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

Jani Ultamo

Regulatory Approach to Implement the FATF Travel Rule on Transfers of Crypto-Assets – Fitting Together the Need for Standardisation and the Principle of Technology Neutrality

Master's thesis
Programme HAJM08/21, specialisation Law and Technology

Supervisor: Thomas Hoffmann, Dr. iur.
Co-supervisor: Henrik Mägi, LL.M.

Tallinn 2022

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 19 941 words from the introduction to the end of conclusion.

Jani Ultamo ……

(signature, date)

Student code: 214197HAJM

Student e-mail address: jani.ultamo@ultamo.fi

Supervisor: Thomas Hoffmann, PhD:

The paper conforms to requirements in force

……

(signature, date)

Co-supervisor: Henrik Mägi, LL.M.:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT 4
ABBREVIATIONS 5
INTRODUCTION 6
1. THE FATF TRAVEL RULE 12
1.1. Background 12
1.2. The requirements set out in the FATF Travel rule 14
1.3. The implementation of the Travel rule 17
2. THE PRINCIPLE OF TECHNOLOGY NEUTRALITY 23
2.1. Background of the principle 23
2.2. Meaning and object of the principle 25
2.3. Functional equivalence and effects equivalence 29
2.4. FATF Travel rule and technology neutrality 33
3. STANDARDISATION 35
3.1. Standard 35
3.2. Creation of standards 37
3.3. Standardisation by private sector 38
3.4. Standardisation and technology-neutrality 41
3.5. The necessary steps to achieve standard 45
3.5.1. Creator of standard 45
3.5.2. Technology-neutral standard for Travel rule technology 49
4. NATIONAL REGULATOR'S RISK-BASED APPROACH TO TRAVEL RULE 52
4.1 Possibilities for a national regulator 52
4.2 Supranational consensus 56
4.3 Risk-based approach for interim period 57
CONCLUSION 62
LIST OF REFERENCES 66
APPENDICES 72
Appendix 1. Non-exclusive licence 73

ABSTRACT

This thesis introduces the FATF Travel rule, it's background and its implications for virtual asset service providers and national regulators. The thesis studies the present status of implementation of the Travel rule and the problem arising out of the lack of common global technical standard to comply with the Travel rule. The thesis analyses the research topic in the crypto assets, and do not take into consideration other kinds of digital assets

The thesis then introduces the principle of technology neutrality and studies its meaning and implications on the standardisation process. The aim of the thesis is to study how a national regulator should approach the question of implementing Travel rule and which options does the regulator have bearing in mind that a state bound by FATF Recommendations should implement the Travel rule on national regulation, but the crypto industry on the other hand do not have a common way to implement the Travel rule yet on global scale. The author then analyses regulator's possibilities on implementing the Travel rule and setting standard for the Travel rule compliance in the light of the principle of technology neutrality.

The author comes into conclusion that transnational co-operation is required in order to create the necessary standard and that national regulator's possibilities to set standard, or require full compliance with the Travel rule before a common global standard is created, are very limited. Finally this thesis provides suggestions for a national regulator in implementing the Travel rule during interim period while common global standard for Travel rule compliance do not exist yet.

Keywords: Anti-money laundering, technology neutrality, cryptocurrency, virtual asset

ABBREVIATIONS

AML – Anti-Money Laundering
AMLD – Anti-Money Laundering Directive
EU – The European Union
FATF – The Financial Action Task Force
FIU – Financial Intelligence Unit
INR – (FATF's) Imperative Note
SSO – Standard setting organization
TFEU – The Treaty of Functioning of the European Union
VASP – Virtual Asset Service Provider

INTRODUCTION

Cryptocurrencies are math-based virtual currencies that are protected by cryptography[1], and which circulation is enabled by "decentralized, anonymous transactions that do not depend on central banks or governments"[2]. Technologically cryptocurrencies are based on blockchain technology. The use of cryptocurrencies for different purposes has seen a remarkable rise during the recent years.[3] As cryptocurrencies are comparatively new phenomenon (the first initiative for cryptocurrencies was a white paper that was release by pseudonym Satoshi Nakamoto only in 2008[4]), we have probably only seen a small sample of the possibilities blockchain technologies and cryptocurrencies may offer the financial industry in the future. As usual with innovations, the regulation follows behind the practise and thus the legal framework for cryptocurrencies is only developing yet.

Traditionally transfer of funds between financial institutions are conducted on so called fiat-currencies (like Euro, US Dollar and GB Pounds, for example). Fiat-currencies are usually regulated by central authorities and accepted as government-issued currencies by states. In contrast, cryptocurrencies like Bitcoin are based on peer-to-peer structure and not on governments or banks structural support.[5] Compared to the traditional transactions between traditional financial institutions, like banks, where the payer and receiver of transferred funds as well as the owner of those funds are identified, but the records of the transactions are hold by the banks, in cryptocurrency transactions the identities of the payer and receiver as well as that of the owner of the funds are anonymized by the system, but records of all the transactions are public[6]. The individuals taking part in cryptocurrency transactions are not identified by names in the

[1] FATF (2014). Virtual Currencies. Key Definitions and Potential AML/CFT Risks. Financial Action Task Force. June 2014. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 30 March 2022, 5.

[2] Luther, W. J. (2016). Cryptocurrencies, Network effects, and switching costs. Contemporary Economic Policy, 34(3), 553–571, referenced in Lee, M., Frank, L., IJsselsteijn, W. (2021). Brokerbot: A Cryptocurrency Chatbot in the Social-technical Gap of Trust. Computer Supported Cooperative Work, 30(1), 79-117. 82.

[3] For example, Foley, S., Karlsen, J., Putniņš, T. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? The Review of Financial Studies, 32(5), 1798-1853, 1798-1799.

[4] For example, Luther, W. (2016). Bitcoin and the Future of Digital Payments. The Independent Review (Oakland, Calif.), 20(3), 397-404, 397; and Aiyar, K., Halgamuge, M. N., Mason, N. (2021). Blockchain and Cryptocurrencies: Legal and Ethical Considerations. Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector. IGI Global, March 2021, 132-152, 133.

[5] Donmez, C., Sen, D., Dereli, A., Horasan, M., Yildiz, C., Kaplan Donmez, N. (2021). An Investigation of Fiat Characterization and Evolutionary Dynamics of the Cryptocurrency Market. *SAGE Open, 11*(1), 2.

[6] Lee, M., Frank, L., IJsselsteijn, W. (2021). Brokerbot: A Cryptocurrency Chatbot in the Social-technical Gap of Trust. Computer Supported Cooperative Work, 30(1), 79-117, 82.

blockchain, but by so called public keys, which are alphanumeric characters created by complex algorithm.[7] Thus, the identity of an individual taking part of the transaction stays anonymous and the individual can only access the funds received from transactions by so called private keys, which do not identify the individual behind that private key either.[8] Transactions on cryptocurrencies, like Bitcoin, can also be operated without any involvement of an intermediary (and thus, without the control financial institutions and the authorities controlling them) unlike fiat-transactions between banks.[9] These fundamental differences, together with few additional advantages, are key features that have made cryptocurrencies attractive vehicle for criminal purposes as it is much easier for a payer or a receiver of a cryptocurrency payment to keep his/her identity anonymous than when using a fiat-currency payment intermediated by bank.[10]

Due to the cryptocurrencies pseudonymous and decentralized nature, it is difficult to measure the amount of illegal activities associated to cryptocurrencies, but on their study Foley and others (2019) estimated that nearly half of transactions that involved bitcoin (amounting to 76 billion US dollars a year during the researched period from January 2009 to April 2017) was associated with illegal activities[11].

Widely speaking, many of the illegal activities associated with cryptocurrencies can be referred to as money-laundering. Cryptocurrencies can be utilized in money-laundering activities in countless ways. Through the pseudonymity of transactions cryptocurrencies basically offer a way to circumvent any government prohibitions of trade[12] and otherwise avoid regulation[13]. The most obvious way that criminals utilize cryptocurrencies in money-laundering is taking advantage of the fact that through the decentralized structure of cryptocurrencies, criminals are able to bypass the centralized control over transactions that banks have over traditional fund transfers. For

[7] Lee, J., Long, A., McRae, M., Steiner, J., Handler, S. (2015). Bitcoin Basics: A Primer on Virtual Currencies. Business Law International, 16(1), 21-48, 43.
[8] Turner, A., Irwin, A. (2018). Bitcoin transactions: A digital discovery of illicit activity on the blockchain. Journal of Financial Crime, 25(1), 109-130, 110.
[9] Soana, G. (2022). Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry? Economic Notes - Monte Paschi Siena, 51(1), 2.
[10] Gonzálvez-Gallego, N., Pérez-Cárceles, M. (2021). Does goodness of governance dissuade citizens from using cryptocurrencies? Economics & Sociology, 14(1), 11-27, 11.
[11] Foley, S., Karlsen, J., Putniņš, T. (2019), s*upra nota 3*, 1800, 1808.
[12] Bagus, P., De la Horra, L. (2021). An ethical defense of cryptocurrencies. Business Ethics, the Environment & Responsibility, 30 (3), 423– 431, 427.
[13] Gonzálvez-Gallego, N., Pérez-Cárceles, M. (2021), *supra nota* 10, 15.

example, illegal payments (for example, funds originating from drug sales[14] or ransom payments[15]) can be executed on cryptocurrencies, or illegal funds in fiat-currencies can be transferred to cryptocurrencies to fade the origin of the funds through one or several anonymous transactions by cryptocurrencies and then, for example, change the received cryptocurrencies back to fiat-currencies or use the cryptocurrencies, originating from illegal activities or funds, to finance purchases or otherwise integrating the funds back to "mainstream economic activity" such as investments. Also, the possibilities, that cryptocurrencies offer, to easily transfer funds cross state borders can be utilized in the money-laundering process, and for example to transfer funds to offshore accounts that further obscure the origin of the funds.[16]

The problematics described above in this chapter has proposed a new challenge for regulators around the World: how to create a regulatory framework, or develop the current regulatory framework, so that we can enjoy the benefits provided by blockchain technology and cryptocurrencies, but still mitigate the potential dangers the newish technology bring about.[17] On the other hand, regulators have the challenge of constantly evolving technology and business models, that are especially present in the crypto industry: any existing and new regulation should be able to be applied to constantly evolving market.[18] As the idea behind cryptocurrencies is extremely libertarian, it is a good question though, whether cryptocurrencies can be enough regulated without breaking the foundations of it. Due to the aspiration towards totally free and open currency market, even views, that transactions in cryptocurrencies should not be regulated at all, has been presented.[19] Thus, regulating cryptocurrencies is balancing between the freedoms of the users and other market participants and the libertarian values behind the cryptocurrencies on one side, and the request to secure the financial market, society and the users of cryptocurrencies on the other side.

[14] FATF (2021). Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. July 2021. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf, 12 December 2021, 25.
[15] For example, Gromek, M. (2020, October 31). Ransom Hackers In Finland Are Using Psychotherapy Medical Records As Ammunition. Forbes. Retrieved from https://www.forbes.com/sites/michalgromek/2020/10/31/ransom-hackers-in-finland-are-using-psychotherapy-medical-records-as-ammunition/?sh=3272f3fa2f2e, 13 December 2021.
[16] Albrecht, C., Duffin, K., Hawkins, S., Morales Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210-216, 211.
[17] Reijers, W., Coeckelbergh, M. (2016). The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. Philosophy & Technology, 31(1), 103-130, 127.
[18] Naheem, M. (2018). Regulating virtual currencies, the challenges of applying fiat currency laws to digital technology services. Journal of Financial Crime, 25(2), 562-575, 563.
[19] Kiviat, T. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal, 65*(3), 569-608, 587.

Due to the risks related to cryptocurrencies, as well as the difficulties to regulate and control something that happens in decentralized blockchain, different jurisdictions have taken different approach towards cryptocurrencies.[20] European Union has decided to create own legal framework for cryptocurrency industry with an aim to support utilizing the good sides of this innovation in financial market by adopting European Commission's proposal for a regulation on Markets in Crypto-assets ("MiCA")[21] and adopting cryptocurrencies in the already existing anti-money laundering framework. However, the blockchain technology utilized by cryptocurrencies challenges the European anti-money laundering regulation in a new way. As described above in this chapter, there are some fundamental structural issues that distinguishes transactions in cryptocurrencies, based on blockchain technology, from transactions in fiat-currencies. Dupuis[22] as well as Houben and Snyers[23] have argued that the present anti-money laundering framework (the 5th AMLD[24]) does not address the anonyme nature of cryptocurrencies enough. The present European Union anti-money laundering framework leaves it to a great extent to the national regulators, financial intelligence units and regulated entities to decide how to deal in practise with the money-laundering risks and problems arising from cryptocurrencies.

The Financial Action Task Force (FATF) has taken steps forward to address the money-laundering issues related to cryptocurrencies by introducing virtual asset service providers (VASPs) as subjects to the FATF Recommendations in it's update on October 2018 and updating its Imperative Notes (IRNs) in June 2019 by pointing certain FATF Recommendations that should be applied to VASPs[25]. One of the requirements that FATF by the referred updates introduced to VASPs is especially aiming to solve the AML risks arising from the anonymity of cryptocurrency

[20] Panova, O., Leheza, Y., Ivanytsia, A., Marchenko, V., Oliukha, V. (2019). International Models of Legal Regulation and Ethics of Cryptocurrency Use: Country Review. Journal of Legal, Ethical and Regulatory Issues, 22 (2), 2-5.
[21] European Commission's Proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. 24 September 2021. COM/2020/593.
[22] Dupuis, D., Gleason, K. (2020). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. Journal of Financial Crime, 28(1), 60-74, 61.
[23] Houben, R., Snyers, A. (2018). Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion. Study requested by the TAX3 committee. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, 9. Retrieved from www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, 2 April 2022.
[24] 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 (the 5th AML Directive or AMLD) PE/72/2017/REV/1, OJ L 156, 19.6.2018, 43 – 74.
[25] FATF (2012-2021), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 136. Retrieved from www.fatf-gafi.org/recommendations.html, 29 December 2021.

transactions, namely the so called “Travel rule”, which requires certain originator and beneficiary information to be transferred between obliged entities (financial institutions and VASPs) that takes part on transfer of funds, even when such transfer takes place in cryptocurrency. The introduction of the Travel rule has caused technical challenge for the crypto industry, because neither the technology on which transfers of for example bitcoins are yet executed nor the yet scarce industry standards among the crypto industry include a common technical way to transfer the information that compliance with Travel rule would require.

Now the national regulators of all jurisdictions bound by the FATF Recommendations are expected to implement in their national regulative framework requirements that are necessary in order to ensure that VASPs in their jurisdiction shall comply with the Travel rule. But as there is no common global technology for VASPs to transfer the necessary information between themselves, the national regulators are sceptical to implement the Travel rule to their regulative frameworks. To solve this problem a common standard on the information transfers between the VASPs should be created. This could be done, inter alia, by a regulation, that would set out certain technological standard that would be applied to the transferring of the necessary information.

However, the principle of technology neutrality that is applied by the regulators in the European Union and its Member States, would contradict with a regulator determining which technologies are used to achieve goals such as the FATF Recommendations. According to this principle it should be the market, and not regulation or state, that decides which technologies will succeed on different industries or businesses.[26]

As cryptocurrencies do not technically rely on traditional banking infrastructures and central banks, cryptocurrencies, at least theoretically, do no encounter state borders. Thus, when considering the possibilities to regulate cryptocurrencies and crypto industry, we must understand that the money-laundering risks related to cryptocurrencies are global.[27] This means that even though some standard on transferring information would be set on national level, or even at European Union level, it would not be enough to solve the problem. Instead, just as in traditional banking industry, framework and certain standardization is needed on global level. In respect to

[26] Kamecke, U., Körber, T. (2008). Technology neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood. European Competition Law Review, 29(5), 330-337, 331-337.
[27] Gonzálvez-Gallego, N., Pérez-Cárceles, M. (2021), *supra nota* 10, 16.

money laundering issues related to cryptocurrencies, FATF have stated that jurisdictional arbitrage (service providers taking advantage of discrepancies in the legal framework between different jurisdictions) is a growing problem as there is still large caps on global scale in implementing necessary regulative framework for virtual currency services.[28] As certain jurisdictions take steps to implement the Travel rule, while other jurisdictions stays waiting for industry standards to be developed, this will probably grow the problem of jurisdictional arbitrage, at least for limited period of time.

The pressure for national regulators to implement Travel rule in regulation on national level and the need to standardise the transferring of the originator and beneficiary information between VASPs on global level, and the collision of these needs with the principle of technology neutrality is the main question that will be analysed in this study. The author will study the problematics from a national regulators viewpoint taking into consideration the obligation of a jurisdiction to follow the FATF Recommendations while considering the other interests that regulators have – especially the need to keep the legal framework competitive, fair and level for VASPs. The study aims to find out, how a national regulator of an EU Member State should implement the Travel rule into its national regulation so that the Member State would duly fill its obligations arising out of the FATF Recommendations, but also follow the principle of technology neutrality and keep the regulative environment in that Member State fair and level for different kind of technologies and obliged entities.

For the sake of clarity, it is noted that FATF uses in its Recommendations and Imperative Notes (later "INR") term "virtual asset service provider" (VASP) and refers to "virtual assets", which terms are used throughout this study also. The term "virtual asset" refers to a wide variety of digital assets. Cryptocurrencies (also referred to as "crypto assets") are a subcategory of virtual assets, but there can also be other kind of virtual assets than crypto assets.[29] Thus, also VASPs can provide services regarding other assets than crypto assets. However, this study analyses the research topic in the crypto assets and crypto asset service providers viewpoint, also when referring to "virtual assets" and VASPs, and do not take into consideration other kinds of digital assets.

[28] FATF (2021). Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota 14*, 25-26.

[29] IFAC (2020). Anti-money laundering: the basics. Retrieved from https://www.ifac.org/system/files/publications/files/Anti-Money-Laundering-The-Basics-Installment-7-Virtual-Assets.pdf, 4 May 2022; and FIN-FSA. Financial Supervisory Authority (2019). What do the terms virtual currency, cryptocurrency, crypto asset, ICO and wallet service mean? Retrieved from https://www.finanssivalvonta.fi/en/Consumer-protection/virtual-currencies/, 4 May 2022.

1. THE FATF TRAVEL RULE

1.1. Background

The roots of the so called "Travel rule" can even be traced as far back as to the Bank Secrecy Act in the United States in the 1970s. During the decades the principle developed together with general development of the banking industry and technology. The FATF Travel Rule in its current form was, however, introduced for traditional banks and financial institutions in the FATF's revised International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF Recommendations[30]) in 2012. However, at that time the rule did not apply to transfers made in cryptocurrencies and it was only in October 2018 when FATF updated the FATF Recommendations to cover also virtual asset service providers and the Travel rule set out in FATF Recommendation 16 came applicable to virtual asset service providers.[31]

The basis of the FATF Travel Rule is set out in the FATF Recommendation 16, according to which

> *Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.*
>
> *Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.*

[30] FATF (2012-2021). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, *supra nota 9*.

[31] Crypto.com (2020). FATF Travel Rule. A Brief Introduction, 5-13. Retrieved from https://assets.ctfassets.net/hfgyig42jimx/7ezqnx47HERbjVAofseOnf/792ed1f4c49384a65541aa4456cf037d/Crypto.com_Macro_Report_-_FATF_Travel_Rule.pdf, 29 January, 2022.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), relating to the prevention and suppression of terrorism and terrorist financing.

FATF introduced virtual assets and VASPs as subjects to the FATF recommendations, including the referred Recommendation 16, in its update on October 2018[32] by revising the Recommendation 15 with an addition of the following clause:

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

Later, in June 2019, FATF made an addition to the Interpretive Note (INR.) of Recommendation 15 in which it stated that the FATF Recommendations 10 to 21 applies to VASPs subject to certain conditions (INR. 15, paragraph 7).[33]

Even though, the FATF Recommendations are called "recommendations", they are in practice binding to most of the countries as over 200 jurisdictions around the World has committed to the FATF recommendations.[34] FATF conducts reviews on its members on an on-going basis to evaluate the level of their implementation of FATF Recommendations.[35] Also International Monetary Fund and the World Bank has assessment processes regarding the countries' implementation of the FATF recommendations.[36] As the reviews are published and non-compliance with the recommendations could even lead to a country being listed on some of FATF "negative lists" ("black list"[37] and "grey

[32] FATF (2012-2021). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, *supra nota 9,* 136.
[33] *Ibid*.
[34] Countries. FATF. Retrieved from https://www.fatf-gafi.org/countries/, 29 January 2022.
[35] Mutual Evaluations. FATF. Retrieved from https://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate), 29 January 2022.
[36] FATF (2012-2021). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, *supra nota 9.*
[37] FATF. High-Risk Jurisdictions subject to a Call for Action – October 2021. Retrieved from http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2021.html, 4 May 2022.

list"[38]), a country's failure to implement FATF Recommendations may damage a country's reputation as trustful partner in international trade and the possibilities for private businesses in that country to do business outside their origin country. Thus, the countries committed to the FATF Recommendations have strong endeavour to compliance with the recommendation.

1.2. The requirements set out in the FATF Travel rule

The Imperative Notes ("INR.") of the FATF Recommendations provides more detailed description of the meaning of the requirements set out in the Recommendations. According to the paragraph 7 of the INR. 15

> *With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:*
>
> *(a) R. 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.*
> *(b) R. 16 – Countries should ensure that* ***originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely****, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.*

The subparagraph (b) of the paragraph 7 of the INR. 15 embodies the essential contents of the Travel rule, namely that the originating VASPs should ***"obtain and hold required and accurate***

[38] FATF. Jurisdictions under Increased Monitoring – October 2021. Retrieved from http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html, 4 May 2022.

originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely".

The **originator information** and **required beneficiary information** in turn are listed in the paragraph 6 of the INR. 16 as follows:

> *(a) the name of the originator;*
>
> *(b) the originator account number where such an account is used to process the transaction;*
>
> *(c) the originator's address, or national identity number, or customer identification number, or date and place of birth;*
>
> *(d) the name of the beneficiary; and*
>
> *(e) the beneficiary account number where such an account is used to process the transaction.*

According to clarifying footnote of the paragraph 6 of the INR. 16, the customer identification number referred to in subparagraph (c) above *"refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number".*

What comes to account numbers referred to in subparagraphs (b) and (e) above, the paragraph 7 of the INR. 16 clarifies that *"in the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction".*

The list of originator and beneficiary information (a-e) referred to in the paragraph 6 of the INR. 16, is the information that the Travel rule requires originating VASPs to obtain, hold and submit to the beneficiary VASP or financial institution. When this information is obtained, held and submitted to the beneficiary VASP or financial institution immediately and securely, the Travel rule requirement is fulfilled by the originating VASP. Obtaining the required information from its client should not be difficult for the originator VASP as the originator VASP can set it as a prerequisite for executing any transfer that the originator provides this information. Also, when the required information is provided to the originating VASP, it does not constitute a problem for the originator VASP to hold this information as long as required. However, submitting this

information to the beneficiary VASP or financial institution is something that constitutes challenge for the VAPSs.

There are basically two main problems identified in respect to the originating VASPs requirement to submit the referred information to the beneficiary VAPS or financial institution.

Firstly, the originator VASP should be able to identify whether it is interacting with another VASP as a beneficiary VASP. Namely, when a transfer is conducted in blockchain, the beneficiary might be neither VASP nor financial institution. Instead, due to the special nature of the virtual currencies, a transfer between two wallets could be settled without any professional institution taking part, for example through distributed consensus on the blockchain between individual wallet addresses (unhosted wallets) alone[39], in which case the referred information would not be required by paragraph 6 of the INR. 16 to be sent to the beneficiary[40]. Indeed, when the paragraph 6 of the INR. 16 requires the referred information to be submitted securely and if the receiver of the transfer (and the information) is not a licensed institution, which operates under certain duty of care and confidentiality requirements, this might put the information submitted to it by the originator VASP to danger (which might be opposite to the obligation of the originator VASP to submit the necessary information securely).

As VASP as a concept is so recent origin, and yet only developing, there is no common global regulatory approach to VAPSs.[41] In some states, VAPSs are licensed entities, while in some other states not. Thus, there is also no possibility to have a global level listing of VASPs. In states, where VASPs are licensed institutions, there is some regulative framework for VAPSs and probably the VAPS supervised by local financial conduct authorities are listed by the authorities, while in many other states the regulative framework for VASPs, as well the listing of VAPSs, do not exist.

Another problem identified by FATF and VASPS, according to the FATF's Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers on July 2021 (later "FATF's Second 12-months Review"), is the lack of unified technology that would

[39] FATF (2021), Virtual Assets and Virtual Asset Service Providers. Updated Guidance for a Risk-Based Approach. October 2021. Retrieved from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html, 12 December 2021.
[40] *Ibid*, paragraph 204, 65.
[41] Panova, O., Leheza, Y., Ivanytsia, A., Marchenko, V., Oliukha, V. (2019), *supra nota* 20, 2-5.

support the transmission of the information required by the Travel rule.[42] On its Guidance for a Risk-based Approach to Virtual Assets and Virtual Assets Service Providers FATF listed technologies, such as public and private keys, Transport Layer Security/Security Sockets Layer (TLS/SSL) connections and X.509 certificates, which could be used by VASPs to comply with Travel rule. However, FATF has emphasized its technology-neutral approach and has not prescribed a particular technology that VASPs should use.[43] Thus, the VASPs around the World do not yet have a common understanding on how to transfer the required information in between them, and which technology they would use in doing that. On the other hand, it seems clear, that common compliance with the Travel rule by the whole virtual asset industry cannot be achieved without the VASPs having a common way to transfer the required information in between them. According to the European Commission's Study on developments with regard to virtual assets users and the possibility to set-up and maintain a central database registering users' identities and wallet addresses accessible to financial intelligence units (FIUs) (later referred to as "EC Study") the implementation of Travel rule requires common technical standards that would harmonise and standardise information transmission between originators and beneficiaries.[44]

1.3. The implementation of the Travel rule

The FATF Recommendations are not legally binding for obliged entities, but the Recommendations are directed to national states, which are expected to take actions to implement the recommendations into their national regulative frameworks. When the recommendations are implemented to national regulation, they become applicable to the obliged entities in that state.[45]

According to the FATF's Second 12-month report on June 2021, most jurisdictions and VASPs were still not complying with the Travel rule in June 2021.[46] At least on global scale, the question is not only about implementing the Travel rule to national regulations, but also about regulating

[42] FATF (2021). Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota* 14, paragraph 54, 17.
[43] FATF (2021). Virtual Assets and Virtual Asset Service Providers. Updated Guidance for a Risk-Based Approach, *supra nota 39,* paragraphs 282 and 285, 82-83.
[44] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Study on developments with regard to virtual assets users and the possibility to set-up and maintain a central database registering users' identities and wallet addresses accessible to financial intelligence units (FIUs)", Publications Office, 2021. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/dbaa8b83-5bc3-11ec-91ac-01aa75ed71a1/language-en, 5 February 2022, 58.
[45] *Ibid*., 6.
[46] FATF (2021). Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota 14,* paragraph 59, 18.

VAPSs in general. Namely, as virtual assets and VASPs are rather new phenomenon, national regulators are still at different stages on regulating virtual assets and VASPs overall, as described above in this study. Different jurisdictions have also taken different approach to regulate VASPS; some are implementing VASPs to their existing legislation, while some other are creating tailor-made legislation for VASPs. Even within the European Union, different member states are also in different phase on regulating VAPSs and implementing the Travel rule.[47]

According to the EC Study[48], published in November 2021, the main challenges to implement Travel rule are:

1. The fact, that Travel rule has not been implemented in many jurisdictions yet (it is difficult or even impossible for VAPSs in certain jurisdiction to take part in information sharing, if the counterparties, other VASPs in other jurisdictions, are not ready for that);
2. The non-interoperability of different technological solutions for Travel rule compliance;
3. Difficulties to identify counterparty-VASPs (to know, whether the counterparty of a transfer is a VASP and whether it is compliant with the Travel rule);
4. The cost of implementation and ensuring compliance with the Travel rule (for VASPs, but also regulators' resources are required);
5. Concerns relating to data protection and privacy; and
6. Ambiguity on how VAPSs should approach the Travel rule requirements in transactions between VASPs and unhosted wallets.[49]

In this study the author will especially concentrate on the two first ones of the challenges listed above (non-implementation by many jurisdictions and non-interoperability of different technological solutions), which together creates a "self-reinforcing conundrum", as FATF describes it in the Second 12-months Review: The lack of implementation into national regulation reduces incentive for technological progress to solve the technical side of the problem, while the

[47] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *supra nota* 44, 6-7.
[48] *Ibid*.
[49] *Ibid*., 7.

lack of technical progress provides national regulators a justification for the lack of national implementation.[50]

The technical implementation of the Travel rule would require the VAPSs operating in different jurisdictions to have a common, or at least interoperable, technological solutions to transfer the required data between the VASPs. That would according to the EC Study be achieved by establishing common technical standards such as messaging to harmonise and standardise the information transmission. The EC Study also points out, that VASPs lack globally accepted standards like SWIFT that is applied in transfers between banks and other financial institutions. However, the problem with virtual asset transactions is, that virtual asset transactions differ from traditional transactions between banks on that the virtual asset transfers occur on decentralised blockchain and must be validated by the network before considered final. Thus, also the exact point, at which the transfer actually happens and when Travel rule data must be provided is questionable and the approach on that varies between different jurisdictions.[51]

Not only lacks the virtual asset industry globally accepted standards that would harmonise the technological solutions, but the industry also lacks global associations or industry networks that would strive towards standardisation in the industry. Just as the virtual asset industry itself is yet fragmented, so are the initiatives to create solutions to comply with Travel rule. Efforts to create a solution to comply with Travel rule are being made by private companies as well as by joint industry groups, and as the solutions are developed with different protocols, technology and systems, there are concerns among regulators about the interoperability of the solutions to be created. Also, regional differences in implementing the Travel rule may lead to regional differences between the created solutions, which also may cause problems in the interoperability with other solutions as well as also restrict the scalability of the created Travel rule solutions.[52]

As the situation with the technological approach to solve the Travel rule issue is yet ambiguous, this of course affects the national regulators willingness to implement the Travel rule requirements on national legislation. One reason that affects national regulators willingness to implement Travel rule is probably the jurisdictional competition between different governments due to which some

[50] FATF (2021). Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota* 14, paragraph 61, 19.
[51] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *supra nota 44, 5*8-59.
[52] *Ibid*., 60-61.

governments are concentrating their regulative efforts to attract blockchain businesses to their territory.[53] As virtual assets industry, and blockchain based solutions as whole, are considered one trend which may have huge effects in the financial market in the future, many states see virtual asset industry as interesting future industry that the states want to attract. The question is not solely about a competition of tax-revenue between different jurisdictions, but question is also about gaining reputation, or band, as a jurisdiction being friendly to technological innovation.[54] In regarding the competition of VASPs between jurisdictions, the regulative framework is in key role. In order for a state to attract VASPs the regulative framework in that state should be competitive compared to other competing markets. If a certain state at this moment would require VASPs operating there to strictly comply with the Travel rule, this would actually restrict the business that the VASPs operating in this state could engage themselves with, because majority of jurisdictions and VASPs around the World are not complying with Travel rule yet, which means that a VASP that is required to comply with Travel rule could possibly not engage in transfers where counterparty-VASPs would not complying with Travel rule. And even though the counterparty-VASP of a transfer would comply with the Travel rule, it is highly probable, that the VASPs would not have interoperable technological solution to transfer the Travel rule data between them. Thus, a strict demand by regulator of certain jurisdiction for VASPs to comply with the Travel rule would at the moment lead to that the regulative framework in that jurisdiction would be considered unattractive, or even impossible to comply with, in the eyes of the VAPSs. Such strict demand would probably lead to remarkably reduce the business opportunities for VASPs already existing in that jurisdiction and new VASPs to consider other jurisdictions as place where to begin their business. Thus, demanding the industry to comply with the Travel rule would seem unattractive solution for national regulators until there are genuine possibilities for the industry to comply with such requirements.

The fact that countries are implementing Travel rule on their regulatory framework, and requires their VASPs to comply with it, on different pace, creates what is called as “sunrise issue” by FATF. Sunrise issue refers to challenges that arise due to the different pace of implementation, like the challenge for VASPs already complying with Travel rule on dealing with VASPs that are located

[53] Finck, M. (2018). Blockchain Regulation and Governance in Europe. Cambridge University Press, 143.
[54] Neitz, M. (2021). How To Regulate Blockchain's Real-Life Applications: Lessons From The California Blockchain Working Group. Jurimetrics (Chicago, Ill.), 61(2), 185-217.

in jurisdictions that have not enforced Travel rule yet. The question is how should the VASPs on complying jurisdictions approach those VASPs on non-complying jurisdictions.[55]

As the nature of virtual asset industry is global and transfers on virtual assets are easily made cross state borders, possibilities for a single jurisdiction to implement Travel rule effectively on its regulatory framework (and still being considered enough attractive jurisdiction for VASPs) is practically very restricted, as described above, unless at least certain amount of other significant markets implement the requirements as well. According to the EC Study, there is a general understanding among both private and public sector stakeholders that in order for the Travel rule to be effective, it needs to be implemented by all jurisdictions in a timely manner.[56] The FATF Second 12-month-review[57] on June 2021 as well as the private sector stakeholders interviewed for the EC Study[58] confirmed that at least one of the main barriers to compliance with Travel rule is the delayed action by jurisdictions on implementation. Thus, a prompt and effective regulative reaction by national legislators is clearly necessary yet to direct the development of the industry and technical solutions into right direction.

Yet, as the European Union is adapting its regulative framework to cryptocurrencies, also the regulative framework for collecting and sharing information on virtual asset transfers are being developed. Currently effective Regulation (EU) 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (hereinafter referred to as "Wire Transfer Regulation") sets out obligations for payment service providers to accompany certain information on the sender and beneficiary of a wire transfer to each transfer. However, the present Wire Transfer Regulation do not apply to transfers of virtual assets and thus the European Commission gave a Proposal for recasted regulation on information accompanying transfers of funds and crypto-assets (European Commission's Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast), hereinafter referred to as "Recast Regulation"[59]) on July 2021.[60] Even though Commission is

[55] FATF (2021). Virtual Assets and Virtual Asset Service Providers. Updated Guidance for a Risk-Based Approach, *supra nota* 39, paragraph 200, 64.
[56] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *supra nota* 44, P.59.
[57] FATF (2021), Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota 14*, paragraph 28, 11.
[58] European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *supra nota* 44, p.59.
[59] European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (2021/0241).
[60] *Ibid*., 2-3.

"hopeful for speedy legislative procedure" the proposed updated Recast Regulation will obviously be applied on 2024 at earlies.[61] The Recast Regulation itself will not bring the industry nor the national regulators instruments for Travel rule compliance, but of course clarifies the situation with Travel rule requirement in the European Union.

To conclude this chapter, there is yet great uncertainty on how and when different jurisdictions will implement Travel rule to their national regulation and will and how the different approaches by national regulators affect, for example, the possibilities of VASPs to operate in certain jurisdictions or the interoperability between VASPs located in different jurisdictions. Regulatory uncertainty in turn can curtail the growth the virtual asset industry, due to for example investors' hesitation to participate in the market.[62] Thus, regulative steps are needed in order for different jurisdictions to comply with the Travel rule, but also to create legal certainty that is necessary for the growth and development of the industry.

[61] European Commission, Financial Stability, Financial Services and Capital Markets Union. Anti-Money laundering and countering the financing of terrorism legislative package. Press Release, 20 July 2021. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690, 21 March 2022.
[62] Kaal, W. A. (2021). Digital asset market evolution. Journal of Corporation Law, 46(4), 909-964, 934.

2. THE PRINCIPLE OF TECHNOLOGY NEUTRALITY

2.1. Background of the principle

FATF has announced that its Recommendations, including the Travel rule, are technology neutral and listed a range of technologies that could be used to comply with Travel rule.[63] Technology neutrality is a principle that is not clearly and unambiguously described in the European Union regulation, but it is generally accepted and referenced in several regulative documents in different fields and levels of European Union regulation.

The principle of technology neutrality can be considered to derive from the values of equality and non-discrimination set out in the Article 2 of the Treaty of the European Union (TFEU) as well as the European Union's aim to establish an internal market that promotes "scientific and technological advance" as set out in the article 3 of the TFEU.

The term ***technology neutrality*** is defined through the freedom of individuals in the summary of Regulation (EU) No 283/2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC as

> *"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."*[64]

This can also be seen as a link with the fundamental EU rights of freedom of establishment and freedom to provide services, which would forbid Member States of EU to discriminate self-

[63] FATF (2021), Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota* 14, paragraph 54, 17.

[64] 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". Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:26030103_1, 27 February 2022.

employed-persons, professionals or legal persons legally operating in one Member State to operate in another Member State, inter alia, by unjustified technological requirements set out in the regulation of that other Member State.[65]

As the technological development is rapid and new technical innovations are introduced faster than ever before, there is a fear that regulation, which tends to develop much slower than technology, might set barriers for the deployment of new and efficient technological innovations.[66] The principle of technology neutrality originates from this fear in connection with the arise of possibilities to operate online instead of traditional offline domain, and from the aim to secure that offline and online means are treated equivalently by regulation. The introduction of the principle of technology neutrality aimed "to neutralize any preference of the regulator towards the offline domain".[67] First, the principle was used in regulation addressed to ICT-sector, such as Framework Directive. The recital 18 of the Framework Directive 2002/21 describes the Member States pursuit to technologically neutral regulation as:

> *"The requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified, for example digital television as a means for increasing spectrum efficiency."*[68]

By stating that technology neutrality does not preclude "taking steps to promote certain specific services" the recital 18 of the Framework Directive thus acknowledges that technologically neutral regulation may influence on market outcomes in order to promote certain objectives of the regulator, when such influencing is justified. However, the regulative measures should not be discriminatory. Instead of legal subjects, this "anti-discriminatory rule" of technology neutrality principle protects technologies (and through technologies, the property rights).[69]

---

[65] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021). 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 (Dissertationes iuridicae Universitatis Tartuensis [Võrguteavik]; 81). Tartu: University of Tartu Press. P. 30-31.
[66] Kamecke, U., Körber, T. (2008), *supra nota* 26, 330.
[67] Veerpalu, A., Ebers, M., Osula, A., Norta, A. & Tartu Ülikool. Õigusteaduskond (2021), *supra nota* 65, 27-28.
[68] 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, 33.
[69] Kamecke, U., Körber T. (2008), *supra nota* 26, 331.

Later as technology has become more cross-sectoral issue, the principle has become a value for more general regulation also, and the principle has been referenced to for example in GDPR.[70] Koops even argues that the idea of technology neutrality should be applied to regulation in general, and not only in specific fields of regulation.[71]

Regarding the regulation in financial industry, the European Commission's proposal on markets in Crypto-assets (MiCA) expresses pursuit towards technology neutrality by naming "respecting technology neutrality" (when removing regulatory obstacles for crypto-assets) as one of the proposals specific objectives and confirming in recital 6 that "Union legislation on financial services should not favour one particular technology".[72]

As Veerpalu mentions, the principle is especially relevant for any new technologies that are "deconstructing the key structures of society, trade and communication".[73] Virtual assets, and the distributed ledger technology behind them, are definitely technological innovations that strives to change the centralized infrastructure that the banking sector is traditionally based on, and this makes the principle of technology neutrality especially important to be considered when creating and reforming the regulatory framework in the financial sector.

2.2. Meaning and object of the principle

The principle of technology neutrality is a principle that is directed towards regulators and states. The principle aims to that the regulators would endeavour to create regulation that supports free and undistorted market competition between competing technologies when possible. According to the principle it is the market rather than regulation or state that should decide which technologies will succeed.[74] In its simplicity this means, that if there are multiple technological means to gain compliance with certain requirement set out in regulation, the regulator should not take a stand on which of these technological mean is chosen by any subject of the regulation, but it should be the

[70] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota* 65, 36.
[71] Koops, B-J (2006). "Should ICT Regulation Be Technology-Neutral?", in Koops et al. Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners, IT & Law Series, Vol. 9 (77-108). The Hague: T.M.C. Asser Press, 4.
[72] European Commission. (2020). Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 (2020/0265), *supra nota* 21, 16 and 145.
[73] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota* 65, 28.
[74] Kamecke, U., Körber T. (2008), *supra nota* 26, 331-332.

subjects themselves that would analyse the costs, effectiveness and other relevant features of the different technological means and would then choose the mean that according to this analysis is the best way for the subject to comply with the regulation, when the subject takes into account its other objectives in addition to complying with regulation, such as its own economic objectives. Thus, technologically neutral regulation should intent to regulate the legal subjects' behaviour, and not the technological means that are used to achieve such behaviour.[75]

As the principle of technology neutrality is directed towards regulators and states (i.e. public authority), Veerpalu describes the meaning of the principle by comparing it with the principles of equality of treatment, non-discrimination and transparency in the context of public procurement processes, in which the listed principles highlight that public contracts should be awarded to tenderers on the basis of objective criteria, and not for example due to public entities preferring certain tenderers.[76] In the context of technology, this thought is well described in the Recital 74 of Public Procurement Directive (Directive 2014/24/EU) that states following:

> *"..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…"*[77]

In the light of the Recital quoted above, the comparison of the principle of technology neutrality and the principles guiding public procurement procedure (equality of treatment, non-discrimination and transparency) made by Veerpalu seems legitimate and well descriptive. It is easy to accept that the idea and aim behind technology neutrality and the mentioned procurement principles is the same: the competition should not be narrowed by setting discriminating requirements, and technical specifications should be rather functional and performance-related than requirements specifying the technical means how the required functions and performance are

[75] Greenberg, B. A. (2016). Rethinking technology neutrality. Minnesota Law Review, 100(4), 1495-1562, 1512.
[76] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota* 65, 34.
[77] 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, 78.

achieved. Setting the necessary requirements according to these guidelines makes both, the public procurement procedure and technology-related regulation, seem transparent and objective and can also strive technological innovation as economic operators have room to choose, how they technically achieve the necessary functions and performance.

The reference to public procurement procedure also well highlights the relation of competition law and technology neutrality. It is obvious that unjustified technical requirements that are set out in any regulation might distort competition between economic operators if technical specifications in that regulation distinguish different products that can perform similar functions to acceptable and non-acceptable products. This is an interesting point also to consider in regarding the subject of this study and to bear in mind, when considering a national regulator's possibilities to set technical requirements on Travel rule compliance.

The referred similarities with public procurement procedure also highlight the duplex nature of the principle of technology neutrality. On one hand the principle guides law-making procedure and aims to restrict regulators on discriminating certain technologies in favour of other technologies in the regulation. But in addition to the law-making procedure, the principle should be adhered to in implementing and interpreting the created regulation by courts and authorities.[78] This is important to note, especially due to the fact that, as explained above, often regulation lags behind the emerging of new technologies, which means that often a regulation, or certain requirement set out in it, has been created by regulator without understanding the possibilities that new technological innovation might later generate. In this kind of case, the author suggests, the principle of technology neutrality should strive authority or court interpreting regulation to an interpretation that supports technology neutrality, and do not favour any certain technology, if such interpretation is possible. In this regard, it would also be helpful if a regulator would provide the interpreters clear guidelines regarding the aims and rationale of the regulation.[79] The possibilities to have multiple interpretations of course also vary between different legal systems.[80]

On the other hand, in order to be able to interpret regulation on technology neutral way, the regulation must be formed in a way that allows such interpretation. This would require more

[78] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota* 65, 29; and Koops, B-J (2006), *supra nota* 71, 25.
[79] Koops, B-J (2006), *supra nota* 71, 27.
[80] *Ibid.*, 22.

general, and not technology-specific, formulation of regulation.[81] On the other hand, general and non-technology-specific regulation creates uncertainty on how the regulation will apply to future unforeseen technological developments.[82] Also, however generally a regulation today is worded, as Greenberg has argued, it is still drawn with the yet "known technologies in mind"[83] and might still fail to deal with the future developments in desired way. Thus, technology neutrality requires balancing between technology-specific regulation and more general formulation of regulation as well as with the objectives of a specific regulation. According to Kamacke and Körber technology neutrality in regulation is often sought by deleting references to specific technologies. This however, may create overly broad market definitions and, as Kamacke and Körber by a practical example shows, better outcomes could be achieved by setting certain requirements by regulation for the technologies used (technology-specific regulation).[84] Other suggested means to find balance between technology neutrality and the need to set technology-specific requirements, as well as sustainability of the regulation and legal certainty in regulation, are for example using technology-neutral wording in higher level regulation and setting the technology-specific requirements in lower lever regulation (like technology-specific regulation), defining technology neutrality in the framework and principles that are followed when creating technology specific laws, and conducting periodical reviews of regulation to assess whether the regulation is still up to date in consideration of the development of technology.[85]

In this respect, the concept of "sustainability of law" can also be linked with the principle of technology-neutrality. The sustainability of law (in the context of technology) means that laws should be "sustainable enough to cope with the technological development over a sufficiently long period of time". In this context, too technology-specific law is not likely to cope with future technological developments and thus, must be adapted during rather shorter period of time than more sustainable law. This way Koops interprets technology-neutrality as a specification of sustainability of law.[86] The value of sustainability in turn can be considered as linked with the aim of endorsing innovation that is also an aim built in the principle of technology neutrality.[87] In this respect, in the context of regulating crypto assets and blockchain-technology, regulators should

[81] *Ibid.*
[82] Shadikhodjaev, S. (2021). Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? European Journal of International Law, 32(4), 1249-1282, 5; and Reed, C. (2007). Taking Sides on Technology Neutrality. *SCRIPT-ed, 4*(3), 263-284, 280.
[83] Greenberg, B. A. (2016), *supra* nota 75, 1498.
[84] Kamecke U., Körber, T. (2008), *supra nota* 26, 333.
[85] Shadikhodjaev, S. (2021), *supra nota* 82, 5-6; and Koops, B-J (2006), *supra nota* 71, 27.
[86] Koops, B-J (2006), *supra nota* 71, 10-11.
[87] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65,* 41.

bear in mind that blockchain technology can enable great variety functionalities beyond crypto assets and traditional "money-transmitting", and we do not even know yet all the possibilities this technology can offer in the future.[88] Thus, it would be desirable that the regulatory decisions regulators make today, regarding the money-transfer and payment functionalities of cryptocurrencies, would not create obstacles or "chilling effect" on the development of the other, and even yet unknown, functionalities of cryptocurrencies and blockchain technologies.[89] On the other hand it must be stated that regulating some technological innovation does not necessarily mean chilling innovativeness: on the contrary, legal certainty can promote innovation and legal uncertainty can discourage entrepreneurial resolve due to the fear of legal repercussions.[90] In this respect, the acceptability of technology specific regulation or technological requirements in regulation would depend on whether there are uncertainties in the present regulative framework, and whether these uncertainties could be solved through regulation without chilling too much the possibilities for further innovative developments among the industry.

As described above in this chapter, applying the principle of technology neutrality in practise is not uncomplicated and the principle cannot be applied without compromises. Instead, careful application of the principle requires regulators to analyse the expected impacts of regulation and then find balance between the benefits and costs gained through regulation.[91]

2.3. Functional equivalence and effects equivalence

According to Veerpalu[92], Reed[93] and Koops[94], there is two components in the technology neutrality, through which one can analyse neutrality of regulation. These components are:

1. Functional equivalence; and
2. Effects equivalence.

[88] Weinstein, S. N. (2021). Blockchain neutrality. Georgia Law Review, 55(2), 499-592, 509; and Kiviat, T. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. Duke Law Journal, 65(3), 569-608, 607.
[89] Kiviat, T. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. Duke Law Journal, 65(3), 569-608, 607.
[90] Finck, M. (2018), *supra nota* 53, 150.
[91] Wylly, P. (2015). Evaluating the costs of technology neutrality in light of the importance of social network influences and bandwagon effects for innovation diffusion. New York University Environmental Law Journal, 23(2), 298 – 353, 310.
[92] Veerpalu, A. (2018). Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De Voogd and Hedqvist. Baltic journal of law & politics, 11(2), 61–94, 78.
[93] Reed, C. (2007), *supra nota* 82, 267.
[94] Koops, B-J (2006), *supra nota* 71, 6.

Functional equivalence refers to aim, that different technologies should not be discriminated by regulator in case the technologies are able to perform equivalent functions or "even merely reach similar objectives with the performance of different functions". Thus, the aim of functional equivalence can be considered to secure that functionally equivalent solutions are legally as recognized.[95] In general, if a regulation rather describes the effects of the required solution than the technology itself, the regulation is likely to produce functional equivalence between different technologies. As Koops points out, in order to achieve functional equivalence between different techniques to achieve certain functions, it may however be necessary to adapt specific regulation to specific technologies, i.e. different treatment of technologies in regulation may be used to achieve technology neutrality.[96] In this case, the implementation of neutrality actually means finding "the closest equivalent approach" to different technologies.[97]

Regulation on digital signatures is a perfect example of technology-specific regulation that is used to achieve neutral treatment between online and offline signatures[98]. Originally it was a signature on a paper that was given certain status under regulation: signature was generally considered trustworthy way of expressing commitment to agreements and other judicial acts. When the possibilities to sign documents electronically evolved, a similar kind of status of trustworthiness was created to online signatures by creating specific regulation to electronic signatures. The aim of the specific legal framework for online signatures was to reduce uncertainty of the legal status of new techniques to sign.[99] The regulation was used to create certain parameters to trustworthy electronic signatures. The reduction of uncertainty related to electronic signature by this specific regulation concerning online signatures, according to the author, gave certain online signatures the status of trustworthiness and thus brought the online signatures on equal position compared to traditional offline signatures.

The example of regulating online signatures is interesting in terms of functional equivalence. The aim of functional equivalence would require that regulator would consider different technologies that produce equivalent functions equally acceptable and trustworthy. Thus, the regulator could

[95] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65*, 37.
[96] Koops, B-J (2006), *supra nota 71,* 7-8.
[97] Reed, C. (2007), *supra nota* 82, 272.
[98] The example is referred to by e.g. Reed, C. (2007), *Ibid*., 271; and Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota* 65, 38-39.
[99] UNCITRAL Model Law on Electronic Signatures with Guide to Enactement (2001).

not take certain specific technology as the basis for the status of "trustworthiness" provided by the regulation, but rather set certain conditions for a trustworthy electronic signature and guarantee the same status of "trustworthiness" for every technical solution that satisfies these conditions.

To reach the aim of functional equivalence, one must first identify, what is actually considered *functionally equivalent*, meaning that when can a function, that certain acceptable system executes, be considered to be "transposed, reproduced or imitated" through another system.[100] As one possible tool to evaluate this Veerpalu cites *functional analysis* that was used as an example in developing the UNCITRAL Model Law on Electronic Signatures and features the following steps:

> 1) an analysis of the requirements applied to acceptable system (in the example paper-based signatures);
> 2) identification of the purposes and objectives of these requirements; and
> 3) an analysis of the functions of the novel system.[101]

Through this analysis one could finally decide whether the functions of the reviewed novel system fill the purposes and objectives for which the requirements to the traditional, acceptable system were set. If they do, then the systems could be considered functionally equivalent. If the purposes and objectives are not totally fulfilled, the regulator could set necessary adjustive requirements to the reviewed new system so that filling these requirements by the new system would bring the new system functionally equivalent with the traditional system. Setting such technology-specific requirements on regulation would be acceptable, if it aims to achieve similar societal effects of the different technologies[102]. However, to justify the different treatment in regulation, the difference between the compared solutions should be enough substantial and the difference in treatment proportional to the substance.[103]

The basis of the functional analysis lies in the aim to not discriminate any technology as the analysis gives different technologies opportunity to satisfy the set requirements[104], and even if the

[100] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65*, 38.
[101] UNCITRAL Model Law on Electronic Signatures with Guide to Enactement (2001), referenced in Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65*, 38.
[102] Koops, B-J (2006), *supra nota* 71, 8.
[103] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65*, 54.
[104] UNCITRAL Model Law on Electronic Signatures with Guide to Enactement (2001), 57.

requirements are not satisfied, the purposes and objectives for which the requirements were set (i. e. the purposes and objectives of the regulation).

However, Reed points out, that each "acceptable" solution under regulation do not need to be equally "good", or in terms of electronic signatures "equivalent in terms of evidential weight", but the meaning of the regulation may rather be to set up the level that is sufficient (for example in terms of the evidential level) for the technical means to produce certain functions.[105] Thus, the requirements regulation sets for different technologies would not need to aim to a completely equal result when using different technologies, but the requirements set out in technologically neutral regulation would be just to set minimum acceptable level, for example in terms of security. According to this thought functional equivalence could be relative to some extent. This is to say, that "equal" do not necessary mean "same".

Effects equivalence in turn refers to the outcomes of the regulation and aims to substantively equivalent effects across different technologies, even if different technologies are regulated specifically.[106] The effects equivalence requires that if functional equivalence is established between two solutions, the solutions should be treated equivalently in terms of the effects on applying regulation in practise.[107]

Effects equivalence can be explained using the same example of offline and online signatures. For example, if offline signature filling certain requirements set out in regulation, and online signature, filling corresponding technology-specific requirements, are accepted as functionally equivalent, the regulation should also establish similar societal effects for both signatures. Thus, if for example an agreement is given legally binding effect, if it signed on paper, the same effect should be given to similar agreement signed on functionally equivalent online signature. In this respect, the author argues, that the aim of effects equivalence not only puts pressure on lawmaker, but also operates an interpreting guideline to authorities implementing and interpreting existing regulation.

As the principle of technology neutrality emphasizes equality and free competition, the effects of regulation should be analysed especially against these values. In respect of the outcomes regulation might have, the principle of technology neutrality is directed against unjustified regulation in

[105] Reed, C. (2007), *supra nota* 82, 271.
[106] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65*, 37.
[107] *Ibid*., 56.

general, and on the other hand, against distortion of competition by discrimination in the level of regulation.[108] If regulation, and not the functional differences of different solutions, create circumstances where one technical solution is less effective or otherwise on weaker position than other functionally equivalent solution, the regulation does not grant effects equivalence to the solutions.[109] However, sometimes, even if certain solutions are considered functionally equivalent regarding certain purposes and objectives, these functionally equivalent systems may have somewhat different societal effects, which could justify different treatment of the systems under regulation.[110]

The question of effects equivalence is a major question also in respects of anti-money laundering regulation in relation to cryptocurrencies and fiat currencies. A regulator should justify any difference in the treatment of cryptocurrencies and fiat currencies on basis of non-discriminatory reasons.[111] As shown earlier in this study, complying with the FATF Travel rule is much more difficult when transferring cryptocurrencies than when transferring fiat-currencies due to the lack of similar global industry infrastructures on cryptocurrency industry than what exists on traditional banking industry. This means that the FATF Travel rule, and any regulation deriving from it, do not grant effects equivalence to cryptocurrencies and fiat currencies. As long as the difference in effects of the anti-money laundering regulation is however based on non-discriminatory reasons (i. e. fundamental difference in the functions of the technologies), the different outcomes of the regulation can be considered non-discriminatory and thus acceptable, but this difference in the outcomes of applying the Travel rule needs to be beard in mind, when applying implementing the Travel rule in the national regulation. The difference in the effects of the regulation for cryptocurrencies and fiat-currencies should be no greater than what is necessary in order to protect the purposes for which Travel rule was created.

2.4. FATF Travel rule and technology neutrality

It is noteworthy, that the main change that the referred updates in FATF Recommendation and Interpretive Notes brought into FATF framework, as referred in chapter 1 of this study, is that they bring new regulated entities under their umbrella, namely the VASPs. The Travel rule

[108] Kamecke, U., Körber, T. (2008), *supra nota 26,* 335.
[109] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota 65*, 40.
[110] Koops, B-J (2006), *supra nota 71*, 6.
[111] Veerpalu, A., Ebers, M., Osula, A., Norta, A., & Tartu Ülikool. Õigusteaduskond. (2021), *supra nota* 65, 40.

recommendation is identical for both, the traditional financial institutions like banks, and VASPs. This way the Travel rule itself seems technologically neutral indeed. Soana has, however, justly questioned the Travel rule's technology neutral character, as the FATF's approach do not take into consideration the fundamental differences that exists between decentralized cryptocurrencies and centralized fiat-currencies. Soana bases this argumentation especially to the fact that transactions on cryptocurrencies do not require intermediaries (VASPs) and thus part of all transactions still happens outside the applicability of FATF Recommendations.[112] Even though part of fiat-transactions also happens outside of the FATF Recommendations scope (cash transactions), it is an essential question, whether regulators both at EU level and national level should take the specific features of cryptocurrencies into consideration, when implementing the Travel rule, and have a more technology-specific approach on regulation than the one FATF have taken and customize the regulation for cryptocurrencies at some extent. As described in chapter 1 of this study, there are some crucial differences between fiat-currencies and cryptocurrencies in regarding the way transactions are transmitted. These differences are partly technological in nature, but also relates to different industry standards, especially to the immaturity of industry standards among the VAPSs.

[112] Soana, G. (2022), *supra nota 9,* 11.

3. STANDARDISATION

3.1. Standard

A technical "standard" can be defined as *"a set of parameter values that can be adhered to by a collective, either tacitly, or in accord with some formal agreement that defines the design, material composition, processing, or performance characteristics of a technical system or product"*.[113] In practise one could define standards as technical rules that guide and govern technical interaction and relations between different participants.[114] As explained earlier in this study, in regarding the Travel rule compliance, a common standard is needed for VAPSs to transfer the Travel rule data between themselves.

Standardisation is a process of developing consensus-based technical specifications in certain field.[115] Technical consensus enables or ensures interoperability of technologies of different market participants. As Neele Kroes, the European Commissioner for Competition Policy back then, stated on her speech for OpenForum Europe in June 2008 *"interoperability encourages competition on the merits between technologies from different companies, and helps prevent lock-in. Standards are the foundation of interoperability".*[116] Standards are important vehicles to promote interoperability and thus encourage competition between manufacturers in innovating and competing to create and provide products that conform to the standard.[117] Properly implemented standards can bring predictability and compatibility to market players and thus ensure a level playing field for different economic actors.[118] Standards may also promote many kinds of public interests such as security and quality requirements.[119]

---

[113] David, P., & Steinmueller, E. (1992). The economics of compatibility standards and competition. Stanford University, Center for Economic Policy Research, paper presented at the Technology Organizations, and Productivity (TOP) Workshop, January 21 1992; referenced in Ewertsson, L. (2010). Is Seeing Believing?: The Experimental Production of Technical Standards for HDTV. East Asian Science, Technology and Society, 4(3), 383-418, 386.
[114] Ewertsson, L. (2010). Is Seeing Believing?: The Experimental Production of Technical Standards for HDTV. East Asian Science, Technology and Society, 4(3), 383-418, 386.
[115] Van Eecke, P., Truyens, M. (2008). Standardization in the European information and technology sector: official procedures on the verge of being overhauled. Shidler Journal of Law, Commerce & Technology, 5(3), 1-9, 1.
[116] Kroes, N. (2008). Being open about standards. Speech to OpenForum Europe, Brussels, June 10, 2008. SPEECH/08/317, referenced in Dolmans, M. (2010). A tale of two tragedies- pleas for open standards. International Free and Open Source Software Law Review, 2(2), 115-138, 117.
[117] Weinstein, S. N. (2021), *supra nota 88*, 558.
[118] Van Eecke, P., Truyens, M. (2008), *supra nota 115*, 1.
[119] *Ibid*.

Though the ideas of technological innovation and technological standardization may sound contradictory, standards can encourage innovation as standards create some certainty for future development.[120] In addition to creating and ensuring interoperability between different technologies, standardisation aims to solve the problem of technological uncertainty, which refers to situation in which it is difficult for market participants to forecast specific technological development in the market and/or markets acceptance for some developed technological solution.[121] If standardisation succeeds, it makes the market participants sure about the technological development in the future and allows them to concentrate on building their operation on more stable base instead of having to prepare themselves for multiple future scenarios. Thus, standardization is generally accepted as essential driver for long-term productivity, competitiveness and innovation.[122]

On the European Union level standardization is used by the regulator to diminish technical trade barriers between the Member States and thus increase innovation and competitiveness among the market players in the EU.[123] However, standardization is not solely a question of European internal market, but in today's global technological environment, it is a global question, and Europe's competitiveness and technological sovereignty is dependent on how successful European actors are in standardisation at international level. The new EU Strategy on Standardisation, that was published in February 2022, acknowledges that the European standardisation needs to become more agile, flexible and focused to anticipate needs for standardisation in order for Europe to be successful in the present international competition.[124] The use of blockchain technology and decentralized finance are certainly such new innovative fields of technology on which standards will be created in the near future and the Europe certainly should take active role in the process of standardisation in these fields in order to promote Europe's own values, objectives and competitiveness int his field.

[120] *Ibid.*
[121] Riillo, C., Allamano-Kessler, R., Asnafi, N., Fomin, V., & Van de Kaa, G. (2022). Technological Uncertainty and Standardization Strategies: A Coopetition Framework. IEEE Transactions on Engineering Management, 1-14, 1.
[122] *Ibid.*
[123] Van Eecke, P., Truyens, M. (2008), *supra nota 115*, 1-2.
[124] European Commission. An EU Strategy on Standardisation; Setting global standards in support of a resilient, green and digital EU single market. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 2.2.2022 COM(2022) 31 final, 1.

3.2. Creation of standards

When we consider standards as "something that guides interaction between participants", there is no one predefined institution that can create standards. Efforts to achieve standard can be done by regulators or industry associations, that represent different market participants, but creation of a standard can also be left to the market to achieve the standard.[125] Both formal and informal institutions can set norms that indicate acceptable and appropriate interaction.[126] Another thing is whether set/agreed norms become generally accepted and implemented among desired participants, so that they can be considered standards that actually govern interaction between different market participants. As the objective of a "standard" is that it is applied universally, or at least by certain group of participants in their interaction, the author considers that becoming a "standard" requires that created norm also gains at least certain level of acceptance and implementation in use among desired target group of participants – thus, sole agreement of standard by minority of participants for example do not yet create a general "standard" even though it may constitute a standard in the interaction between the minority that agreed upon it.

Also, there is no one clear path to create technical standards. Agreeing on technical standards is usually not a question of pure technical coordination, but there are many stakeholders that have their own interests involved in the standard creation and thus if an agreement of standard is reached at any institution, the result is always an outcome of negotiations and compromise.[127]

It is not always the case that standards are created consciously by active efforts to create standards. Standards may also *de facto* emerge from the markets[128], when for example some technological specifications practically gain a status of standard, at least unofficial, through widespread use and general acceptance by relevant stakeholders. In this sense one could for example consider Apple's iOS and Google's Android being certain kind of standards as mobile operating systems in that sense that if someone creates a new programme that is meant to be used on mobile devices, this programme should be interoperable with iOS and Android operating systems, or at least one of them, in order for the new programme to gain large scale global user base. IOS and Android has

[125] Braunstein, Y. M., White, L. J. (1986). Setting technical compatibility standards: an economic analysis. Journal of Reprints for Antitrust Law and Economics, 16(2), 685-[ii], 688.

[126] Ewertsson, L. (2010), *supra nota* 114, 386.
[127] *Ibid.,* 384.
[128] Kroes, N. (2008). Being open about standards. Speech to OpenForum Europe, Brussels, June 10, 2008. SPEECH/08/317. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/speech_08_317, 17 April 2022.

gained this status by gaining enough significant global market share, and as they have reached this position, it is possible that regulators around the world will also intervene and begin to require interoperability with these two operating systems for new mobile applications for example in order to stabilize the competition methods between these two main operating systems.

The same way certain standards are being created among the virtual assets and virtual assets services markets also as this rather new industry evolves. And the technical solution to achieve Travel rule compliance in the industry is one significant of those standards that will be created. The author suggests that if the regulator do not intervene, it will be the industry itself that creates the standards that the industry participants need in order to interact with each others. When we consider the aims of technological neutrality (e. g. the aim that market will decide the used technology, not the regulator), industry creating the necessary technological standard sounds ideal. However, the creation of standards by private sector does not always happen without problematic side effects as later shown.

3.3. Standardisation by private sector

Standard setting can happen at least through three different mechanisms on private sector (without the involvement of regulator): *cooperation, competition and coopetition.*[129]

In *cooperation* a standard is reached through the work of one or several committees/organizations where interested parties negotiate upon the standard's content.[130] The cooperation mechanism includes especially the so-called standard setting organizations (SSOs), which are private organizations that promote technical coordination in search for general consensus, usually by seeking to take into account the views of all concerned parties and to reconcile conflicting arguments.[131]

In *competition* variant a standard is arrived in the market through a "standard's battle".[132] The previous example of iOS and Android operating systems creating standards themselves is an

[129] Riillo, C., Allamano-Kessler, R., Asnafi, N., Fomin, V., Van de Kaa, G. (2022), *supra nota* 121, 1.
[130] *Ibid.*
[131] Farrell, J., & Simcoe, T. (2012). Choosing the rules for consensus standardization. The Rand Journal of Economics, 43(2), 235-252, 236.
[132] Riillo, C., Allamano-Kessler, R., Asnafi, N., Fomin, V., Van de Kaa, G. (2022), *supra nota 121,* 1.

example of the second variant, competition. In competition's case, arriving to standard may happen without a definite plan to standardise through kind of "natural drifting" towards standard as result of possibly unbalanced competition in the market. In the situation like iOS and Android example above, a monopoly or oligopoly kind of naturally creates standard practises (albeit it may also often be that the dominative players in the market intentionally aim to convert their way of doing something to a standard in the market due to economic incentives in this kind of standardisation). This kind of standardisation is usually proprietary standardisation, where the "creator" of the standard has IP-rights to at least some part of the technology that is needed to implement the standard and thus the "creator" enjoys economic benefits for its technology becoming a standard.

Coopetition refers to combination of cooperation and competition, where competitors co-operate in setting a standard.[133] In their study Riillo and others define *coopetition* as a hybrid form of standardization that happens both within individual company level and in SSOs.[134] However the author points out that coopetition type of standardization could well happen outside the SSOs sphere of influence also. Namely different kind of co-operation arrangements between competitors could lead to *de facto* standardisation, without the involvement of specific SSOs. If the stakeholders participating in the creation of standard are able to agree on standard among themselves and if they together have enough strong position in the ecosystem, this kind of agreement may eventually lead to create a general industry standard the same way as in the competition variant. The operating logic of coopetition variant might even be quite similar as in the cooperation model, but the main difference between cooperation and coopetition models is obviously that the structure of the co-operation between the participants could be more organized in cooperation variant and the idea of cooperation variant would also be to involve all interested stakeholders in the creation process, while in competition variant it might be beneficial for the participants to delimit the number of participants. In this study the author does not touch the competition issues that might arise when competitors agree on standards, but the author wants to point out that agreeing on standards between competitors, especially outside SSOs framework might be controversial in the competition regulations respect. However, as later shown in this study, the relationship of competition and standardisation is complex and multidimensional, and standardisation can have both negative and positive impacts on competition in market.

[133] *Ibid.*
[134] *Ibid.*

However, classifying standardisation procedures to committee-based (meaning SSOs), government-based and market-based standards or to private- and public-based is not necessary are standards are created through hybrid processes also nowadays.[135] Standards that are agreed upon by private standardisation bodies can later be provided the status of *de jure* standards for example by national regulators or by the International Organization for Standardization (ISO).[136] As Ewertsson has shown on her study regarding standardisation of HD-television, many different participants (individuals, organizations and administrations) throughout the world may be involved in the process of creating a worldwide standard.[137] And this is probably a correct way to operate, when the participants are aiming at as universal standard as possible. Also, it is possible that a standard has to be created for more than just one industry or at least different industries are affected by the standard and has to be engaged in the standardization procedure[138]. However, the author suggests that the wider the cluster of stakeholders is, the more involvement by public sector is probably needed in order to create the circumstances for the relevant stakeholders to co-operate in creating a standard and to push the standardisation.

Either way, when industry itself creates standards, it does not usually (or at least always) happen through fair and balanced involvement of all market participants to the creation of the standard, but there are certain logistics how industry created standards are born. Namely, setting whatever technological standards involves economic interests of different stakeholders. For example, some market participants may have already invested in certain technology that solves the problem and have thus economic interests to promote that technological solution. Technology providers or other stakeholders that create technical solutions would of course want their technological solution to create the standard. Actually, standardizing their technological solutions as a standard for the whole industry could be a financial lottery win for the developer, especially if the developer happens to own patent or other IP-right over technical solution that is essential in complying with the created standard. Sometimes a standard can even create an "essential patent" meaning a situation where there is no technical possibility to acquire, use or operate an equipment or method that complies with the standard without infringing this essential IP-right. Balancing between standardization and IP-rights is therefore characteristics of standardisation efforts.[139]

---

[135] Fukami, Y. (2021). Open and Clarified Process of Compatibility Standards for Promoting Data Exchange. The Review of Socionetwork Strategies, 15(2), 535-555, 537.
[136] *Ibid.*
[137] Ewertsson, L. (2010), *supra nota 114*, 405.
[138] Riillo, C., Allamano-Kessler, R., Asnafi, N., Fomin, V., & Van de Kaa, G. (2022), *supra nota 121,* 9.
[139] Bekkers, R., Iversen, E., & Blind, K. (2012). Emerging ways to address the reemerging conflict between patenting and technological standardization. Industrial and Corporate Change, 21(4), 901-931, 902.

Standard setting should be based on the merits of the different technologies. If the standard setting procedure is characterized rather by side agreements and inducements between the stakeholders, than the merits of the technologies involved, there is a risk that the standard setting procedure falls out of the EU competition rules[140], and also a risk, that the agreement on standard will not be as efficient to drive towards its objective than it would have been, if it would have been agreed upon on pure basis of the merits of the technology. Also, due to the economic interests that the stakeholders have, such as the ones mentioned above, finding consensus on technical standard may not be easy and fast on private sector. As Farrell and Simcoe describe the vested interests that different participants have may make it difficult to achieve enough universal consensus and rather turns the industry coordination to "war of attrition", a kind of deadlock where participants instead of seeking compromise just seeks for the opposing side to concede.[141]

No matter which way standard is being created, as Ewertsson has shown on her study on standardising HD-television, creating a worldwide standard is a progress that can take decades and finding a single worldwide standard may even turn out to be an impossible mission.[142]

3.4. Standardisation and technology-neutrality

Similarly, as technology-specific regulation is an exemption to the principle of technology neutrality, standardisation means an exception to technology neutrality. Standardising interaction between market participants may also mean exception to the prohibition of restrictive agreements set out in the Article 101(1) of the Treaty of the Functioning of the European Union (TFEU) which prohibits "*agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market".* However, Article 101(3) of the TFEU mandates exceptions to this prohibition in case of such agreements between undertakings, decisions by associations and concerted practises

[140] Kroes, N. (2008), *supra nota 128.*
[141] Farrell, J., & Simcoe, T. (2012), *supra nota 131*, 235.
[142] Ewertsson, L. (2010), *supra nota 114*, 403-406.

> ***"…which contributes** to improving the production or distribution of goods or **to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit**, and which does not:*
>
> *(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;*
>
> *(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question."*

This sets a fundamental basic premise for standardisation in the European Union: agreeing on one technology as the basis for a standard, and excluding others, is only possible when, the consumers get *fair share* of the benefit and the restrictions are dispensable to attain the objectives of the standard and the competition in the products implementing the standard is not eliminated.[143]

Thus, the decision on whether to standardise or not, should depend on analysis balancing the different aspects (kind of cost-benefit analysis, just like when deciding on whether to set out technology-specific regulation), and standardisation should only happen when there are demonstrable benefits[144] and standardisation should only be used in the market to the extent it is necessary for its objectives (technological certainty and interoperability between different technologies). This means that the target standard should not be more restrictive than necessary in order to achieve the objectives and should on opposite allow maximum consumer (or stakeholder) choice without locking the stakeholders with single vendor. Just like technology neutral regulation, a standard should aim to maximize competition of participants within the standard, so that participants would freely seek and choose the products that fulfil the standard on the basis of the differences on the product features and quality.[145] This means especially, that if there are open technological alternatives available, no standard (as nor regulation either!) should force or encourage market participants to choose a proprietary technology (technology for which the technology-originator has patent or other IP-rights over) instead of non-proprietary alternative.

[143] Dolmans, M. (2010). A tale of two tragedies- pleas for open standards. International Free and Open Source Software Law Review, 2(2), 115-138, 126.
[144] Kroes, N. (2008), *supra nota 128.*
[145] Dolmans, M. (2010), *supra nota 143*, 123.

In regarding the standardisation of Travel rule compliance technology, the requirement of balance between the measures taken to deviate from the prohibition of agreements and concerted practises as set out in the Article 101(1) of the TFEU and the objectives of standardisation are understandable against the ideological background of technology neutrality, as discussed earlier in this study. Similarly, the requirement of not allowing undertakings to eliminate competition is understandable in the context of Travel rule technology. These two requirements set out in Article 101(3) of the TFEU for exceptions to the prohibition of agreements and concerted practises reflect the same ideology of free competition and non-discrimination that was already discussed above in this study regarding the principle of technology neutrality.

The idea of consumers getting a *fair share of the benefit* of standardisation in turn sounds something not discussed in the earlier. In the case of Travel rule compliance technology, the consumers would see the benefits for successful standardisation (or disadvantages of unsuccessful standardisation) at least as more stable service providers (VASPs) that are interoperable with each other. When the VAPSs are interoperable with each other, consumers are expected to have more possibilities to choose their service provider and interact with other consumers through their service providers: If no common standard is found in the industry, there is a risk of proliferation of competing standards[146], which leads to the industry becoming even more fragmented as certain group of service providers use certain technology, while other group of service providers use another technology and these two or more different groups are not able to interact (i.e. transfer payments) with each other. This kind of situation of multiple standards is also possible[147] in the case of Travel rule compliance technology, simply because the industry is yet fragmented and because national regulators may, at least at beginning, do different decisions concerning technical specifications. However, in respect to the objectives of the Travel rule, as well as the interoperability between different VASPs and the economies of scaling, the author would not see multi-standard situation attractive. However, several standards to comply with Travel rule would be better for the start than no standard at all.

When considering the consumers' benefits from standardisation and disadvantages due to limiting the technological variance in the market, we must also consider that what are the benefits for consumers due to ultimate technological neutrality in regarding the technological solutions to

[146] Simcoe, T. (2012). Standard Setting Committees: Consensus Governance for Shared Technology Platforms. The American Economic Review, 102(1), 305-336, 332.
[147] Fukami, Y. (2021), *supra nota 135*, 537.

implement Travel rule. The benefit of ultimately neutral approach to technology could in ideal World be that the market would eventually find and agree on the best possible technological solution, which would become a standard, that the whole industry would use. However, in order to benefit the customers, an innovation must be used in the market.[148] However, if the ambition to technology neutrality would lead to fragmentation of the market, even temporarily, the consumers could have less possibilities to choose between different service providers and thus only part of the consumers would benefit from (some) service providers using the best possible technological solution, while the other ones would not. Also, the author suggests that possible fragmentation of the industry would lead to restrain the growth of general adoption of cryptocurrencies in the market as fragmented industry would not be as attractive for users than widely interoperable industry. In this sense, benefits of technological advantages due to ultimately neutral regulation could remain unrealized, if the technological advantages would not be widely used in the market and bring benefit to large number of consumers.[149] Of course, the aim of free market competition is that eventually the best possible technological solution would win the market and the market would become integrated, but before that, consumers and the whole industry could pay price for the neutrality.

Another clear benefit for consumers that should be sought through the standardisation is pricing of the services (transferring of virtual assets) for customers. Compliance with Travel rule will sure cause costs for VASPs, especially due to the need to deploy technology they need to comply with the Travel rule. In this respect, standardising procedure provides a possibility to ensure that existing patents do not restrict efficient and economic implementation of the standard, and if there are patents that are "essential" for the implementation of the standard, the licenses and use of the relevant technology are priced fairly from the consumers point of view, so that using such essential technology as a tool to implement the standard is fair for the industry participants and beneficial in the consumer's point of view.

As we consider, what is written above in this chapter, we can conclude that standardisation and the principle of technology neutrality are not completely opposite to each other. Instead, standardisation may support certain values behind technology neutrality. As Commissioner Kroes mentioned on her speech, *standards are the foundation of interoperability.*[150] Interoperability in

[148] Wylly, P. (2015), *supra nota* 91, 302.
[149] *Ibid.*
[150] Kroes, N. (2008), *supra nota 116,* referenced in Dolmans, M. (2010), *supra nota* 143, 117.

turn creates possibility for technologies to compete on level playing field and supports the market to avoid lock-ins (situations where the market becomes dependent on certain proprietary technology or service provider). Thus, even though standardisation may lead to exclude certain technological solutions outside certain market, standardisation may in turn support technology neutrality in the standardized market among the technologies that can be used to implement the standard.

As standardisation and interoperability facilitates economies of scale[151], the write suggest that standardisation of Travel rule compliance technology would create the participants in the market (VASPs and technology providers) possibilities to grow their business and at the same time encourage the scaling up and growth of the whole virtual asset industry. On the other hand, standardisation would reduce the market participants need to prepare themselves for different market outcomes and eliminate the possibility that circumstances would develop so that some VASPs would need to deploy several different technological solutions to comply with Travel rule in the meanwhile when waiting for the industry standard to develop.

Considering what is written above in this chapter, it seems clear that standardisation of Travel rule compliance technology would have several positive effects on the market. Thus, the author suggests that standardisation is needed and would positively support the development of virtual asset market and the industry. However, standardisation should be done carefully.

3.5. The necessary steps to achieve standard

If we come into conclusion that standardisation is needed in the industry, then the next step is to decide, how to standardise. To get closer to a standard, the main issues to discuss are, which institution will take steps to create standard (the regulators, private sector or both) and what qualities should we expect from a good, technology-neutral standard.

3.5.1. Creator of standard

First choice that regulating authorities should do, is to decide, whether regulation is needed to enforce standardisation or if the efforts to seek standard are left solely to the industry and/or market.

[151] Kroes, N. (2008), *supra nota 116.*

Even though, there are several problems that can be associated with standards emerging from the markets through competition, as described earlier in this study, we should remember that market-based standards can also be good in the view of free competition and technology-neutrality, if the standard emerge as a response to consumers' or other market participants expressed preferences.[152] In ideal market economy, technological standard would emerge through free competition and balanced decision making in the market, customers' needs and preferences being the ultimate driver towards the standard, but the problem is that decision making concerning the technologies used is not always fair and balanced due to the imbalance of power of economic operators in the market and the different kind of relationships of dependency between different stakeholders, due to which standardisation process on market may not always lead to choosing the best possible technology on the basis of the merits of technology.[153] When the market develops so that other drivers than customers benefit drives towards standard, then regulator intervention to such standardisation procedure through sole competition is necessary. Regulators input can be useful in that sense that as an "outsider" regulator can be suspicious towards industry arrangements, that could involve unfair collusion or raise barrier to entry into market by for example favouring present market participants over potential entrants.[154] Thus, regulator can have the role of protecting the customers benefits in the process.

Also, when we in the light of technology neutrality consider the problems that may relate to standard creation by private sector as mentioned above in this study, we realize that even though the principle of technology neutrality favours market decisions instead of regulatory involvement, the creation of standard by the private sector is not necessarily the best possible solutions in the technology neutrality's respects. This is due to the objectives that private sector participants have towards the standardization which may conflict with the objectives of technology neutrality (level playing field, efficient markets etc.). Because different stakeholders in the market have different economic and political power to impact to the creation of standard, the standard as a result of sole private efforts could be imbalanced and contrary to the objectives of principle of technology neutrality. In this sense the idea behind the principle of technology neutrality, that the "market and not regulator should decide" should be interpret as "market" meaning not solely the market participants (VASPs for example), but also and especially the customers using the end-products

[152] *Ibid.*
[153] Braunstein, Y. M., & White, L. J. (1986), *supra nota 125,* 703.
[154] *Ibid*., 702-703.

that utilize the technological solutions for which standard is sought (in the case of VASPs and Travel rule, the customers using virtual assets), because the customers are the ones that enjoys the benefits of efficient, reliable and economic technical solutions to transfer the Travel rule data between the VASPs (in terms of lower costs for the end product). And the customers are also the ones that pay the price for inefficient and expensive solutions that industry decides to use. Of course, on large scale the customers cannot be involved in the decision making, but there are ways to have the customers' view taken into account in the standardizing process. Again, regulator is the most obvious actor that can take the general good, including the customers position, into account.

Another issue that the author wants to stress regarding the correct institution to begin with the standardising process is the time-schedule of the standard. As mentioned earlier in this study, FATF has called for rapid action from jurisdictions to implement Travel rule. Also, as earlier mentioned, both the industry and regulators seem to be waiting for technical solution now. Market itself may not be able to standardize enough rapidly (through neither competition nor cooperation).[155] The cooperation method to create standards on SSOs framework is blamed to sometimes delay standardisation, because SSOs seek consensus, which gives interested parties possibilities to block or delay adoption of standards.[156] Simcoe studied delays in standard setting by SSOs by testing predictions of a developed model using data from the Internet Engineering Task Force (an SSO that produces standards that are used to run the Internet) and the study showed that distributional conflicts (conflicts of different commercial interests that participants have in the process) as well as high number of commercial participants do (on average) have a delaying effect on finding consensus on SSOs framework.[157] In regarding the standardisation of Travel rule technology one could assume that the fact that virtual asset industry is yet fragmented and involves great amount of small operators located in different jurisdictions, that should be engaged at some level (not all and not directly, but enough of them through some kind of representation mechanism) would alone make standardisation procedure through SSO too slow for the rapid need to implement the Travel rule expressed by FATF. In addition, some market participants could sure have interests to delay the standardisation due to the simple fact that many regulators seem to wait for standard before implementing the Travel rule on national regulation and some market

[155] *Ibid*., 703.
[156] Simcoe, T. (2012), *supra nota 146,* 308.
[157] *Ibid*., 308, 331-332.

participants could find this as a possibility to stay outside the Travel rules applicability, which must feel as an extraordinary regulatory burden to many VASPs.

As Braunstein and others suggest, regulation could serve as vehicle for industry to agree on standard by arbitrating differences among industry participants or even force the industry to standardise. Even in case, when regulator's intervention to speed-up the standardisation procedure would lead to choosing technology which is not the best, there could still be positive outcomes for such intervention as the industry would gain the benefits of scaling faster and conversion costs a later standardization process could be avoided.[158] Adoption of new technology may also delay due to the uncertainty in the industry on what technology will succeed[159]. The delay in implementation of Travel rule in the virtual asset industry, as FATF has reported referring to the "self-reinforcing conundrum"[160], can be considered as more or less equivalent circumstance, in which the industry waits for confirmation before it proceeds to comply with the Travel rule. In this respect, speed-up for the standardisation process would be needed on the virtual asset industry.

Also, the author suggests that the longer it takes to create common standards for Travel rule compliance, the higher amount of necessary technological solutions will be some way IP-protected, if possible, because the providers that provide technical solutions try to prepare themselves for the future industry standard by getting maximum protection for solutions they have created. Such an IP competition between the technology providers could lead to stifle innovation, standardisation and implementation of standard if there is a fear that IP rights challenge the implementation of standard.[161]

According to the author view, the factors relating to technology neutrality, customers benefit and time-schedule as outlined above, drives for regulator's involvement in the standardisation process. However, it must be stated, that what is mentioned above in this study do not either mean that the creation of standard by private sector, or involvement of private sector, would necessarily be a negative issue. On the contrary, the private sector involvement is certainly needed in order to create

[158] Braunstein, Y. M., White, L. J. (1986), *supra nota* 125, 703.
[159] Katz, M. L., Shapiro, C. (1985). "Network Externalities, Competition, and Compatibility." American Economic Review 75(3): 424–40, and Farrell, J., Saloner, G. (1986). "Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation." American Economic Review 76(5): 940–55, referenced in Simcoe, T. (2012), *supra nota 146,* 305.
[160] FATF (2021), Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota 14*, paragraph 61, 19.
[161] Dolmans, M. (2010), *supra nota 143*, 120-121.

purpose-built and sustainable technical solution to comply with the Travel rule. Also, the author wants to remind that the problematics around creation of standards by private sector as described in this study, are not absolute and present in every standardisation procedure by private sector, but the mentioned problems are only findings of possible problems related to private-based standardisation that have been made in literature. On the other hand, it should be also mentioned that regulator-based standards also have their own inconvenience – the most fundamental of them being that, when regulator involves in standard creation the regulator intervenes the market. Also, many of the problems associated with private-sector standard setting in this study, such as risks of anticompetitive conduct, could apply in government-based standardisation procedure also. Even though co-operation with private sector in standard setting process for Travel rule compliance technology is necessary, or at least recommendable, there is of course risk, that some market participants try to influence a government-based standard setting process to favour their proprietary technologies.[162]

3.5.2. Technology-neutral standard for Travel rule technology

When we think about the aim of technology neutrality, the standard for Travel rule technology should be formed so that it would not narrow the scope of technological solutions that can be used to achieve Travel rule compliance more than is necessary in order to have the minimum interoperability to the industry for the Travel rule purposes. In this respect the creators of standard must especially consider that standardisation itself narrows the scope of technological solutions for this purpose and especially that there is a risk that standardising might narrow the scope of technological solutions even more than creator of a standard could imagine at the time when the standard is created. Namely, once a standard has been created and implemented by the industry, the situation becomes "locked in", when new innovations "outside the standard" cannot compete in the market.[163] Even though there would not be "essential patents" for the standard at the creation moment, locked-in-situation may still bring in possibilities for technology providers to create certain IP-rights that can utilize the lock-in-situation. For example, certain patent holders could use their rights strategically to limit competition and to establish or retain their market power within the industry.[164] Thus, the standard creator should aim at a truly non-proprietary standard[165] that avoids subjecting the standard and the technology implementing it to commercial interests of

[162] Weinstein, S. N. (2021), *supra nota 88,* 559.
[163] Dolmans, M. (2010), *supra nota* 143, 199; and Wylly, P. (2015), *supra nota* 91, 310.
[164] Weinstein, S. N. (2021), *supra nota* 88, 515.
[165] Kroes, N. (2008), *supra nota 116.*

the technology's originator, if possible. If a standard would favour a technology for which a single firm has patent or relevant know-how, even though the standard could be implemented by using competing technology, the standard could through excess inertia[166] (a situation where none of the competing technologies gains popularity among the industry) actually lead to establish a new dominant position in the market that could be difficult for others challenge and would thus be harmful in terms of competition in the market.[167] These risks should be carefully taken into consideration when creating the standard.

On the other hand, lock-in-situation means that some possibilities are locked outside the standard, and this may not only exclude certain technologies and possibilities brought on by them, but also exclude certain future developments, like technological possibilities that future development of technologies might bring in later. Also, standardisation could possibly lead to loss of technologies that have some unique properties, which would be valued by some users, and market participants that have already invested into developing or deploying a technology which cannot be used to implement the standard could lose the investments made to "losing" technology.[168] To avoid such risks, at least at the time of creating the standard the institutions responsible for creating the standard should be enough aware of all technological possibilities available and used at the time as well as the consequences of choosing a specific technology.

The forementioned concerns drives to that the target standard should be as open as possible in respect of the technological solutions (and technology providers) that can implement the standard. If the standard and all the stakeholders and technology providers in the market are truly open, a good open standard should allow stakeholders to choose "best of breed" from different manufacturers and this would produce maximum efficiency.[169] Dolmans has listed six criteria that should be filled in the standard setting procedure when aiming to create an open standard:

1) *Open access to the decision-making process,*
2) *Open (transparent and undistorted) procedures in standard-setting bodies,*
3) *Open (published, pro-competitive) goals,*

[166] Fukami, Y. (2021), *supra nota* 135, 541.
[167] Braunstein, Y. M., White, L. J. (1986), *supra nota 125*, 694.
[168] *Ibid*., 693.
[169] Dolmans, M. (2010), *supra nota 143,* 199.

4) *Open (published, objective, relevant, qualitative, and verifiable) criteria for technology,*
5) *No overstandardization, and*
6) *Open access to the standard.*[170]

These criteria reflect the attributes (openness, consensus, balance and transparency) listed in the Commission's White Paper on Modernising ICT Standardisation in the EU - The Way Forward and at the same time the criteria developed within WTO for international standardisation organisations. At the same time the list reflects well the ideas behind technology-neutrality and thus this list could according to the author taken as a premise for creation of the discussed Travel rule compliance standard also.

[170] *Ibid*., 122-123.

4. NATIONAL REGULATOR'S RISK-BASED APPROACH TO TRAVEL RULE

4.1 Possibilities for a national regulator

Above in this study the author has stressed the urgency for national regulators to implement the FATF Travel rule on their national regulations (according to the FATF's Second 12-months Review, the implementation of the Travel rule by jurisdictions should be a "near-term priority"[171]). Also the author has presented problems that seems to be obstacles to the Travel rule implementation on national level, the main problem being that the VASPs do not yet have a common global technical standard on transferring the Travel rule data in between themselves. The author has also pointed out the conflict there might be in between the principle of technology-neutrality on the other hand, and the need for standardisation and/or technology-specific regulation on the other hand. The main question for this study is, how should a national regulator now balance between these conflicting principles, when taking steps towards implementing the Travel rule on their national regulation.

The aim for a national regulator should be, that the jurisdiction complies with the FATF Recommendation that requires implementing the Travel rule while the created legal framework would still be competitive enough for the crypto industry and give the VASPs located in this jurisdiction genuine possibility to operate, develop, grow and succeed in global competition. Applying the principle of technology neutrality, regulative framework should not limit the industry's possibilities to develop and utilize best possible technical solutions to comply with the Travel rule. In this respect, the question is, what should be the national regulator's approach toward the technology: should it give technology-specific regulation, even standardise the Travel rule compliance mechanisms or leave it completely to the industry to decide how it complies with the FATF Recommendations.

It seems clear that the only solution that can solve the problem Travel rule has set for the industry is standardising the transmission of necessary information between the VASPs. As concluded in chapter 3.4 of this study, standardisation can be acceptable in technology-neutrality's respect, when the good gained through standardisation over weights the narrowing of technological

[171] FATF (2021), Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota* 14, 36.

possibilities due to it. In regarding the Travel rule compliance mechanisms, standardisation can be easily supported against "ultimate" technology neutrality, as standardisation is actually necessary in order to solve the problem of the interoperability between different service providers and guarantee the interoperability later on, and, as explained in chapter 3.4, standardisation would also positively support the development of virtual asset market and the industry through the certainty and competitive advantages that successful standardisation could create.

Another question is, whether regulator should intervene the process of standardisation or should it be left to the market and/or the industry. As written in chapter 3.5.1 in this study, factors relating to technology neutrality, customers benefits and the time-schedule to achieve Travel rule compliance in the industry would according to the author's opinion call for regulators' intervention. Especially as the market seems yet too slow to find technical solution to the problem, the author suggests that regulators should intervene the process, at least in order to push the market towards standard. Fast and successful standardisation procedure would bring legal certainty for the industry, which could promote further innovation in the industry, as certainty would diminish fears of legal repercussions for entrepreneurial resolve in the industry.[172] Also, regulators' intervention could be a tool to manage the risk of *anticompetitive abuse of the standard-setting process*[173] that have been stressed in chapter 3.3 of this study, if regulator would involve into the actual standard-setting process and not only push the industry participants in creating the standard among themselves.

In the technology neutrality's respect, a national regulator 's two extreme options to push the crypto industry towards standardising the necessary transmission of information, would be either to:

1. set out a requirement for VASPs to comply with the Travel rule as of from certain set date, but leave the technical details and standardisation completely to the industry to agree upon during a set grace period; or
2. to set out a regulation that details the technology that VASPs should use in order to comply with the Travel rule and sets out a requirement for the industry to comply with the Travel rule as of from certain date by utilizing this referred technology.

[172] Finck, M. (2018), *supra nota 53,* 150.
[173] Weinstein, S. N. (2021), *supra nota* 88, 515.

Option 1 would be an easy one for a national regulator as it would not require the regulator to consider the technical possibilities that the VASPs in practise have. If we consider the question solely in the technology neutrality's point of view, this option 1 would be ideal way to reach standard, if only the market operates in ideal way (the decision on technology is based on merits of technology[174]) and is able to agree upon the standard during the given time. However, if a national regulator wants to respect the FATF guidelines, the planned regulation should entry into force shortly, and the practical problem relating to option 1 would be, as described earlier, that it is highly likely, that the crypto industry would not find a common global technical solution for Travel rule compliance among themselves as quickly as needed, in which case such a regulation would not meet the aims of being a competitive one for VASPs operating in this jurisdiction. Instead, such regulation would probably lead to weaken conditions for the VASPs located in that particular jurisdiction to compete in the global crypto markets as they would be obliged to implement Travel rule completely even if there would not be technological possibilities for them to co-operate with many counterparties. Thus, if option 1 would be chosen by a national regulator, additional activities by the national regulator or other public actor would be required in order to push the industry towards standardisation.

Main problem with option 2, on the other hand, would be that the need to standardise Travel rule technology is global, while a national regulator's competence is limited to its home jurisdiction. Thus, unless the national regulator coordinates the technical details with regulators of other jurisdictions, the end result of the option 2 would most probably be the same as with option 1: the VASPs operating under the regulation of this particular jurisdiction in question, would not have practical possibilities to operate in this global industry, if the VASPs located in other jurisdictions would not apply the same technical standard as required by the regulation in this specific jurisdiction, and so choosing option 2 would weaken the competition position of crypto industry in this particular jurisdiction, or possibly even lead to the end of the industry in this jurisdiction. Thus, choosing option 2 would not make sense either.

When considering the decision on the regulative approach in the technology neutrality's point of view, as described earlier in chapter 2 of this study, the principle of technology neutrality does not exclude the possibility that regulator takes a stand on technical questions and gives technology-specific regulation. Instead, the nature of the principle of technology neutrality seems to be rather

[174] Kroes, N. (2008), *supra nota* 116, 4.

relative than absolute. When creating regulation, the principle of technology neutrality should be assessed against other applicable principles and objectives of the created regulation. The regulation created as an end-result after the assessment should then establish appropriate balance among the conflicting values.[175] Thus, the principle does not forbid a regulator to consider technological differences. Up to some extent, combining technological neutrality and specificity could actually serve innovation through reducing legal uncertainty and limiting efforts to exploit regulatory ambiguity.[176] However, regulation should be created technologically neutral as far as possible and reasonable. As the aims of the technology neutrality are closely linked with competition issues, any regulation should especially be analysed against its economic and competitive effects in the market.[177] Considering the European single market and the competition between VASPs regulated in different jurisdiction inside the European Economic Area, neither of the options (1 and 2) sound appropriate as regarding the aim of level playing field inside the market. In order to support fair and level competition in the European single market, both of the options would require coordination on the European Union level in order for the regulative framework to be level for VASPs from different Member States. Also, in the eyes of the virtual asset industry, coordination throughout the European Union would probably be highly appreciated: in Neitz's query addressed to the blockchain industry leaders in the United States 2019, the industry leaders stated that they would appreciate uniformity of blockchain regulation across the United States.[178] Regulatory uniformity would make it easier for them to plan and expand their business across the United States.[179] The VASPs in the European Economic Area could benefit from uniformity of the Travel rule compliance requirements in the EEA similarly. On the other hand, without any coordination in the European Union level, differences in the approach to Travel rule by different jurisdictions could lead to the sunrise issue inside the European Economic Area.

Thus, considering the findings written in the chapters 2 and 3, as well as the considerations above in this chapter, the author does not find the principle of technology neutrality to set an obstacle for national regulator to intervene in creation of the necessary technological standard and, if necessary, to set technology-specific regulation. Thus, in the technology neutrality's respects, even the option 2 could be acceptable if it would lead to create the necessary certainty and level playing field in

[175] Hojnik, J. (2017). Technology neutral EU law: digital goods within the traditional goods/services distinction. International Journal of Law and Information Technology, 25(1), 63-[iii], 84.
[176] Greenberg, B. A. (2016), *supra nota 75,* 1500.
[177] Kamecke, U., Körber, T. (2008), *supra nota 26*, 331-332.
[178] Neitz, M. (2021), *supra nota 54.*
[179] *Ibid.*, and Reddy, A. (2018). Coinsensus: The Need for Uniform National Virtual Currency Regulations. Dickinson Law Review, 123(1), 251-280, 277.

the industry. The question is only about balancing the different principles and interests together in regulative actions. However, as explained earlier, due to the global nature of the crypto industry, technology-specific regulation on national level (option 2) is not a comprehensive solution to solve the Travel rule problematics either. The author suggests that ideal solution to the implementation of Travel on national level lies somewhere in between the options 1 and 2, but additional activities by public actors are needed to push the crypto industry towards standardisation.

4.2 Supranational consensus

On the basis of the reasoning written in this chapter, the author suggests that the best solution to find a common standard on Travel rule compliance, would be regulatory coordination on supranational level. In the European Union, the European Union would be natural framework to operate in terms of regulatory harmonization. A harmonized regulatory approach in the European Union would support the creation of necessary standard in the European Union. EU's active role in the standardisation process would also be supported by the aims to more agile and focused anticipation of needs for standardisation as set out in the new EU Strategy on Standardisation.[180]

The EU itself is that significant economic player in the global level, that the Union could try to coordinate the standardisation issue at a more global level also. Natural co-operation partners in this respect could be the United Kingdom and the United States. If a common approach to standardise Travel rule compliance mechanism would be found between the European Union and the United States, the created standard would most probably have rather global significance and would later be implemented by several other jurisdictions due to the economic relationships of dependence and the economic significance of these two economies. It is clear of course, that not even harmonized approach by the United States and the European Union would create a totally global standard, as not all the jurisdictions would join, but the author suggests that a common approach by the United States and the European Union would probably be the most comprehensive approach possible to reach at global level.

[180] European Commission. An EU Strategy on Standardisation; Setting global standards in support of a resilient, green and digital EU single market. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 2.2.2022 COM(2022) 31 final, 1.

However, we must consider that finding a common regulatory approach between the United States and the European Union might not be easy, and not that swift either. But the European Union could also try to approach the problem alone on the basis of its own values like the European Union did with the data protection framework by introducing the General Data Protection Regulation (GDPR). The GDPR was created as the European Union standard of data protection, but it ended up having implications outside the Union as several jurisdictions outside the EU are adopting principles arising out of the GDPR to their national regulation and the EU rules have also been successful at shaping foreign companies' practises even when they operate outside the EU. The adoption of the GDPR principles outside the European Union has surely been partly due to the requirements the GDPR sets for all transfers of personal data to third countries (that personal data must enjoy adequate protection in the third country, to which personal data is transferred from the EU[181]), but also due to the so called "first mover advantage" and the lack of a widely accepted, comprehensive alternative for it.[182] This way, the GDPR has been a European success story in creating a multinational standard in the field of data protection. The same way the author suggests that the European Union should seek to take the advantage of the first regulator (or one of the first ones) in reaching a standard on Travel Rule compliance. If the European Union would be able to achieve a common standard of transferring the Travel rule data among the VASPs in the European Union, the same approach could be adopted on more global level also. And the same way as with the GDPR, the European VASPs could then be required by the European Union regulation to require their counter-VASPs in third countries to transmit the necessary Travel rule data to the European VASPs in order for the European VASPs to co-operate with them. However, in the crypto industry's respect we must also remember that not even this kind of pushing of a European standard would solve the whole problem as not all the transfers of virtual assets are transferred by using regulated VASPs.

4.3 Risk-based approach for interim period

Even though the author considers that common European standard to Travel rule compliance is highly required and possible to reach, we must consider that achieving such a standard even at

[181] Roos, A. (2020). The European Union's General Data Protection Regulation (Gdpr) And Its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. Comparative And International Law Journal of Southern Africa, 53(3), 1-37, 5.

[182] Pernot-Leplay, E. (2020). EU Influence On Data Privacy Laws: Is The Us Approach Converging With The EU Model?. Colorado Technology Law Journal, 18(1), 25-48, 25-29.

European level would take more time than a national regulator now have to implement the Travel rule on national regulation. The same goes if regulators settle for waiting the standardisation to happen in the market. Thus, we return to consider the national regulator's options in the present situation as it seems clear that there will have to be an "interim period" on national level for the time when we are still waiting for the common global standard to develop.

On its Second 12-month Review FATF stated that jurisdictions may implement the Travel rule in a *"staged approach"* supplementing this statement with the following explanation:

> *"For example, requirements may be introduced with a 'grace period' where the requirements are introduced but not yet enforced. Alternatively, jurisdictions may allow for the introduction of partial or temporary measures for a transitional period."*[183]

However, when deploying the so-called staged approach, the countries should according to the FATF's Updated Guidance for a Risk-Based Approach *"continue to ensure that VASPs have alternative measures in place to suitably mitigate the ML/TF risks arising from VA transfers in the interim"*. Also, FATF emphasizes in the Updated Guidance for a Risk-Based Approach the possibilities for originating entities to require Travel rule compliance from the beneficiary entities by contract or business practise, and the VASPs responsibility to take into account the level of ML/TF risks related to each customer and counterparty VASP.[184] According to the author's interpretation of these guidelines, the interim regulative approach, before the full compliance with Travel rule, would be such that would require the VASPs full compliance with Travel rule in transfers with such counterparty VASPs whose home jurisdiction have already implemented the Travel rule, while other measures aligned according to risk-based approach would be required for interaction with counterparty VASPs from other jurisdictions, possibly even refusing from interaction with such VASPs.

Thus, even though an exemption for full compliance with Travel rule would be granted for VASPs in a national regulation until the Travel rule compliance measures are enough standardised, it is

[183] FATF (2021), Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, *supra nota 14*, 36.
[184] FATF (2021), Virtual Assets and Virtual Asset Service Providers. Updated Guidance for a Risk-Based Approach, *supra nota 39*, 64.

clear, that the originator VASPs should be required to collect the necessary beneficiary information from the originator of each transfer regardless of the beneficiary VASP. Even though sending the information for the beneficiary VASP would not be technically possible yet, there is no reason why the originator VASP would not also be required to retain the beneficiary information as the Travel rule would expect.

The questions that the above referred FATF guidelines to do not give straight answer to are, first, the question of how a regulator should approach the question of transmitting of the collected originator and beneficiary data in the interim period for counterparty VASPs, and secondly, how a regulator and VASPs should treat counterparty VASPs from countries that have not implemented Travel rule yet.

Even though, as described above, FATF states that VASPs have possibility to require compliance with Travel rule from their counterparty VASPs regardless of their jurisdiction, the author argues that it is probably not a realistic variant in global scale yet as it would require setting out individual processes on transmitting the Travel rule data with each counterparty VASP and would probably be too big a burden for many small VASPs. And considering the usual imbalance on contractual relationships between smaller and bigger counterparties, small VASPs would probably just not be able to require the information transmitting from bigger counterparty VASPs in jurisdictions that do not yet require similar implementation of Travel rule. And this could practically drive small VASPs from smaller economies like Estonia or Finland out of the market, if they would not be able to conclude transactions with many bigger VASPs. Thus, the author considers that transferring the Travel rule data between all counterparty VASPs should not be required at this stage by national regulation. However, as the regulation should push the industry towards standardisation, it is worth to consider whether transmitting the Travel rule data between the VASPs should be required at some level as requiring it at some transactions could push the industry participants to take into use, develop and test some technical solutions. This could drive the industry on national level towards standardisation and could possibly contribute to the development towards standardisation and Travel rule compliance outside the borders of that jurisdiction as well. For example, the VASPs could be required to transmit the Travel rule data in between themselves on transactions that are committed between originator and beneficiary VASPs that are both locals in that same jurisdiction. If there are enough economic solutions available for the VASPs to use, this could be reasonable solution for the start as the author believes that on national level, at least on small jurisdictions the VASPs would have genuine possibility to enough easily agree upon a solution that would be used

to transfer the Travel rule data. On the other hand, the regulator should take economic issues into consideration and not to make a jurisdiction a test environment, if it would require inconsiderable resources and investments from the VASPs taking into consideration that the global standard that will hopefully be reached in the future could require another technical solution that the VASPs would then need to deploy to replace the national system they would have deployed earlier.

Also, a regulator could consider some kind of a reward and punishment mechanism for the interim period to supper the full implementation of Travel rule: this kind of mechanism could possibly be created through the due diligence requirements that FATF according to the Updated Guidance for a Risk-Based Approach would require to be applied during the interim period, when not completing the Travel rule requirements completely.[185] Thus, VASPs should be required to apply certain enhanced measures when completing transfers with counterparty VASPs with whom there is no mechanism in place to send and receive the Travel rule data.

Nevertheless, in this interim period at least some part of transactions, if not all, between VASPs would stay outside of the scope of transmission of the Travel rule data, and according to the FATF's Updated Guidance for a Risk-Based Approach the approach towards such transactions should be taken on a risk-based approach by considering especially the ML/TF risks related to each customer and counterparty VASP.[186] According to the authors understanding this assessment of each customer and counterparty VASP could base for example on the following factors:

a. whether the counterparty VASP is able to transfer/receive and retain the necessary Travel rule data as required by Travel rule,
b. whether the jurisdiction of the counterparty VASP has implemented the Travel rule and what is the level of Travel rule implementation in that jurisdiction, and
c. what is the common ML/TF risk level of the jurisdiction of the customer/counterparty VASP (if the jurisdiction is a high-risk jurisdiction).

Of course, the assessment of the risks related to each customer and counterparty VASP should include other relevant factors as required by the other applicable FATF guidelines. In order to comply with the guideline as set out in the paragraph 200 of the Updated Guidance for a Risk-Based Approach and to ensure that *"VASPs have alternative measures in place to suitably mitigate*

[185] *Ibid.*
[186] *Ibid.*

the ML/TF risks arising from VA transfers in the interim"[187], a regulator should require VASPs when not transferring or receiving Travel rule data from counterparty VASPs to apply additional measures to mitigate ML/TF risks. According to the author, such measures could for example be:

> 1) applying enhanced due diligence measures to such transfers, and
> 2) based on the assessment of the customer and counterparty VASP as referred above (a-c) to, for example, refuse from transactions with counterparty VASPs that involve exceptionally high ML/TF risk.

These regulative requirements for VASPs during the interim period would according to the author's understanding fill in the requirements set out for the national regulators by the Travel rule. However, as mentioned, the author sees that additional coordinating steps would be required from public authorities in supranational level in order to drive the industry towards common global standard and full compliance with the Travel rule enough quickly. Thus, it might be necessary to set out some final deadline for full Travel rule compliance even on national level. However this deadline should ideally be coordinated supranationally also, and the period to that deadline should be enough long so that the industry will have enough time to agree on the standard. However, there is also the contrast with such deadlines, that often if a deadline is given, the necessary change will happen in the market at the time of the deadline and no earlier even though there would be possibilities to that.

[187] *Ibid.*

CONCLUSION

As described in this study, the implementation of FATF Travel rule for VASPs on national level seems to be stuck to a great extent. The difficulties that national regulators now have in regarding their approach to the Travel rule are due to the technological differences there are in conducting transfers in cryptocurrencies when compared to transfers in fiat-currencies by traditional financial institutions, but especially due to the immaturity of common industry standards among VASPs. The key to solve this problematic would be a common standard for transmitting the Travel rule data between VASPs around the world, which should now be promptly created. Yet the attempts to solve the problem and create this standard is in "self-reinforcing conundrum", as FATF has described in its Second 12-months Review, where both the industry and regulators seem to wait for the other one to take the next step. This study aimed to research, how a national regulator should implement the Travel rule into its national regulation while global standard to comply with the Travel rule do not exist yet.

When taking into consideration the substantial social interest to intervene the use of cryptocurrencies in money-laundering, in which regard the implementation of Travel rule is crucial step forward, and the ambition to encourage the development of stable while innovative virtual asset market in the European Union, legal certainty on Travel rule implementation is needed both national and EU level without delay. As argued earlier in chapter 4.1 of this study, the author considers that regulator's prompt intervention to the process of standardising the Travel rule compliance technology is required in order to speed up the standardisation. Also, as argued earlier in chapter 4.1, the author does not consider the principle of technology neutrality as an obstacle for regulators intervention in standardising the Travel rule compliance technology. On the contrary, the author considers that regulator's intervention that would bring legal certainty regarding the Travel rule compliance would create credibility and stability to the crypto industry and would thus further promote the crypto industry's and VASP's possibilities to compete with traditional financial industry and financial institutions. Thus, regulator's intervention could be perfectly justified in regarding the principle of technology neutrality, as technology neutrality is not absolute, but rather relative principle, that must be balanced with other principles and objectives in an individual case.

However, when taking into consideration the global nature of the crypto industry and a single VASPs need for interoperability with other VASPs in other jurisdictions, an idea that national regulator in a small state like Estonia or Finland, for example, would set out a standard for transmitting of Travel rule data, do not sound viable, because as argued more specifically in chapter 4.1 in this study this kind of approach by national regulator would probably lead to weaken the competitiveness of VASPs located in that jurisdiction, but not probably to the creation of the needed global standard.

As a solution to this problem of incomplete standardisation, which calls for regulator's intervention, but on which a single national regulator is incompetent to act effectively, the author suggests coordination of the standardisation process on European Union level. Timely and technical coordination of the Travel rule compliance on EU level would guarantee level playing field for VASPs in the Union and avoid the so-called sunrise issue that could born due to different approaches and states of implementation among the Member States. The crypto industry in the European Union could benefit from prompt and uniform standardisation process through the legal certainty and stability, which would encourage the development of the industry in the European Union and possibly enhance the European crypto industry's competitiveness on global scale. Such development would be consistent with the European Commission's objectives to create comprehensive legal framework for the crypto assets as set out in the MiCA Proposal. Also, as described in chapter 4.2 in this study the European Union could take advantage of the first regulator in reaching a standard on Travel rule compliance. If the European Union would be able to achieve a common standard of transferring the Travel rule data among the VASPs in the European Union, the same approach could be adopted on more global level also. European Travel rule compliance standard could thus be a small part of the whole framework for virtual assets that could make the European Union a global trend-setter on virtual assets regulation and the European regulative framework for virtual assets similar success story as the GDPR has been in terms of its implementation by third countries. The global effects of the EU standard on Travel rule compliance could of course even be more significant, and more valuable for the crypto industry, if the European Union would be able coordinate the standardisation process together with the United States and/or the United Kingdom.

As a conclusion of this study, the author suggests that national regulator of a jurisdiction bound by the FATF Recommendations should take urgent action to implement the Travel rule and promote

the standardisation of Travel rule compliance mechanisms on the industry. Different possible regulatory actions and approaches has been analysed in the chapter 4 of this study. As a national regulator's possibilities to influence the global standardisation procedure are very limited, the first step that each national regulator should now take in order to implement the Travel rule, would be to require the VASPs operating in their jurisdiction to comply with the Travel rule as far as possible without common standard on transferring the Travel rule data globally among the industry. This would mean for example, that originator VASP of a transaction would be required to collect the full originator and beneficiary data from the originator of a transaction and retain this data.

Thus, even though an exemption for full compliance with Travel rule would be granted for VASPs in a national regulation until the Travel rule compliance measures are enough standardised, it is clear, that the originator VASPs should be required to collect the necessary beneficiary information from the originator of each transfer regardless of the beneficiary VASP. Even though sending the information for the beneficiary VASP would not be technically possible yet, there is no reason why the originator VASP would not also be required to retain the beneficiary information as the Travel rule would expect. In addition to that, a national regulator could evaluate, whether there would be fair possibilities to require closer-to-full-compliance with the Travel rule for the VASPs in its jurisdiction, for example requiring transferring the Travel rule data between certain counterparty-VASPs, for example other VASPs from this same jurisdiction. This kind of additional requirements could however according to the author be set only as far as compliance with such additional requirement would not require excessive actions from the VASPs. In the interim period, when full compliance with Travel rule would not be reached due to the lack of common standard, a regulator should however require VASPs to apply risk-based approached and possibly enhanced due diligence requirements on transactions and counterparty-VASPs, when full compliance with the Travel rule is not applied. As suggested in chapter 4.3 of this study, a national regulator could also consider some kind of a reward and punishment mechanism for the interim period to support the full implementation of Travel rule, for example through fair and feasible due diligence requirements set out for transactions not complying fully with the Travel rule during the interim period.

Even though supranational attempts are required in order to create common global standard, national regulators do play yet key role on pushing the industry towards standardisation and Travel rule compliance. Requiring the VASPs operating in the jurisdiction to comply with the Travel rule at feasible extent would push the industry towards full compliance and create pressure to create

solutions forward. Referring to many sources referred in this study, the author concludes that national regulators should not refrain from implementing the Travel rule on national regulation due to the uncertainties relating to the compliance with Travel rule. Instead, requiring the crypto industry to comply with the Travel rule at appropriate extent could possibly benefit the industry and VASPs in the regulator's jurisdiction, if the requirements set out by the regulator are fair, feasible and unbiased and do not require something that is yet not possible due to the immature standardisation process.

LIST OF REFERENCES

Scientific books

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

2. Veerpalu, A., Ebers, M., Osula, A., Norta, A. & Tartu Ülikool. Õigusteaduskond (2021). Regulatory challenges to the use of of distributed ledger technology: Analysis of the compliance of existing regulation with the principles of technology neutrality and functional equivalence. Tartu: University of Tartu Press.

Scientific articles

3. Aiyar, K., Halgamuge, M. N., Mason, N. (2021). Blockchain and Cryptocurrencies: Legal and Ethical Considerations. Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector. IGI Global, March 2021, 132-152. Retrieved from Retrieved from https://www.researchgate.net/publication/349753192_Blockchain_and_Cryptocurrencies_Legal_and_Ethical_Considerations, 30 March 2022.

4. Albrecht, C., Duffin, K., Hawkins, S., Morales Rocha, V. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210-216.

5. Bagus, P., De la Horra, L. (2021). An ethical defense of cryptocurrencies. Business Ethics, the Environment & Responsibility, 30 (3), 423– 431.

6. Bekkers, R., Iversen, E., Blind, K. (2012). Emerging ways to address the reemerging conflict between patenting and technological standardization. Industrial and Corporate Change, 21(4), 901-931.

7. Braunstein, Y. M., & White, L. J. (1986). Setting technical compatibility standards: an economic analysis. Journal of Reprints for Antitrust Law and Economics, 16(2), 685-[ii].

8. Dolmans, M. (2010). A tale of two tragedies- pleas for open standards. International Free and Open Source Software Law Review, 2(2), 115-138.

9. Donmez, C., Sen, D., Dereli, A., Horasan, M., Yildiz, C., Kaplan Donmez, N. (2021). An Investigation of Fiat Characterization and Evolutionary Dynamics of the Cryptocurrency Market. *SAGE Open, 11*(1).

10. Dupuis, D., Gleason, K. (2020). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. Journal of Financial Crime, 28(1), 60-74.

11. Ewertsson, L. (2010). Is Seeing Believing?: The Experimental Production of Technical Standards for HDTV. East Asian Science, Technology and Society, 4(3), 383-418.

12. Farrell, J., Simcoe, T. (2012). Choosing the rules for consensus standardization. The Rand Journal of Economics, 43(2), 235-252.

13. Foley, S., Karlsen, J., Putniņš, T. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? The Review of Financial Studies, 32(5), 1798-1853.

14. Fukami, Y. (2021). Open and Clarified Process of Compatibility Standards for Promoting Data Exchange. The Review of Socionetwork Strategies, 15(2), 535-555.

15. Gonzálvez-Gallego, N., Pérez-Cárceles, M. (2021). Does goodness of governance dissuade citizens from using cryptocurrencies? Economics & Sociology, 14(1), 11-27.

16. Greenberg, B. A. (2016). Rethinking technology neutrality. Minnesota Law Review, 100(4), 1495-1562.

17. Hojnik, J. (2017). Technology neutral EU law: digital goods within the traditional goods/services distinction. International Journal of Law and Information Technology, 25(1), 63-[iii].

18. Kaal, W. A. (2021). Digital asset market evolution. Journal of Corporation Law, 46(4), 909-964.

19. Kamecke, U., Körber, T. (2008). Technology neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood. European Competition Law Review, 29(5), 330-337.

20. Kiviat, T. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal, 65*(3), 569-608.

21. Koops, B-J (2006). "Should ICT Regulation Be Technology-Neutral?", in Koops et al. Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners, IT & Law Series, Vol. 9 (77-108). The Hague: T.M.C. Asser Press.

22. Lee, J., Long, A., McRae, M., Steiner, J., Handler, S. (2015). Bitcoin Basics: A Primer on Virtual Currencies. Business Law International, 16(1), 21-48.

23. Lee, M., Frank, L., IJsselsteijn, W. (2021). Brokerbot: A Cryptocurrency Chatbot in the Social-technical Gap of Trust. Computer Supported Cooperative Work, 30(1), 79-117.

24. Luther, W. (2016). Bitcoin and the Future of Digital Payments. The Independent Review (Oakland, Calif.), 20(3), 397-404.

25. Naheem, M. (2018). Regulating virtual currencies, the challenges of applying fiat currency laws to digital technology services. Journal of Financial Crime, 25(2), 562-575.

26. Neitz, M. (2021). How To Regulate Blockchain's Real-Life Applications: Lessons From The California Blockchain Working Group. Jurimetrics (Chicago, Ill.), 61(2), 185-217.

27. Panova, O., Leheza, Y., Ivanytsia, A., Marchenko, V., Oliukha, V. (2019). International Models of Legal Regulation and Ethics of Cryptocurrency Use: Country Review. Journal of Legal, Ethical and Regulatory Issues, 22 (2).

28. Pernot-Leplay, E. (2020). EU Influence On Data Privacy Laws: Is The US Approach Converging With The EU Model?. Colorado Technology Law Journal, 18(1), 25-48.

29. Reddy, A. (2018). Coinsensus: The Need for Uniform National Virtual Currency Regulations. Dickinson Law Review, 123(1), 251-280.

30. Reed, C. (2007). Taking Sides on Technology Neutrality. *SCRIPT-ed, 4*(3), 263-284.

31. Reijers, W., Coeckelbergh, M. (2016). The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. Philosophy & Technology, 31(1), 103-130.

32. Riillo, C., Allamano-Kessler, R., Asnafi, N., Fomin, V., Van de Kaa, G. (2022). Technological Uncertainty and Standardization Strategies: A Coopetition Framework. IEEE Transactions on Engineering Management, 1-14.

33. Roos, A. (2020). The European Union's General Data Protection Regulation (GDPR) And Its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. Comparative And International Law Journal of Southern Africa, 53(3), 1-37.

34. Shadikhodjaev, S. (2021). Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? European Journal of International Law, 32(4), 1249-1282.

35. Simcoe, T. (2012). Standard Setting Committees: Consensus Governance for Shared Technology Platforms. The American Economic Review, 102(1), 305-336.

36. Soana, G. (2022). Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry? Economic Notes - Monte Paschi Siena, 51(1), N/a.

37. Turner, A., Irwin, A. (2018). Bitcoin transactions: A digital discovery of illicit activity on the blockchain. Journal of Financial Crime, 25(1), 109-130.

38. Van Eecke, P., Truyens, M. (2008). Standardization in the european information and technology sector: official procedures on the verge of being overhauled. Shidler Journal of Law, Commerce & Technology, 5(3), 1-9.

39. Veerpalu, A. (2018). Decentralised Technology and Technology Neutrality in Legal Rules: An Analysis of De Voogd and Hedqvist. Baltic journal of law & politics, 11(2), 61–94.

40. Weinstein, S. N. (2021). Blockchain neutrality. Georgia Law Review, 55(2), 499-592.

41. Wylly, P. (2015). Evaluating the costs of technology neutrality in light of the importance of social network influences and bandwagon effects for innovation diffusion. New York University Environmental Law Journal, 23(2), 298-353.

Estonian legislation

42. Money Laundering and Terrorism Financing Prevention Act [Rahapesu ja terrorismi rahastamise tõkestamise seadus]. RT I 17.11.2017, 2.

EU and international legislation

43. 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.

44. 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. 78.

45. 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 (the 4th AML Directive). OJ L 141, 5.6.2015, p. 73–117.

46. 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 (the 5th AML Directive or AMLD) PE/72/2017/REV/1, OJ L 156, 19.6.2018, p. 43–74.

Other sources

47. Commission of the European Communities. White Paper On Modernising ICT Standardisation In The EU - The Way Forward. Brussels, 3.7.2009. COM(2009) 324 final.

48. Countries. FATF. Retrieved from https://www.fatf-gafi.org/countries/, 29 January 2022.

49. Crypto.com (2020). FATF Travel Rule. A Brief Introduction. Retrieved from https://assets.ctfassets.net/hfgyig42jimx/7ezqnx47HERbjVAofseOnf/792ed1f4c49384a65541aa4456cf037d/Crypto.com_Macro_Report_-_FATF_Travel_Rule.pdf, 29 January, 2022.

50. European Commission. An EU Strategy on Standardisation; Setting global standards in support of a resilient, green and digital EU single market. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Brussels, 2.2.2022 COM(2022) 31 final.

51. European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, Study on developments with regard to virtual assets users and the possibility to set-up and maintain a central database registering users' identities and wallet addresses accessible to financial intelligence units (FIUs)", Publications Office, 2021.

52. European Commission, Financial Stability, Financial Services and Capital Markets Union. Anti-Money laundering and countering the financing of terrorism legislative package. Press Release, 20 July 2021. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690, 21 March 2022.

53. European Commission. Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (2021/0241).

54. European Commission. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and amending Directive (EU) 2019/1937 (2020/0265).

55. FATF. High-Risk Jurisdictions subject to a Call for Action – October 2021. Retrieved from http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2021.html, 4 May 2022.

56. FATF (2012-2021), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France. Retrieved from www.fatf-gafi.org/recommendations.html, 29 December 2021.

57. FATF. Jurisdictions under Increased Monitoring – October 2021. Retrieved from http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html, 4 May 2022.

58. FATF (2021), Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. July 2021. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf, 12 December 2021.

59. FATF (2014). Virtual Currencies. Key Definitions and Potential AML/CFT Risks. Financial Action Task Force. June 2014. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, 30 March 2022.

60. FATF (2021). Virtual Assets and Virtual Asset Service Providers. Updated Guidance for a Risk-Based Approach. October 2021. Retrieved from https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html, 12 December 2021.

61. FIN-FSA. Financial Supervisory Authority (2019). What do the terms virtual currency, cryptocurrency, crypto asset, ICO and wallet service mean? Retrieved from https://www.finanssivalvonta.fi/en/Consumer-protection/virtual-currencies/, 4 May 2022.

62. Gromek, M. (2020, October 31). Ransom Hackers In Finland Are Using Psychotherapy Medical Records As Ammunition. Forbes. Retrieved from https://www.forbes.com/sites/michalgromek/2020/10/31/ransom-hackers-in-finland-are-using-psychotherapy-medical-records-as-ammunition/?sh=3272f3fa2f2e, 13 December 2021.

63. Houben, R., Snyers, A. (2018). Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion. Study requested by the TAX3 committee. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies. Retrieved from www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf, 2 April 2022.

64. IFAC (2020). Anti-money laundering: the basics. Retrieved from https://www.ifac.org/system/files/publications/files/Anti-Money-Laundering-The-Basics-Installment-7-Virtual-Assets.pdf, 4 May 2022.

65. Kroes, N. (2008). Being open about standards. Speech to OpenForum Europe, Brussels, June 10, 2008. SPEECH/08/317. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/speech_08_317, 17 April 2022.

66. Mutual Evaluations. FATF. Retrieved from https://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate), 29 January 2022.

67. 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". Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:26030103_1, 27 February 2022.

68. UNCITRAL Model Law on Electronic Signatures with Guide to Enactement (2001). Retrieved from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf, 17 March 2022.

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[188]

I Jani Ultamo

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis

Regulatory Approach to Implement the FATF Travel Rule on Transfers of Crypto-Assets – Fitting Together the Need for Standardisation and the Principle of Technology Neutrality,

supervised by Thomas Hoffmann and Henrik Mägi,

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.5.2022

[188] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*