Alex Norta, 'The hybrid smart-contract agreement challenge to European electronic signature regulation' (2020), 28/1 International Journal of Law and Information Technology, pp. 39–84.
Article IV	Anne Veerpalu, 'Functional equivalence – an exploration through shortcomings to solutions' (2019) 12/2 Baltic Journal of Law & Politics, pp. 135–163.
Article V	Anne Veerpalu, 'Computational Law & Blockchain Festival DISCUSS Symposium Reports: Tartu Node' (2018) 1 Stanford Journal of Blockchain Law & Policy. June 24, 2018.
Article VI	Anne Veerpalu; Eduardo da Cruz Rodrigues e Silva, 'Hitting the white ball: the technology neutrality principle and blockchain based application' (2019). 15/2 Indian Journal of Law and Technology, pp. 300–320.

ELULOOKIRJELDUS

Nimi: Anne Veerpalu
Sünniaeg: 3. mai 1977
E-mail: anne.veerpalu@techxlegal.com

Töökäik

2020–praegu	vandeadvokaat ja partner, TECH x LEGAL Advokaadibüroo OÜ
2015–praegu	külalislektor infotehnoloogiaõiguse magistriprogramm, õigusteaduskond, sotsiaalteaduste valdkond, Tartu Ülikool, Eesti
2001–2020	jurist, advokaat ja vandeadvokaat erinevates advokaadibüroodes ja konsultatsioonitevõtetes

Hariduskäik

2016–praegu	doktoriõpe, infotehnoloogiaõigus, õigusteaduskond, sotsiaalteaduste valdkond, Tartu Ülikool, Eesti
2015–2016	magistriõpe, infotehnoloogiaõigus, õigusteaduskond, sotsiaalteaduste valdkond, Tartu Ülikool, Eesti
2001–2006	magistriõpe rahvusvaheline ärijuhtimine, Estonian Business School, Eesti
1998–2000	magistriõpe avalik rahvusvaheline õigus, õigusteaduskond, Helsingi ülikool, Soome
1995–1998	bakalauruseõpe, sotsiaalteadused (õigus) õigusteaduskond, sotsiaalteaduste valdkond, Tartu Ülikool, Eesti

Publikatsioonid

Artikkel I	Anne Veerpalu, 'Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of *De Voogd* and *Hedqvist*' (2018) 11/2 Baltic Journal of Law & Politics, pp. 61–94.
Artikkel II	Anne Veerpalu, 'Shareholder ledger using distributed ledger technology: the Estonian perspective' (2019) 13/2, Masaryk University Journal of Law and Technology, pp. 277−310.
Artikkel III	Anne Veerpalu, Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva, Alex Norta, 'The hybrid smart-contract agreement challenge to European electronic signature regulation' (2020), 28/1 International Journal of Law and Information Technology, pp. 39–84.
Artikkel IV	Anne Veerpalu, 'Functional equivalence – an exploration through shortcomings to solutions' (2019) 12/2 Baltic Journal of Law & Politics, pp. 135–163.
Artikkel V	Anne Veerpalu, 'Computational Law & Blockchain Festival DISCUSS Symposium Reports: Tartu Node' (2018) 1 Stanford Journal of Blockchain Law & Policy. June 24, 2018.
Artikkel VI	Anne Veerpalu; Eduardo da Cruz Rodrigues e Silva, 'Hitting the white ball: the technology neutrality principle and blockchain based application' (2019). 15/2 Indian Journal of Law and Technology, pp. 300–320.

DISSERTATIONES IURIDICAE UNIVERSITATIS TARTUENSIS

1. **Херберт Линдмяэ**. Управление проведением судебных экспертиз и его эффективность в уголовном судопроизводстве. Тарту, 1991.
2. **Peep Pruks**. Strafprozesse: Wissenschaftliche "Lügendetektion". (Instrumentaldiagnostik der emotionalen Spannung und ihre Anwendungsmöglichkeiten in Strafprozess). Tartu, 1991.
3 **Marju Luts**. Juhuslik ja isamaaline: F. G. v. Bunge provintsiaalõigusteadus. Tartu, 2000.
4. **Gaabriel Tavits**. Tööõiguse rakendusala määratlemine töötaja, tööandja ja töölepingu mõistete abil. Tartu, 2001.
5. **Merle Muda**. Töötajate õiguste kaitse tööandja tegevuse ümberkorraldamisel. Tartu, 2001.
6. **Margus Kingisepp**. Kahjuhüvitis postmodernses deliktiõiguses. Tartu, 2002.
7. **Vallo Olle**. Kohaliku omavalitsuse teostamine vahetu demokraatia vormis: kohalik rahvaalgatus ja rahvahääletus. Tartu, 2002.
8. **Irene Kull**. Hea usu põhimõte kaasaegses lepinguõiguses. Tartu, 2002.
9. **Jüri Saar**. Õigusvastane käitumine alaealisena ja kriminaalsed karjäärid (Eesti 1985–1999 longituuduurimuse andmetel). Tartu, 2003.
10. **Julia Laffranque**. Kohtuniku eriarvamus. Selle võimalikkus ja vajalikkus Eesti Vabariigi Riigikohtus ja Euroopa Kohtus. Tartu, 2003.
11. **Hannes Veinla**. Ettevaatusprintsiip keskkonnaõiguses. Tartu, 2004.
12. **Kalev Saare**. Eraõigusliku juriidilise isiku õigussubjektsuse piiritlemine. Tartu, 2004.
13. **Meris Sillaots**. Kokkuleppemenetlus kriminaalmenetluses. Tartu, 2004.
14. **Mario Rosentau**. Õiguse olemus: sotsiaalse käitumise funktsionaalne programm. Tartu, 2004.
15. **Ants Nõmper**. Open consent – a new form of informed consent for population genetic databases. Tartu, 2005.
16. **Janno Lahe**. Süü deliktiõiguses. Tartu, 2005.
17. **Priit Pikamäe**. Tahtluse struktuur. Tahtlus kui koosseisupäraste asjaolude teadmine. Tartu, 2006.
18. **Ivo Pilving**. Haldusakti siduvus. Uurimus kehtiva haldusakti õiguslikust tähendusest rõhuasetusega avalik-õiguslikel lubadel. Tartu, 2006.
19. **Karin Sein**. Ettenähtavus ja rikutud kohustuse eesmärk kui lepingulise kahjuhüvitise piiramise alused. Tartu, 2007.
20. **Mart Susi**. Õigus tõhusale menetlusele enda kaitseks – Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsiooni artikkel 13 Euroopa Inimõiguste Kohtu dünaamilises käsitluses. Tartu, 2008.
21. **Carri Ginter**. Application of principles of European Law in the supreme court of Estonia. Tartu, 2008.
22. **Villu Kõve**. Varaliste tehingute süsteem Eestis. Tartu, 2009.

23. **Katri Paas**. Implications of Smallness of an Economy on Merger Control. Tartu, 2009.
24. **Anneli Alekand**. Proportsionaalsuse printsiip põhiõiguste riive mõõdupuuna täitemenetluses. Tartu, 2009.
25. **Aleksei Kelli**. Developments of the Estonian Intellectual Property System to Meet the Challenges of the Knowledge-based Economy. Tartu, 2009.
26. **Merike Ristikivi**. Latin terms in the Estonian legal language: form, meaning and influences. Tartu, 2009.
27. **Mari Ann Simovart**. Lepinguvabaduse piirid riigihankes: Euroopa Liidu hankeõiguse mõju Eesti eraõigusele. Tartu, 2010.
28. **Priidu Pärna**. Korteriomanike ühisus: piiritlemine, õigusvõime, vastutus. Tartu, 2010.
29. **René Värk**. Riikide enesekaitse ja kollektiivse julgeolekusüsteemi võimalikkusest mitteriiklike terroristlike rühmituste kontekstis. Tartu, 2011.
30. **Paavo Randma**. Organisatsiooniline teovalitsemine – *täideviija täideviija taga* kontseptsioon teoorias ja selle rakendamine praktikas. Tartu, 2011.
31. **Urmas Volens**. Usaldusvastutus kui iseseisev vastutussüsteem ja selle avaldumisvormid. Tartu, 2011.
32. **Margit Vutt**. Aktsionäri derivatiivnõue kui õiguskaitsevahend ja ühingujuhtimise abinõu. Tartu, 2011.
33. **Hesi Siimets-Gross**. Das „Liv-, Est- und Curlaendische Privatrecht" (1864/65) und das römische Recht im Baltikum. Tartu, 2011.
34. **Andres Vutt**. Legal capital rules as a measure for creditor and shareholder protection. Tartu, 2011.
35. **Eneken Tikk**. Comprehensive legal approach to cyber security. Tartu, 2011.
36. **Silvia Kaugia**. Õigusteadvuse olemus ja arengudeterminandid. Tartu, 2011.
37. **Kadri Siibak**. Pangandussüsteemi usaldusväärsuse tagamine ja teabekohustuste määratlemine finantsteenuste lepingutes. Tartu, 2011.
38. **Signe Viimsalu**. The meaning and functioning of secondary insolvency proceedings. Tartu, 2011.
39. **Ingrid Ulst**. Balancing the rights of consumers and service providers in electronic retail lending in Estonia. Tartu, 2011.
40. **Priit Manavald**. Maksejõuetusõigusliku regulatsiooni valikuvõimaluste majanduslik põhjendamine. Tartu, 2011, 193 lk.
41. **Anneli Soo**. Remedies against ineffectiveness of defense counsel. Judicial supervision over the performance of defense counsel in Estonian criminal proceedings. Tartu, 2011, 282 p.
42. **Arnold Sinisalu**. Mõjutustegevuse piirid rahvusvahelises õiguses. Tartu, 2012, 277 lk.
43. **Kaspar Lind**. Käibemaksupettused ja nende tõkestamine. Tartu, 2012, 155 lk.
44. **Berit Aaviksoo**. Riigi otsustusruumi ahenemine: kodakondsus nüüdisaegses Euroopas. Tartu, 2013, 368 lk.
45. **Kai Kullerkupp**. Vallasomandi üleandmine. Õigusdogmaatiline raamistik ja kujundusvõimalused. Tartu, 2013, 398 lk.

46. **Iko Nõmm**. Käibekohustuse rikkumisel põhinev deliktiõiguslik vastutus. Tartu, 2013, 212 lk.
47. **Piia Kalamees**. Hinna alandamine õiguskaitsevahendite süsteemis. Tartu, 2013, 232 lk.
48. **Irina Nossova**. Russia's international legal claims in its adjacent seas: the realm of sea as extension of Sovereignty. Tartu, 2013, 205 p.
49. **Age Värv**. Kulutuste kondiktsioon: teise isiku esemele tehtud kulutuste hüvitamine alusetu rikastumise õiguses. Tartu, 2013, 273 lk.
50. **Elise Vasamäe**. Autoriõiguste ja autoriõigusega kaasnevate õiguste jätkusuutlik kollektiivne teostamine. Tartu, 2014, 308 lk.
51. **Marko Kairjak**. Keerukuse redutseerimine Eesti õiguses karistusseadustiku § 217^2 objektiivse koosseisu relatiivsete õigusmõistete sisustamise näitel. Tartu, 2015, 179 lk.
52. **Kadi Pärnits**. Kollektiivlepingu roll ja regulatsioon nüüdisaegsetes töösuhetes. Tartu, 2015, 179 lk.
53. **Leonid Tolstov**. Tort liability of the director to company's creditors. Tartu, 2015, 169 p.
54. **Janar Jäätma**. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Tartu, 2015, 242 lk.
55. **Katre Luhamaa**. Universal Human Rights in National Contexts: Application of International Rights of the Child in Estonia, Finland and Russia. Tartu, 2015, 217 p.
56. **Mait Laaring**. Eesti korrakaitseõigus ohuennetusõigusena. Tartu, 2015, 267 lk.
57. **Priit Kama**. Valduse ja kohtuliku registri kande publitsiteet Eesti eraõiguses. Tartu, 2016, 194 lk.
58. **Kristel Degener**. Abikaasade vara juurdekasvu tasaarvestuse varasuhe. Tartu, 2016, 242 lk.
59. **Olavi-Jüri Luik**. The application of principles of European insurance contract law to policyholders of the Baltic states: A measure for the protection of policyholders. Tartu, 2016, 228 p.
60. **Kaido Künnapas**. Maksukohustuse täitmise preventiivne tagamine enne maksukohustuse tuvastamist: ettevaatuspõhimõte maksumenetluses.Tartu, 2016, 388 lk.
61. **Eve Fink**. Õiguspärase ootuse kaitse põhimõtte eeldused ja piirid Euroopa liidu õiguses. Tartu, 2016, 245 lk.
62. **Arsi Pavelts**. Kahju hüvitamise nõue täitmise asemel ostja õiguste näitel. Tartu, 2017, 414 lk.
63. **Anna-Maria Osula**. Remote search and seizure of extraterritorial data. Tartu, 2017, 219 p.
64. **Alexander Lott**. The Estonian straits. Exceptions to the strait regime of innocent or transit passage. Tartu, 2017, 259 p.
65. **Dina Sõritsa**. The Health-care Provider's Civil Liability in Cases of Prenatal Damages. Tartu, 2017, 365 p.

66. **Einar Vene**. Ajaline faktor halduskohtumenetluses tühistamis- ja kohustamiskaebuse lahendamist ning rahuldamist mõjutava tegurina. Tartu, 2017, 294 lk.
67. **Laura Feldmanis**. Süüteokatsest loobumise instituudi põhjendus ja kohaldatavuse piirid kuritegelikule eeltegevusele. Tartu, 2017, 292 lk.
68. **Margit Piirman**. Inimese pluripotentsete tüvirakkudega seotud leiutiste patentimise piirangud vastuolu tõttu avaliku korra ja moraaliga (Eesti patendiõiguse näitel). Tartu, 2018, 246 lk.
69. **Kerttu Mäger**. The Taming of the Shrew: Understanding the Impact of the Council of Europe's Human Rights Standards on the State Practice of Russia. Tartu, 2018, 305 p.
70. **Tambet Grauberg**. Õiguse kuritarvitamise keelamise põhimõte: Euroopa Kohtu seisukohtade mõju liikmesriigi maksuõigusele. Tartu, 2018, 277 lk.
71. **Maarja Torga**. The Conflict of Conflict Rules – the Relationship between European Regulations on Private International Law and Estonian Legal Assistance Treaties Concluded with Third States. Tartu, 2019, 252 p.
72. **Liina Reisberg**. Semiotic model for the interpretation of undefined legal concepts and filling legal gaps. Tartu, 2019, 232 p.
73. **Mari Schihalejev**. Debtor-Related Creditors' Claims in Insolvency Proceedings. Tartu, 2019, 137 p.
74. **Ragne Piir**. Mandatory Norms in the Context of Estonian and European International Contract Law: The Examples of Consumers and Posted Workers. Tartu, 2019, 117 p.
75. **Madis Ernits**. Constitution as a system. Tartu, 2019, 201 p.
76. **Kärt Pormeister**. Transparency in relation to the data subject in genetic research – an analysis on the example of Estonia. Tartu, 2019, 184 p.
77. **Annika Talmar**. Ensuring respect for International Humanitarian Law 70 years after the adoption of the Geneva Conventions of 1949. Tartu, 2020, 286 p.
78. **Liliia Oprysk**. Reconciling the Material and Immaterial Dissemination Rights in the Light of the Developments under the EU Copyright *Acquis.* Tartu, 2020, 397 p.
79. **Katrin Sepp**. Legal Arrangements in Estonian Law Similar to Family Trusts. Tartu, 2020, 163 p.
80. **Taivo Liivak**. Tort Liability for Damage Caused by Self-driving Vehicles under Estonian Law. Tartu, 2020, 206 p.