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

Tuomas Capraro

THE 5th ANTI-MONEY LAUNDERING DIRECTIVE IN THE LIGHT OF VIRTUAL CURRENCIES: THE EXPLOITATION OF THE DECENTRALIZED SYSTEM AND RISING LEGISLATIVE CHALLENGES

Bachelor's thesis
HAJB08/17 - Law, European Union and International Law

Supervisor: Agnes Kasper, PhD

Tallinn 2021

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 11003 words from the introduction to the end of conclusion.

Tuomas Capraro

183934HAJB

tuomas.capraro@icloud.com

Supervisor: Agnes Kasper

The paper conforms to requirements in force
……

Chairman of the Defence Committee:
Permitted to the defence
……

TABLE OF CONTENTS

ABSTRACT 4
INTRODUCTION 5
1. UNDERSTANDING VIRTUAL CURRENCY 7
1.1. Characteristics 7
1.2. The blockchain technology 8
1.3. Monetary policy 10
2. VIRTUAL CURRENCY IN THE LIGHT OF MONEY LAUNDERING AND TAX EVASION SCHEMES 12
2.1. Money laundering 12
2.2. Virtual currency and money laundering 14
2.3. Tax evasion 17
3. THE EUROPEAN UNION AND U.S. APPROACH 20
3.1 Past measures and calls for regulation 20
3.2 The 5th Anti-Money Laundering Directive 21
3.3 Virtual currencies in the United States 24
4. PROPOSED AMENDMENTS TO THE 5th ANTI-MONEY LAUNDERING DIRECTIVE AND FUTURE LEGISLATION 27
4.1 Amendments proposed to the 5th Anti-Money Laundering Directive 27
4.2 The future of virtual currency regulation 29
4.2.1 Markets in Crypto-Assets Regulation 29
4.2.2 The 6th Anti-Money Laundering Directive 30
CONCLUSION 32
LIST OF REFERENCES 34
Appendix 1. Non-exclusive licence 39

ABSTRACT

The legal position of virtual currency service providers and the regulation regarding the field has been an important regulatory question in the European Union for a long period of time. After concerns were raised by European lawmakers, the EU decided to regulate virtual currency service providers and include them to the scope of the 5th Anti-Money Laundering Directive (AMLD5). The AMLD5 presented new AML obligations to service providers within the field, and further provided important definitions regarding the virtual currency market.

The aim of the present thesis is to briefly present the technology behind virtual currencies, analyse the AMLD5 and more importantly review the AML obligations which have been imposed to different service providers in the field of virtual currency markets. The thesis aims to review the effectiveness of the Directive, and present suggested amendments. Qualitative research methods are used in the thesis relying on, *inter alia*, European Union legislation, national legislation and articles written by legal scholars in peer-reviewed journals.

The hypothesis of the thesis is that although the European Union has provided clarity to the field of virtual currencies by adopting the AMLD5, it simply does not correspond to the regulatory requirements of a quickly evolving field and lacks in the definitions presented. As the outcome of the thesis indicates, the definitions laid down in the AMLD5 are narrow in their nature and therefore exclude important aspects from the scope and the list of obliged entities arising from the Directive.

Keywords: anti-money laundering, virtual currencies, 5th Anti-Money Laundering Directive, European Union

INTRODUCTION

The fast emergence and constant growing popularity of the use of cryptocurrencies has been a frequent topic of discussion over the past few years. Being a field which is still quite vaguely legislated, the position of, for example, service providers within the market has been an uncertain factor for a long period of time in the European Union. Although cryptocurrencies facilitate concluding business transactions by possessing a decentralized system and a consensus validation mechanism, the absence of central authorities or banks increases the risk of criminal conduct related to cryptocurrencies. As a response to the uncertain atmosphere of the field, the European Union adopted the 5th Anti-Money Laundering Directive in 2018 which for the first time included virtual currency providers and custodian wallet providers into the list of obliged entities to follow EU anti-money laundering obligations and procedures.

This graduation thesis provides a comprehensive overview of the different functions of virtual currencies in the context of money laundering schemes as well as systematically explains how virtual currencies are used in the laundering process. Furthermore, it examines the current virtual currency legislative framework of the European Union with a special attention to the 5th Anti-Money Laundering Directive. The aim of the paper is to provide an analysis of the Directive and the AML obligations introduced to service providers within the virtual currency market as a result of the adoption of the Directive, and to contribute to a topical and quickly evolving area of legislation. The thesis seeks to answer to the questions of what kind of virtual currency regulation preceded the 5th Anti-Money Laundering Directive, what kinds of amendments regarding virtual currencies and service providers were introduced by the Directive, and how will virtual currencies be regulated in the future.

This paper relies on qualitative research methods using sources such as European Union legislation, national legislation as well as official reports issued by different bodies within the European Union. Research articles and other articles by legal scholars in peer-reviewed journals analysing and discussing virtual currencies in the context of money laundering schemes are also used as qualitative sources in the thesis. As a very topical and recent field, virtual currency

regulation does not include a substantial amount of case law at this time, but despite this some case law regarding the taxation and criminal misuse of virtual currencies is presented.

Chapter one aims at introducing the concept of virtual currencies and explaining their key characteristics and the technology behind them. It presents the decentralized nature of the currency, which is a key distinctive feature of virtual currencies. The relationship between virtual currencies and authentic central bank-issued currencies is covered, and a brief introduction to the blockchain technology and distributed ledger technology is given.

Chapter two discusses the crime of money laundering in a general manner, describing the different stages of the process, the goals which are expected to be achieved with a laundering scheme and the definitions given in legislation. It also investigates the means and methods of the laundering process from the viewpoint of laundering operations through virtual currencies. Issues related to tax evasion are also briefly presented.

Chapter three focuses on the legislative framework of virtual currencies within the European Union by presenting past measures and having a particular focus on the 5th Anti-Money Laundering Directive. It will discuss the provisions of the Directive in a detailed manner and present the changes in AML obligations of service providers within the virtual currency market.

Chapter four brings forward the expected measures regarding virtual currencies which will be adopted in the future. It will present some problematic areas within the legislative framework and examine possible solutions. The recent proposal for the Markets in Crypto-Assets Regulation, and the changes presented in the proposal regarding virtual currencies will also be covered in the chapter.

The expected outcome of the research is that even though legislative steps regarding virtual currencies have been made, they have not solved essential issues related to the prevention and tracing of illegal activities. Virtual assets continue to offer criminals a more anonymous and discrete way of concluding transactions. Furthermore, the European Union needs to adopt more comprehensive rules regarding the whole virtual currency market as setting AML obligations is only a part of the regulatory potential. However, as the field of virtual currencies is a relatively new one, it is going to take time before legislators can determine the aspects which have a need to be regulated within the field.

1. UNDERSTANDING VIRTUAL CURRENCY

1.1. Characteristics

Commercial transactions and their nature have changed substantially at the beginning of the 21st century. As e-commerce continues to fortify its position in international trade, innovations of payment services and service providers have risen to the surface. An important development has been the introduction of virtual currencies.[1] There are different types of virtual currencies such as closed system virtual currencies, unidirectional virtual currencies, and bidirectional virtual currencies.

Closed virtual currency schemes lack almost any link to the real economy and are usually applied only in online video games. As an example, users pay a subscription fee and earn money based on their performance on the game. This kind of virtual currency can be spent only for purchasing virtual goods or services offered by the game. Unidirectional virtual currencies can be directly bought using authentic currency, but they cannot be exchanged back to the original authentic currency. The conditions which apply to the conversion are established by the scheme provider. Facebook Credits are a good example of unidirectional virtual currencies. The system allowed users to buy virtual goods on the Facebook platform and it was possible to obtain the currency using a variety of payment methods such as PayPal.[2] The last type, bidirectional virtual currencies, can be obtained against authentic currency and exchanged back as well. As an example, we could mention cryptocurrencies, such as Bitcoin. In comparison to authentic currency, the key distinctive feature which cryptocurrencies possess is that they are not issued by a central authority.[3] In

[1] Vandezande, N. (2017). Virtual Currencies Under EU Anti-Money Laundering Law. *Computer Law & Security Review*, 33 (3), 341-353.
[2] European Central Bank. (2012). *Virtual Currency Schemes.* Retrieved from: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf , 21 November 2020.
[3] Vandezande (2017), *supra nota* 1, 341.

addition to the fact that the flows in cryptocurrencies are bidirectional, their exchange rate varies in accordance with supply and demand.[4]

The present thesis will be focused primarily on bidirectional virtual currencies, and more importantly, on cryptocurrencies. Generally, almost every cryptocurrency can be obtained in exchange for authentic currency or for other kinds of cryptocurrency. The exchange can be performed online at different trading platforms and offline by using certain Automatic Teller Machines (ATMs).[5] Cryptocurrencies are electronic cash systems in which online payments can be executed from one individual to another without the currency going through any financial institutions. As opposed to many other available financial assets, they lack any association with a higher authority. Additionally, unlike many other financial assets, the value of cryptocurrencies is not linked to the economy of a country or a corporation. The value of cryptocurrencies is based on an algorithm, which can trace all transactions. The popularity and fast growth of cryptocurrencies can be associated with low transaction costs and government-free design and development.[6]

1.2. The blockchain technology

The blockchain technology has grown rapidly in the past few years, and as a result the development of applications basing their functions to the blockchain has begun to change the whole financial sector. In addition to the bitcoin, blockchain technology is used in a wide range of applications including platforms for issuing and trading equity shares and corporate bonds.[7] The concept of blockchain was originally brought forward in 2008 by Satoshi Nakamoto in connection with presenting Bitcoin, a software for transferring digital cash free of financial intermediaries and central bank interference.[8] The blockchain technology has many different benefits, which include anonymity and decentralization. There are many applications which utilize the technology of

[4] Peters, G.W., Chapelle, A., Panayi, E. (2016). Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective. *Journal of Banking Regulation,* 17 (4), 239-272.
[5] Dierksmeier, C., Seele, P. (2018). Cryptocurrencies and Business Ethics. *Journal of Business Ethics,* 152 (1), 1-14.
[6] Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L. (2019). Cryptocurrencies as a Financial Asset: A Systematic Analysis. *International Review of Financial Analysis,* 62, 182-199.
[7] Rennock, M. J. W., Cohn, A. Butcher, J. R. (2018). Blockchain Technology and Regulatory Investigations. *Practical Law The Journal,* 4, 35-45.
[8] Grover, P., Kar, A., Janssen, M. (2019). Diffusion of Blockchain Technology: Insights From Academic Literature and Social Media Analytics. *Journal of Enterprise Information Management,* 32 (5), 735-757.

blockchain, which range from cryptocurrency and financial services to risk management and public and social services.[9]

The foundation of the blockchain technology is deemed to be the distributed ledger technology (DLT). The technology introduces a consensus validation mechanism by means of a whole network of computers designed to ease peer-to-peer transactions and cut an intermediary or a centralized authority out of the equation. The DLT also stores the information of all concluded transactions in the network. Each transaction, after being validated in the network, is added as a new block to a chain of transactions which is called the blockchain. Once a transaction is added to the chain it normally cannot be modified or deleted from the chain. There are two different types of blockchain networks, which are permissioned blockchains and public blockchains. Permissioned blockchains are proprietary networks, which means that specific individuals or entities use those blockchains to execute transactions. These entities could be, for example, a group of banks processing financial transactions. Public blockchains are open networks which can be used by anyone. This includes individuals who conduct transactions with each other by using bitcoin as a means of payment.[10]

The technology can be used in a decentralized manner, and this is enabled, *inter alia*, by integrating different technologies such as a digital signature which is based on asymmetric cryptography. The blockchain technology utilizes a peer-to-peer networking system and it does not need a centralized server, but instead the chain is located in an entire network of computers. By the use of a distributed database system, the requirement for a central authority is removed through a digital ledger of every transaction in a given network which can be approved by any computer on the network.[11] Even though Bitcoin is deemed to be the most popular blockchain application, the blockchain can be used in a wide range of different applications. Because the technology allows transactions to be conducted without any intermediaries such as banks, it can be used with a variety of financial services including digital assets, remittance and online payment. The technology is quickly becoming a key feature in the internet interaction systems of the next generation such as smart contracts.[12]

[9] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14 (4), 352-375.
[10] Rennock, Cohn, Butcher (2018), *supra nota* 7, 36.
[11] Woodside, J., Augustine, F., Giberson, W. (2017). Blockchain Technology Adaption Status and Strategies. *Journal of International Technology and Information Management*, 26 (2), 65-93.
[12] Zheng, Xie, Dai, Chen, Wang (2018), *supra nota* 9, 354.

In addition to the different financial instruments, the blockchain technology is also used, for example, for digital identity purposes and the enhancement of transparency in supply and commodity chains. A pioneer in the field of using the blockchain technology for digital identity purposes is the Government of India. They ran a large national digital identity scheme called the Unique Identification Authority of India. As a part of the scheme, each resident obtained a twelve-digit unique code. Another innovative actor in the field is a company called OneName, which offers a decentralized service to clients by ensuring that their digital identity remains free from the control of a central institution or company. The blockchain technology can also be used in order to facilitate transparency in global supply and commodity chains. Often the supply chain of different consumer goods is uncertain to the end consumer, and the blockchain technology could offer a solution to this. The blockchain would create a consensus-based ledger that tracks the origin and the developments of the goods during the period in the supply chain. A formal registry would be created to track the goods and the conditions in which they have been delivered to the end consumer. Finally, with the assistance of the anonymity of the blockchain technology discounts could be sent to consumers without the need for personal information.[13]

1.3. Monetary policy

In the current state of the economy, cryptocurrencies co-exist with official, government-issued currencies. Cryptocurrencies do not challenge the position of official currency due to their small volumes, but with the improvement of algorithms the popularity and use of cryptocurrencies could increase hastily. The increasing use and popularity of cryptocurrencies could eventually lead to a state in which cryptocurrencies and official currencies would be in competition with each other. However, taking into account the current natural monopoly enjoyed by government-issued currencies, it would take a massive lack of trust in established currency for cryptocurrency to completely replace it and gain the absolute trust of the public.[14]

Cryptocurrencies operate alongside official currencies, and therefore they have potential effects on, for example, the European Central Bank (ECB). The effects can be divided into two categories,

[13] Pilkington, M. (2015). Blockchain Technology: Principles and Applications. In: Olleros, F., Zhegu, M. (Eds.), *Research Handbook on Digital Transformations* (225-253). United Kingdom: Edward Elgar Publishing.
[14] Claeys, G., Demertzis, M., Efstathiou, K. (2018). Cryptocurrencies and Monetary Policy. *Bruegel Policy Contribution,* (10).

which are direct and indirect effects. In this context, the direct effects mean those that could have an impact on the price stability, monetary policy or the ability of the ECB in controlling the money supply. The control of the money supply is deemed to be an essential part of the ECB's task of maintaining price stability. The indirect effects include those that derive from the connection of the banking and payment systems of cryptocurrencies, which are both deemed to be in the ECB's scope of competence.[15] Cryptocurrencies also have the ability to challenge the governmental supervision of monetary policy by the avoidance and disturbance of traditional payment systems and escape from existing regulatory schemes. They especially present a way to hide transactions with a range of anonymity which, in the current time, is only deemed possible with certain cash transactions. Furthermore, cryptocurrencies are also of essential interest for those who have a desire of, for example, avoid taxes or practice money laundering.[16]

Although Bitcoin, for instance, is globally traded there is no existing global regulatory framework yet created for it. The attitude of different countries towards cryptocurrencies differs drastically. Ecuador, for example, has attempted to ban Bitcoin altogether while others such as Cyprus have encouraged citizens to use it. In the United States the exchange of virtual currency is regulated by the Financial Crimes Enforcement Network (FinCEN). Among other things, it insists that the identification of purchasers is collected by all bitcoin exchanges. Through a practical test on enforceability it was found that all bitcoin exchanges within the United States collected the information, but only a few outside the United States did and subsequently circumvented the FinCEN regulations.[17]

[15] Nabilou, H., Prüm, A. (2019). Central Banks and Regulation of Cryptocurrencies. *Review of Banking and Financial Law (Forthcoming), University of Luxemburg Law Working Paper,* No. 2019-014.
[16] Middlebrook, S.T., Hughes. S.J. (2014). Regulating Cryptocurrencies in the United States: Current Issues and Future Directions. *William Mitchell Law Review,* 40 (2), 813-848.
[17] Pieters, G.C. (2016). The Potential Impact of Decentralized Virtual Currency on Monetary Policy. Annual Report, Globalization and Monetary Policy Institute, Federal Reserve Bank of Dallas, p. 20-25.

2. VIRTUAL CURRENCY IN THE LIGHT OF MONEY LAUNDERING AND TAX EVASION SCHEMES

2.1. Money laundering

Money laundering refers to different actions subjected to criminally gained assets by which the illegal origin of the assets is attempted to be concealed or faded. When succeeding, money laundering makes the assets seem to be legally obtained.[18] According to the Finnish Criminal Code Chapter 32 Section 6:

"a person who (1) receives, uses, converts, conveys, transfers or transmits or possesses property acquired through an offence, the proceeds of crime or property replacing such property in order to obtain benefit for himself or herself or for another or to conceal or obliterate the illegal origin of such proceeds or property or in order to assist the offender in evading the legal consequences of the offence or (2) conceals or obliterates the true nature, origin, location or disposition of, or rights to, property acquired through an offence, the proceeds of an offence or property replacing such property or assists another in such concealment or obliteration, shall be sentenced for money laundering to a fine or to imprisonment for at most two years."[19]

According to the Criminal Code, the attempt of money laundering is also punishable.[20] The principal idea of money laundering is quite straightforward. A person who has obtained some type of illegal gains will attempt to ensure that the use of these funds would be possible, without other people realizing that the funds are a result of illicit activities. In order for this to be successful, the original source of the gains must be hidden. Subsequently, the funds and their source will appear to be legitimate. As it is usually cash that needs to be concealed, a criminal often seeks legitimate businesses in order to disguise the source of the cash. When dealing with money laundering, there are two general aspects to consider. Firstly, money laundering indicates to the use of legitimate

[18] Kimpimäki, M. (2015). *Kansainvälinen Rikosoikeus.* Helsinki, Finland: Kauppakamari.
[19] Rikoslaki (39/1889), Chapter 32 § 6
[20] *Ibid.*

businesses to ease the process of shuffling legal and illegal funds. Secondly, it also refers to the process of concealing the original source of the funds.[21]

Generally, three different stages can be identified in laundering schemes. The stages are the placement stage, the layering stage and the integration stage. During the placement stage the illegal proceeds are placed into a legitimate bank or financial system during which the risk of being revealed is relatively high.[22] Criminals conduct the placement stage by using different techniques, which contain, for instance, depositing cash into bank accounts and buying high value resources such as land and property with the illicit gains. Subsequently, complex financial transactions are made in order to attempt to conceal the ownership or the original source of the money. The general purpose of this action is to sever the illicit gains from the source of the criminal act by the means of financial transactions aiming to hide any trail, source or ownership of the money.[23] During the layering phase, the money launderer conducts a series of complex financial transactions through which the illegal money is distanced from the original source.[24] The phase can, for instance, contain multiple cross-border transactions between different bank accounts, sophisticated loan arrangements, and trading with assets.[25] The last phase, integration, is done by shaping the illegal gains into legitimate business earnings by financial or commercial transactions.[26] The main purpose of this stage is to re-infiltrate the funds into the legitimate financial system. The money launderer may do so by investing the funds into, for example, real estate or business endeavours.[27]

Through economic globalization, the traceability of money laundering schemes has become increasingly difficult. In the context of money laundering, globalization entails quick transfers of assets across national borders and diversity in the financial market. In order to tackle money laundering on a wide scale, coordinated international tools and responses are necessary. Because of the delocalized nature of financial transactions, the law follows and becomes delocalized through international processes founded in order to adopt international policies and legal

[21] Cox, D. (2014). *Handbook of Anti Money Laundering.* United Kingdom: John Wiley & Sons.
[22] Schneider, F., Windischbauer, U. (2010). Money Laundering: Some Facts. *Economics of Security Working Paper*, No. 25, Deutsches Institut für Wirtschaftsforschung (DIW), Berlin.
[23] Irwin, A. S., Choo, K. R., Liu, L. (2012). An Analysis of Money Laundering and Terrorism Financing Typologies. *Journal of Money Laundering Control,* 15 (1), 85-111.
[24] Ryder, N. (2008). The Financial Services Authority and Money Laundering: A Game of Cat and Mouse. *Cambridge Law Journal,* 67 (3), 635-653.
[25] Doyle, T. (2002). Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactics Needlessly Violate International Law. *Houston Journal of International Law,* 24 (2), 279-313.
[26] Levi, M., Reuter, P. (2006). Money Laundering. *Crime and Justice,* 34 (1), 289-375.
[27] Singh, K., Best, P. (2019). Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity. *International Journal of Accounting Information Systems,* 34.

instruments.[28] The complex issue of money laundering has been the mandate of many different international organizations and non-governmental actors. The activities which they engage in include the enhancement of cooperation between countries, assistance in the process of implementing legislation, and discovering the best methods for the prevention of money laundering. For example, the Financial Action Task Force on Money Laundering (FATF) has created a blacklist for countries who refuse to cooperate in the international fight against money laundering. The FATF, which was established in 1989 at the time of the G7 Summit in Paris, aims at examining strategies and techniques in the fight against money laundering and developing specific anti-money laundering (AML) measures. Furthermore, the FATF has issued 40 recommendations for an applicable universal legal base for the implementation of AML programs at the national level.[29]

2.2. Virtual currency and money laundering

During recent years, in order to avoid regulators, money launderers have restructured the process through the utilization of virtual currencies. Until the emergence of the new process, money launderers were compelled to use the central banking system in order to transfer and hide their illicit assets in the financial system. Since the central banks were involved, governments could control the laundering by imposing heavy regulations and fines on different banks and financial entities. Because of this, transferring and hiding illegal funds within the financial system became an increasingly difficult endeavour.[30] The shift in the money laundering process is very apparent, and launderers increasingly exploit virtual currencies when cashing out their criminal proceeds. Additionally, virtual currencies are also a popular means of payment between criminal individuals. According to Europol, Bitcoin is "accounting for over 40 per cent of all identified criminal-to-criminal payments"[31] in investigations relating to the field of cybercrime.[32]

---

[28] Arnone, M., Borlini, L. (2010). International Anti-Money Laundering Programs: Empirical Assessment and Issues in Criminal Regulation. *Journal of Money Laundering Control,* 13 (3), 226-271.
[29] Lucian, R. (2010). The Concept of Money Laundering in Global Economy. *International Journal of Trade, Economics and Finance,* 1 (4), 354-360.
[30] Albrecht, C., McKay Duffin, K., Hawkins, S., Morales Rocha, V. M. (2019). The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control,* 22 (2), 210-216.
[31] Europol. (2015). *The Internet Organized Crime Threat Assessment.* Retrieved from: www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf , 12 April 2021.
[32] van Wegberg, R., Oerlemans, J., van Deventer, O. (2018). Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin. *Journal of Financial Crime,* 25 (2), 419-435.

Virtual currencies can be used as a means of payment, but also as an asset to which other means of payment may be converted digitally in a cross-border manner. While transferring large sums of cash-based money can be a difficult task, virtual currencies can be transferred fast and secretly from one user to another. The establishment of digital companies is very rapid, and they can be used to move assets beyond state lines. Additionally, the movement and laundering of virtual currencies can be carried out instantly as it does not require similar Know Your Customer (KYC) identity verification and compliance or formal financial institutions as trading with securities.[33] Virtual currencies possess features which provide a certain level of motivation to criminals, and therefore the system is used. One feature which can benefit criminals is that virtual currencies are becoming a widely accepted and popular means of payment in the world of retail. At this time the range of acceptance is limited due to the fact that virtual currencies frequently need to be exchanged for fiat currencies, which means a government-issued currency such as the US dollar. Another desirable feature is that an internet connection is all that is required in order to move and transfer funds across borders.[34]

In their original sense, virtual currencies were created in order to eliminate the banking system as an intermediary in peer-to-peer transactions and subsequently transaction fees could be saved. However, since most people buy virtual currencies in exchange for fiat currencies, intermediaries do have a certain role in the process. Because of their decentralized nature and transactions going between virtual currencies and fiat currencies, financial institutions must be careful and diligent when performing AML checks. Crypto cleansing is a process which can be used to avoid international sanctions, and it usually involves money laundering conducted in a digital form. Generally, the process follows five different stages. Firstly, cryptocurrency is purchased at a digital exchange or digital currency ATM. Usually the first option is preferred since most cryptocurrency ATM providers are often entities with AML duties. Criminals usually take advantage of strawmen when acquiring cryptocurrencies at a digital exchange. Strawmen are people with clean criminal records and employment records. Perpetrators also further ensure their anonymity by adopting, for instance, pseudonyms and anonymous e-wallets. Secondly, as soon as the strawmen have been verified regarding the exchange, fiat currency is used to convert funds and purchase primary coins which include, for example, Bitcoin and Ethereum. After this, the primary coins are used to purchase alt-coins which often offer an advanced level of anonymity. Thirdly, by using tactics

[33] Desmond, D., Lacey, D., Salmon, P. M. (2019). Evaluating Cryptocurrency Laundering as a Complex Socio-Technical System: A Systematic Literature Review. *Journal of Money Laundering Control,* 22 (3), 480-497.
[34] Albrecht, McKay Duffin, Hawkins, Morales Rocha. (2019), *supra nota* 30, 213.

called mixing and tumbling, money launderers attempt to hide the audit trail of the primary coins. It involves using programs such as Bitmixer in order to change coin addresses to random digital wallet addresses to confuse the blockchain and further complicate traceability. Fourthly, privacy coins, exchanges and digital addresses are layered by the money launderers in order to cut the audit trail. This is done to prepare the illicit funds for being re-integrated to the traditional financial system. Finally, after the audit trail has been cut, money launderers have different options for obtaining the cleansed funds from the digital currency and further converting it back to fiat currency. One option is called burst-out integration. According to this method, "privacy coin holdings are exchanged for primary coins and later to a basic currency which can be withdrawn to a connected bank account or transferred to real estate, by citing the legal desire to avoid capital gain taxes."[35]

Haffke, Fromberger and Zimmermann offer a clear and straightforward example of money laundering by using virtual currencies:

"Person P is in possession of cash originating from illicit activities. In a country with low AML standards, he deposits the cash with a bank. He seeks to purchase 10 Monero tokens (XMR) which provide a high level of anonymity. These tokens are only available on crypto markets. Therefore, at first, P has to open up a user account at a cryptocurrency exchange. This exchange provides him with a wallet (pair of public and private key). P transfers a certain amount of fiat money from his bank account to the cryptocurrency exchange. Here, P can exchange the fiat currency into Bitcoins. P now opens up a user account at a crypto market that provides him with another pair of keys. Subsequently, he transfers the Bitcoins from the cryptocurrency exchange to the crypto market. There, he exchanges Bitcoins into Monero tokens. P could exchange the Monero tokens back into 'white money' himself by following the same steps in reverse order. As the tokens can be transferred cross borders between different wallets, P could do so in any other country. Alternatively, he can transfer the tokens to other persons that then conduct the exchange. Additionally, a tumbler service can be used. This way, P has laundered his illicitly earned money."[36]

[35] Sprenger, P., Balsiger, F. Anti-Money Laundering in Times of Cryptocurrencies. KPMG Compliance Matters, June 2018.
[36] Haffke, L., Fromberger, M., Zimmermann, P. (2020). Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them. *Journal of Banking Regulation,* 21 (2), 125-138.

2.3. Tax evasion

Because of its anonymous nature, cryptocurrencies are potential tools which can be beneficial for tax evaders. Additionally, when considering that cryptocurrency transactions do not involve any financial intermediaries such as banks, the tax evasion policies adopted by governments worldwide might potentially be proven ineffective. Since cryptocurrency is considered beneficial for tax evasion and money laundering purposes, there have been a variety of methods and attempts in order to hide the source of the assets or the destination of transactions. One of these methods involves people having multiple wallets that are used only to receive money. No money is sent out from these wallets, and having these so-called passive wallets decrease the possibility of getting identified by tax enforcement agencies such as the Internal Revenue Service (IRS) in the United States.[37] Although the Bitcoin market was of small volume in 2013, many commentators expected that the markets of Bitcoin and other cryptocurrencies will grow in the future and they did become more popular. The earnings which people have in their passive wallets are generally beyond the reach of tax authorities unless the earnings are voluntarily reported. Additionally, research has shown that Bitcoin users use patterns called "fork and merge" patterns. According to this pattern, large sums of Bitcoins are transferred into many small accounts, which are usually owned by the same user. This tactic is used by tax evaders and money launderers when attempting to hide the sources and destination of assets. Some taxpayers have even acknowledged that they have considered avoiding taxes and reporting requirements by using Bitcoin.[38]

When depositing assets in a cryptocurrency account, taxpayers can perform a vast number of transactions and in the event that the cryptocurrency balances are not converted back into fiat currency the gains from the transactions go unreported and undetectable. For example, in the United States, taxpayers could take advantage of this approach in order to evade taxes. However, this requires at the very least transferring U.S. dollars to the blockchain technology which could alert some authorities. The solution to the problem of international tax avoidance presented in the Foreign Account Tax Compliance Act[39] (FATCA) of the United States suggests imposing reporting obligations on foreign financial entities who hold U.S. accounts. However, this approach is unfeasible in relation to tax avoidance schemes based on the blockchain technology because they

[37] Jafari, S., Vo-Huu, T., Jabiyev, B., Mera, A. Mirzazade, R. (2018). *Cryptocurrency: A Challenge to Legal System*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172489 , 12 April 2021.
[38] Marian, O. (2013). Are Cryptocurrencies "Super" Tax Havens? *Michigan Law Review First Impressions*, 112 (38), 38-48.
[39] Foreign Account Tax Compliance Act of 2009, H.R.3933

do not rely on any financial intermediaries and therefore it is out of the regulatory reach of foreign governments. FATCA recommends foreign financial institutions to disclose information relating to U.S. taxpayers in order to avoid the failure to comply with compliance requirements. When speaking about the cryptocurrency network, this is not such an easy task.[40]

The use of Bitcoin moves cash transactions from face-to-face or mail contracts to the world of the Internet, which is highly decentralized and borderless. Of course, this includes legal purchases which we do on a daily basis with fiat currency, but it also involves criminal activities such as tax evasion and money laundering. The scope of tax evasion and other illegal activities in relation to Bitcoin transactions may even exceed that of traditional transactions by cash, but even if the transactions which are likely to result in non-disclosing are usually related to Bitcoin, the deeper problem does not concern this technology. In the context of the Internet, many vendors do not carry out their reporting duties to the IRS even though the transactions are carried out via online payment system such as PayPal, or even by credit card. This shows us that the problem of tax evasion is a serious one in our system which relies on the fact that people practice self-reporting.[41]

The first-ever Court of Justice of the European Union (ECJ) Bitcoin-related case concerned the taxation of exchanges between fiat currency and Bitcoin. In *Skatteverket v David Hedqvist C-264/14* the ECJ held that the services of a Bitcoin exchange in exchanging Bitcoin for fiat currency is exempt from value added tax (VAT) on the basis of an exception in Directive 2006/112/EC (VAT Directive).[42] Prior to this ruling there was no clarity on how Bitcoin should be taxed. In some states Bitcoin was subject to VAT, and in other states not. The ruling provided a guideline on the taxation of Bitcoin, and it required Member States to exempt Bitcoin supplies from VAT.

The case itself was about Mr. Hedqvist, a Swedish national who was hoping to establish a Bitcoin exchange. Before engaging in such activities, he wished to receive some clarity on the fact whether his business would be subject to VAT. In Sweden the case went all the way to the the Supreme Administrative Court of Sweden, which referred the case to the ECJ. The case confirmed that the exchange of Bitcoin for a fiat currency is considered a supply of services in the context of EU law. The Court held that an exchange of Bitcoin for a fiat currency fell within

[40] Viswanathan, M. (2018). Tax Compliance in a Decentralizing Economy. *Georgia State University Law Review,* 34 (2), 283-333.
[41] Slattery, T. (2014). Taking a Bit out of Crime: Bitcoin and Cross-Border Tax Evasion. *Brooklyn Journal of International Law,* 39 (2), 829-873.
[42] VAT Directive 2006/112/EC

the exception in Article 135 (1) (e) of the VAT Directive. The Article states that the Member States shall exempt "transactions, including negotiation, concerning currency, bank notes and coins used as legal tender, with the exception of collectors' items, that is to say, gold, silver or other metal coins or bank notes which are not normally used as legal tender or coins of numismatic interest"[43] from VAT.[44]

[43] *Ibid.,* Art. 135 (1) (e)
[44] Court decision, 22.10.2015, Skatteverket v David Hedqvist, C-264/14, EU:C:2015:718

3. THE EUROPEAN UNION AND U.S. APPROACH

3.1 Past measures and calls for regulation

Over the past few years, a key question related to cryptocurrencies has been the regulatory framework which could be applied to them, and more importantly the position of service providers operating within the field. Although some original developers of Bitcoin had libertarian views to the matter and did not want any interference by any central authorities, many service providers in the field are trying to understand the regulatory framework better and advocate for their solutions to the matter. Among other things, many service providers have hired Chief Compliance Officers (CCO) and aimed for creating more secure services in order to maintain consumer confidence and risk management which are key factors of commercial success.[45]

The first EU AML Directive was adopted in the year of 1991. An AML framework was deemed necessary at the EU level in order to secure the financial system within the EU and coordinate different AML measures in a more efficient way within the Union. Altogether the EU has adopted six different AML Directives, amending previous ones in the process. The concern for virtual currencies began to rise after the adoption of Directive (EU) 2015/849, which is also known as the fourth Anti-Money Laundering Directive (AMLD4).[46] AMLD4 was adopted in order to affirm already adopted rules and to boost the efficiency of the fight against money laundering and terrorist financing. After AMLD4 was adopted there was some debate about whether virtual currencies can be included in the scope of the Directive. Despite the scholarly debate, it was reasonable to argue that it was very difficult or even impossible to apply the Directive to virtual currencies. The fact in the Directive which facilitated the inclusion of virtual currencies to the scope was the definitions of property and funds. Property and funds are defined in Article 3 (3) of AMLD4 as "assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets."[47] Although virtual currencies are not mentioned separately, the definition would seem suitable in order to include virtual currencies in the scope of the Directive as they could be considered as incorporeal immovable assets. However, the list of obliged entities creates

[45] Raymaekers, W. (2014). Cryptocurrency Bitcoin: Disruption, challenges and opportunities. *Journal of Payments Strategy & Systems,* 9 (1), 30-40.
[46] Anti-Money Laundering Directive (EU) 2015/849
[47] *Ibid.*, Art. 3 (3)

an issue. None of the entities involved in virtual currency schemes are directly or indirectly involved with the list of obliged entities, not even crypto exchanges. Because of this, the framework of AMLD4 could not be broadened to the virtual currency scheme and it was therefore fully exempt from the scope of the Directive.[48]

Before the adoption of Directive (EU) 2018/843, which is also known as the 5th Anti-Money Laundering Directive (AMLD5)[49], some Member States had already taken steps regarding the question whether the virtual currency market is subject to AML rules and obligations. One of them was Italy, including a reference to virtual currencies to the already existing AML legislation. This leaves the question whether the EU should have regulated the virtual currency markets before the Member States took actions on their own. One option would have been to extend the scope of the second Payment Service Directive (PSD2).[50] By doing so, the EU legislators would have been able to possibly increase consumer protection within a harmonized legal setting, and automatically extend the scope of obliged entities which are subject to AML obligations. Although this option was proposed to lawmakers in the Union, The Commission refused to take this path, emphasizing that a regulatory measure would offer virtual currencies more legitimacy than they deserve.[51]

3.2 The 5th Anti-Money Laundering Directive

The 5th Anti-Money Laundering Directive was published on 19 June in the year 2018, and it amended the 4th Anti-Money Laundering Directive which was adopted on 20 May 2015. Among other things, the AMLD5 extended the reach of the Directive to include virtual currency platforms and custodian wallet providers and services related to taxation into the scope of obliged entities under the Directive. It also brought an end to the anonymity involved with bank and savings accounts and safe deposit boxes. Furthermore, it contains rules on making ultimate beneficial

[48] Houben, R., Snyers, A. (2018). *European Parliament Policy Department for Economic, Scientific and Quality of Life Policies. Cryptocurrencies and Blockchain Study: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. Retrieved from https://blog.elitex.ir/wp-content/uploads/2020/06/Cryptocurrencies-and-Blockchain.pdf, 8 April 2021.
[49] Anti-Money Laundering Directive (EU) 2018/843
[50] Payment Service Directive (EU) 2015/2366
[51] Covolo, V. (2019). The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5th Anti-Money Laundering Directive. *University of Luxembourg Law Working Paper Series,* No. 2019-015.

ownership (UBO) information of companies in the area of the EU accessible by the general public.[52]

The fact that virtual currency platforms and wallet providers were included to the list of obliged entities of the AMLD5 means that the entities must comply with customer due diligence requirements and measures that have been implemented in order to prevent the misuse of the financial system for the purposes of different criminal activities.[53] According to the recital 8 of the preamble to the AMLD5:

"Providers engaged in exchange services between virtual currencies and fiat currencies (that is to say coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country) as well as custodian wallet providers are under no Union obligation to identify suspicious activity. Therefore, terrorist groups may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. It is therefore essential to extend the scope of Directive (EU) 2015/849 so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers. For the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT), competent authorities should be able, through obliged entities, to monitor the use of virtual currencies. Such monitoring would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship."[54]

Therefore, before the AMLD5 there were no obligations set by the Union for service providers within the virtual currency market, and through that a satisfactory level of supervision and monitoring of suspicious activity by the authorities in the Union was not possible.

The AMLD5 also clarified the status of virtual currencies when compared to other types of currencies. Article 1 (2) (d) point 18 of the Directive states that "virtual currencies means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is

[52] Koster, H. (2020). Towards Better Implementation of the European Union´s Anti-Money Laundering and Countering the Financing of Terrorism Framework. *Journal of Money Laundering Control,* 23 (2), 379-386.
[53] De Vido, S. (2019). All that Glitters is Not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive. *DPCE Online,* 1, 59-76.
[54] Anti-Money Laundering Directive (EU) 2018/843, Recital no. 8

not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."[55] Based on this definition in the Directive, virtual currencies do not possess the legal status of an authentic currency, but it is still considered as one since it can be used as a means of payment or exchange, and therefore it was essential to include it in the framework of the Directive. As can be deduced from the definition above, the Directive excludes digital representations of value issued by public authorities, and representations of value which hold the legal status of currency.[56] Virtual currencies, within the meaning of the Directive, are meant to include currencies despite of whether they are attached to a legally established currency.[57] The Directive also officially defines custodian wallet providers as entities which provide services to "safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies."[58]

As a result of the AMLD5, platforms engaging in virtual currency exchanges and custodian wallet providers must comply with obligations that arise from the FATF recommendations, assess the identities of customers, avoid accounts which are anonymous and maintain records of information regarding the customers. Even if an account is anonymous, upon request by the authorities the service providers have to disclose the IP address which is necessary for the identification of the wallet owner. However, it is not always a given that the service providers are willing to cooperate, and the measure is a *post facto* measure rather than a preventive measure. Therefore, it does not follow the established trend in anti-money laundering and terrorist financing regulation, which mainly has a preventive effect.[59]

The AMLD5 also replaced Article 47 (1) of the AMLD4 with the following: "Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated."[60] This Article speaks to the fact that EU legislators wish to have a deeper

[55] *Ibid.*, Art. 1 (2) (d) point 18
[56] *Ibid.*, Recital no. 10
[57] Haffke, Fromberger, Zimmermann (2020), *supra nota* 36, 10.
[58] Anti-Money Laundering Directive (EU) 2018/843, Art. 1 (2) (d) point 19
[59] De Vido (2020), *supra nota* 53, 72.
[60] Anti-Money Laundering Directive (EU) 2018/843, Art. 1 paragraph 29

insight on the operations of the service providers and to ensure a higher level of transparency regarding virtual currency schemes.

3.3 Virtual currencies in the United States

According to Section 2 (1) of the Securities Act of 1933, a security means, among other things, "any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract…"[61] The term in the definition which has been subject to the most broad form of interpretation is "investment contract". In the past a vast range of contracts have been perceived as falling under this definition, including leasing agreements for payphones with fixed rates of return. The question of whether virtual currency Initial Coin Offerings (ICOs) are deemed as securities is strongly dependant on whether they fall under the definition of investment contracts.[62] According to Section 6 of the Act, securities must be registered with the Securities and Exchange Commission (SEC).[63]

But can virtual currencies be perceived as securities under United States legislation? In order to determine the legal position of virtual currencies, the SEC turned their attention to the Decentralized Autonomous Organization (DAO) and The Howey test. The DAO was a virtual corporation which was run by algorithms instead of actual human beings, and it was perceived to be a virtual corporation and a vehicle for investments. Among other things, the DAO raised 150 million USD with an ICO and after the sale of the tokens, it was ready to fund projects for investment. The SEC investigated the DAO and addressed the important question of whether the sold tokens in the case should be categorized as securities. In its report, the SEC applied the Howey test which determines the existence of an investment contract. In the test, four criteria should be met: there has to be 1) an investment of money; 2) in a common enterprise; 3) with the expectation of profits; 4) solely from the efforts of others. When the SEC applied the test to the DAO, they discovered that 1) the DAO tokens were involved with the investment of money; 2) the DAO can be perceived as a common enterprise; 3) people who held DAO tokens had reasonable expectations

[61] Securities Act of 1933, Section 2 (1)
[62] Preston, J. (2017). Initial Coin Offerings: Innovation, Democratization and the SEC. *Duke Law & Technology Review*, 16 (1), 318-332.
[63] Securities Act of 1933, Section 6

of profits; and 4) the profits arising would in fact be derived from the efforts of others. After applying the test, the SEC concluded that the DAO tokens were securities which were subject to the registration duties under Section 6 of the Act.[64]

In December 2020, the SEC filed a complaint against Ripple Labs Inc., Bradley Garlinghouse and Christian Larsen. According to the complaint, from at least 2013 the defendants in the case sold 14.6 billion units of a virtual security called XRP, and in return they received a consideration of over 1.38 billion USD in cash in order to fund the operations of Ripple Inc. and enrich the other two defendants. The activity was conducted without registering the offers and sales of XRP with the SEC, which is required by the federal securities laws. The requirement was not subject to any exemptions in the light of the case. Since Ripple Inc. never filed a registration statement, it did not provide investors with material information that hundreds of other issuers for when soliciting public investments. Even though Ripple Inc. received legal counsel in 2012 regarding the fact that under some circumstances XRP could be perceived as an "investment contract", Ripple Inc. decided to engage in an illegal securities offering. Larsen and Garlinghouse personally profited from the unregistered sales by a value of approximately 600 million USD. The SEC seeks injunctive relief, disgorgement with prejudgment interest and civil penalties.[65] The case is ongoing at this moment, and a final ruling is still to be reached.

At the state level, many different states have begun to regulate cryptocurrency platforms, and some of them have even addressed matters such as the safeguarding of customer assets. Despite this, there is a deep concern that regulations on a state level are not sufficient since they lack uniformity and are usually easy to bend. For example, the state of New York established a cryptocurrency platform regulation in 2015, which is known as BitLicense. The BitLicense includes not only AML and cybersecurity provisions, but also provisions regarding the safeguarding of customer assets.[66] According to the New York Codes, Rules and Regulations Title 23 Section 200.9 (b), "a Licensee shall hold virtual currency of the same type and amount as that which is owed or obligated"[67] to customers of the cryptocurrency platform. Section 200.9 (c) states that "each Licensee is prohibited from selling, transferring, assigning, lending, hypothecating, pledging, or otherwise

[64] Mendelson, M. (2019). From Initial Coin Offerings to Security Tokens: A U.S. Federal Securities Law Analysis. *Stanford Technology Law Review,* 22 (1), 52-94.
[65] Complaint, United States District Court Southern District of New York, 20 Civ. 10832, *Securities and Exchange Commission v. Ripple Labs Inc., Bradley Garlinghouse, and Christian Larsen.*
[66] Chu, D. (2018). Broker-Dealers for Virtual Currency: Regulating Cryptocurrency Wallets and Exchanges. *Columbia Law Review,* 118 (8), 2323-2359.
[67] New York Codes, Rules and Regulations Title 23 § 200.9 (b)

using or encumbering assets, including Virtual Currency, stored, held, or maintained by, or under the custody or control of, such Licensee on behalf of another Person except for the sale, transfer, or assignment of such assets at the direction of such other Person."[68] By imposing these kinds of obligations to cryptocurrency platforms, the BitLicense regulation of the state of New York addresses the safety of customer assets and contributes to consumer well-being. The state of Hawaii has selected a different approach. According to Section 489D-8 of the Hawaii Money Transmitters Act, "a licensee, at all times, shall possess permissible investments having an aggregate market value, calculated in accordance with generally accepted accounting principles, of not less than the aggregate amount of all outstanding payment instruments issued or sold by the licensee in the United States."[69] Therefore, if a platform holds 100 Bitcoin on behalf of customers, it should hold the dollar equivalent of 100 Bitcoin in cash as reserve. If a cryptocurrency platform is looking to operate both in New York and Hawaii, they should be able to comply with both set of requirements.[70] As shown above, there are significant regulatory differences between states in the United States. This introduces the possibility of regulatory inconsistency and complicates the possibilities of virtual currency entities to operate across state lines. Harmonizing the regulation would be a big step towards a clearer and more uniform system.

[68] New York Codes, Rules and Regulations Title 23 § 200.9 (c)
[69] Hawaii Money Transmitters Act § 489D-8 (a)
[70] Chu (2018), *supra nota* 66, 2343.

4. PROPOSED AMENDMENTS TO THE 5th ANTI-MONEY LAUNDERING DIRECTIVE AND FUTURE LEGISLATION

4.1 Amendments proposed to the 5th Anti-Money Laundering Directive

The AMLD5 has provided a certain level of clarity and guidance of the world of virtual currencies. However, there are legislative gaps which can be found in the Directive, and this is mostly due to the fact that the nature of virtual currencies is constantly evolving. The first problem with the Directive is the definition of virtual currencies which was given above. The definition of virtual currencies was meant to include all potential types of tokens. The definition opens up many different interpretations: for example, if we interpret virtual currencies as means of exchange from an economic perspective, they describe the function of money and therefore do not fall within the tradeable character of goods. Instead, virtual currencies define intermediary objects which assist the trade of services and products between people. Within the meaning of the Directive, the only category which falls within the scope of the definition of virtual currencies is currency tokens. The interpretation is problematic because it excludes utility and investment tokens since they cannot be used as intermediary assets.[71] Utility and investment tokens are used primarily for fund raising purposes. Utility tokens are issued to fund the development of new virtual currencies and they can be used later to purchase goods or services from the issuer of the new currency. Investment tokens can be bought in connection with ICOs, which is the virtual currency equivalent to Initial Public Offerings (IPO).[72]

Legal scholars have suggested several amendments to the wording of the AMLD5. The definition of virtual currencies has been a special issue and, for example, Haffke, Fromberger and Zimmermann have shared their vision of a correct definition. They have proposed that the definition of virtual currencies should be the following:

"a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons **as a means of payment**

[71] Cancelli, L. (2020). The Growing Crypto-Assets Threat to Anti-Money Laundering: How Institutions Are Coping with This Phenomenon. *EUDIFIN Research Working Paper,* No. 12.
[72] di Angelo, M., Salzer, G. (2020). *Tokens, Types, and Standards: Identification and Utilization in Ethereum.* Conference Paper, 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Online Event.

or a means of exchange or which is used for purposes such as investment or redemption of goods or services, and which can be transferred, stored and traded electronically."[73]

By amending the definition of virtual currencies, they would also include investment and utility tokens to their scope in the light of the AMLD5. The wording "such as" which is included in the proposed amendment would allow to extend the scope of virtual currencies significantly, and cover tokens which do not necessarily fall within the categories mentioned in the proposal. By adopting the proposed amendment, the objective of the AMLD5 which was to include all potential types of tokens to the scope and treat them equally, would be fulfilled.[74]

Another issue identified with the AMLD5 is the list of obliged entities in the context of cryptocurrency exchanges. Most of the cryptocurrency exchanges operate in a way that they allow their users to purchase cryptocurrency with fiat currency, or alternatively sell cryptocurrency in exchange for fiat currency. Under the AMLD5, cryptocurrency exchanges of this nature are included on the list of obliged entities. But what about cryptocurrency exchanges which only accept payments in other cryptocurrencies? Because these types of exchanges do not have any association with fiat currencies, they cannot be deemed as custodian wallet providers under the AMLD5 and therefore they are excluded from the scope of obliged entities. This is an issue which should be addressed in a serious manner because it undermines the fight against money laundering and terrorist financing, and offers criminals a way to further conceal the origin of their funds and potentially facilitates the use of cryptocurrencies in a way which is completely outside the scope of the monitoring practiced by law enforcement authorities.[75] Therefore, amending the list of obliged entities to include cryptocurrency exchanges which do not involve the use of fiat currency would be a major step towards better law enforcement in the European Union and preventing money laundering schemes with cryptocurrencies. The definitions provided in the AMLD5 are in the need for some additional clarity as discovered above regarding the definition of virtual currencies. Ambiguous and inconsistent definitions such as that open the path for issues relating to the interpretation of the provisions, and through that reduce the clarity of the AMLD5.

Furthermore, it would be appropriate to add the tumbler services referred to in Chapter 2.2 to the list of obliged entities under the AMLD5. The KYC goals of the AMLD5 include that the obliged

[73] Haffke, Fromberger, Zimmermann (2020), *supra nota* 36, 14.
[74] *Ibid.*
[75] Houben, Snyers (2018), *supra nota* 48, 77.

entities report and control suspicious activities and transactions. As tumbler services are occasionally used in the context of money laundering schemes, their inclusion to the list is very important. Legal scholars have proposed to amend the scope of the AMLD5, namely Article 1 (1), to the following: "Providers engaged in exchange services between virtual currencies and fiat currencies or between virtual currencies; this includes providers of services that exchange one virtual currency into the same virtual currency, irrespective of whether the service is used by a single user or for a transaction between multiple users."[76]

4.2 The future of virtual currency regulation

As we discovered in the previous subchapter, the regulation of virtual currencies within the European Union has provided a certain level of clarity to the quickly evolving field of virtual currencies and the service providers associated with the field. However, the legislative gaps discovered in the AMLD5 reveal the fact that there is still a lot to be done in order to regulate virtual currencies in a convincing manner. In this section I will present two legislative initiatives by the European Union, which aim to further regulate the field of virtual currencies, namely the Markets in Crypto-Assets Regulation (MiCa) and the 6th Anti-Money Laundering Directive.

4.2.1 Markets in Crypto-Assets Regulation

The proposal for MiCa was first published in September 2020 and it has four main objectives. The first objective is to provide an additional level of legal clarity and certainty to ensure a safe and secure development of crypto-assets and the utilization of DLT (see Chapter 1.2) in various financial services. The initiative should also support innovation and ensure an atmosphere of fair competition by establishing a framework for the issuing and providing services in the crypto-assets market. Thirdly, it is designed to ensure a significant level of consumer and investor safety and protection as well as market integrity. The last general objective of MiCa is to address problems in financial stability and monetary policy, and the risks which could arise from the quickly increasing utilization of crypto-assets and DLT mechanisms. Moreover, the regulation seeks to remove regulatory obstacles relating to the issuing and trading of crypto-assets, increase the sources of funding or companies through ICOs, limit the risks of fraud and illegal activities in the

[76] Haffke, Fromberger, Zimmermann (2020), *supra nota* 36, 18.

market for crypto-assets, and allow consumers and investors to take advantage of new investment opportunities and payment instruments.[77]

The proposal is expected to provide a harmonized framework for the regulation of crypto-assets which is currently not covered by existing financial services regulation. It should further develop consumer protection by regulating the main operations of the crypto-assets market, for example wallet provision, and exchange and trading platforms. The European Union expects that imposing a regulatory framework for the crypto-asset market will reduce the amount of theft and fraud in the field. It will also address issues relating to market fragmentation, which arises highly from the different national approaches which the Member States have adopted in the European Union. The proposal also includes monitoring and reporting rules according to which the European Commission, in cooperation with the European Securities and Markets Authority (ESMA), will produce reports regarding the impacts of the MiCa-initiative.[78]

4.2.2 The 6th Anti-Money Laundering Directive

The 6th Anti-Money Laundering Directive (AMLD6)[79] was adopted on 23 October 2018 and it introduces a variety of new provisions related to virtual currencies, the most important provision being the liability of legal persons regarding money laundering offences. According to Article 7 of the AMLD6, legal persons shall be held liable for money laundering offences "committed for their benefit by any person, acting either individually or as part of an organ of the legal person and having a leading position within the legal person…"[80] Furthermore, Article 4 stipulates that also aiding and abetting, inciting and attempting a money laundering offence is punishable as a criminal offence.[81] Before the new provisions, only the individuals that actually monetarily benefitted from the money laundering scheme would be convicted. However, under the new provisions, any legal person that aids in a money laundering scheme will be liable despite the fact whether it receives material benefit or not.[82] In practice, the extension of liability for money laundering offences to

[77] 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)*, Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF , 8 May 2021.
[78] *Ibid.*, 146-151.
[79] Anti-Money Laundering Directive (EU) 2018/1673
[80] *Ibid.*, art. 7.
[81] *Ibid.*, art. 4.
[82] Coinfirm. (2020). *6th Anti-Money Laundering Directive: EU´s 6AMLD,* Retrieved from https://www.coinfirm.com/blog/6amld-6th-anti-money-laundering-directive/ , 8 May 2021.

legal persons indicates that obliged entities are required to have extensive controls in place in order to ensure compliance with money laundering regulations. The extension of liability also aims to impact money laundering policies and compliance of cryptocurrency wallet providers and exchanges directly from the management level of the companies.[83]

The Directive further revises the sanctions imposed for legal persons regarding money laundering offences. According to Article 8 of the AMLD6, a legal person is punishable by sanctions including criminal and non-criminal fines but also with sanctions such as "exclusion from entitlement to public benefits and aid; temporary or permanent disqualification from the practice of commercial activities; and temporary or permanent closure of establishments which have been used for committing the offence."[84] Therefore, the AMLD6 lays down strict penalties for service providers engaging in money laundering activities and they may even have to close their establishments altogether if found guilty. Financial institutions are expected to be compliant with the AMLD6 in June 2021.[85]

[83] Comply Advantage. (2020). *Crypto-Assets, Wallets, Exchanges and 6AMLD,* Retrieved from https://complyadvantage.com/knowledgebase/crypto-assets-wallets-exchanges-6amld/ , 8 May 2021.
[84] Anti-Money Laundering Directive (EU) 2018/1673, art. 8 (a), (c), (f)
[85] Coinfirm (2020), *supra nota* 82

CONCLUSION

The aim of the present paper was to briefly provide an overview of the technology associated with virtual currencies and to analyse the AMLD5 introduced by the European Union in June 2018. The thesis further provided a review of the AML obligations imposed by AMLD5 on virtual currency service providers, analysed the effectiveness of the Directive and presented amendments which have been suggested by legal scholars within the field of virtual currency regulation. Current legislative initiatives were also presented.

The AMLD5 was the first step of regulating virtual currencies and service providers in the European Union. The Directive officially defined virtual currencies and custodian wallet providers, but it also provided advancements in the field of AML obligations which include, *inter alia*, assessing the identities of customers and avoiding anonymous accounts. However, the thesis has shown that the AMLD5 includes severe regulatory gaps especially because of the inadequate and already outdated definitions laid down in the Directive.

The definition of virtual currencies in AMLD5 was meant to cover all types of virtual tokens, but because of the wording of the definition of virtual currencies utility and investment tokens are excluded from the scope of the Directive because they cannot be used as intermediary assets. The aim of the Directive was to treat all tokens equally, but because of this exclusion the aim cannot be adequately reached. Another substantial issue of the AMLD5 was the list of obliged entities since the Directive excludes cryptocurrency exchanges which only accept payments in other cryptocurrencies from the scope of the Directive. These kinds of exchanges do not have any association with fiat currency and therefore they cannot be perceived as custodian wallet providers within the meaning of AMLD5. This fact can constitute a major problem since it allows the use of cryptocurrencies in a way which is totally outside the reach of law enforcement authorities. The research results provided in the thesis can therefore be deemed as being aligned with the hypothesis.

In assessing the effects and adequacy of the AMLD5, the problems which arose were found on the very initial level of the Directive, namely in the definitions. The definitions of a legislative document provide the foundation for the entire legal act, and therefore it is of vital importance that all possible aspects are considered when laying down the definitions. The vague definitions of the Directive hindered the aim of the AMLD5, therefore leaving significant regulatory gaps which were intended to be filled.

It is strongly suggested that the definition of virtual currencies is amended in a way which allows the inclusion of utility and investment tokens into the scope of the Directive. Amending the definition in the proposed manner would also include tokens which do not necessarily fall within the categories of the proposal. By doing so, the definitions of the Directive would correspond to the aim of the AMLD5 in a more convincing manner. It is also suggested that the European Union turns their attention more closely to the list of obliged entities under the AMLD5. By also including exchanges which do not have associations with fiat currency the AMLD5 could make extensive contributions to preventing certain intermediaries to entirely circle AML and KYC obligations altogether.

Furthermore, it is suggested that services which could be used to aid in money laundering schemes, such as tumbler services, would be included in the list of obliged entities under the AMLD5. Tumbler services can be used in money laundering schemes to further hide the audit trail of the virtual currency, and therefore their inclusion to the list is appropriate from the regulatory perspective.

The proposals presented are very applicable in the sense that the amendment of the definitions and the list of obliged entities in the Directive can be accomplished in a straightforward manner, and the difference which can be made with the amendments has the potential of being essential. However, presenting such amendments can create a resistance from the part of the service providers. Despite this, the amendments would serve for the good of the public and reduce the likelihood of criminal activity within the field of virtual currencies.

LIST OF REFERENCES

Scientific books

1. Cox, D. (2014). *Handbook of Anti Money Laundering.* United Kingdom: John Wiley & Sons

2. Kimpimäki, M. (2015). *Kansainvälinen Rikosoikeus.* Helsinki, Finland: Kauppakamari.

3. Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In: Olleros, F., Zhegu, M. (Eds.), *Research Handbook on Digital Transformations* (225-253). United Kingdom: Edward Elgar Publishing.

Scientific articles

4. Albrecht, C., McKay Duffin, K., Hawkins, S., Morales Rocha, V. M. (2019). The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control,* 22 (2), 210-216.

5. Arnone, M., Borlini, L. (2010). International Anti-Money Laundering Programs: Empirical Assessment and Issues in Criminal Regulation. *Journal of Money Laundering Control,* 13 (3), 226-271.

6. Chu, D. (2018). Broker-Dealers for Virtual Currency: Regulating Cryptocurrency Wallets and Exchanges. *Columbia Law Review*, 118 (8), 2323-2359.

7. Claeys, G., Demertzis, M., Efstathiou, K. (2018). Cryptocurrencies and Monetary Policy. *Bruegel Policy Contribution,* (10).

8. Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L. (2019). Cryptocurrencies as a Financial Asset: A Systematic Analysis. *International Review of Financial Analysis*, 62, 182-199.

9. Desmond, D., Lacey, D., Salmon, P. M. (2019). Evaluating Cryptocurrency Laundering as a Complex Socio-Technical System: A Systematic Literature Review. *Journal of Money Laundering Control,* 22 (3), 480-497.

10. De Vido, S. (2019). All that Glitters is Not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive. *DPCE Online,* 1, 59-76.

11. Dierksmeier, C., Seele, P. (2018). Cryptocurrencies and Business Ethics. *Journal of Business Ethics*, 152 (1), 1-14.

12. Doyle, T. (2002). Cleaning Up Anti-Money Laundering Strategies: Current FATF Tactics Needlessly Violate International Law. *Houston Journal of International Law,* 24 (2), 279-313.

13. Grover, P., Kar, A., Janssen, M. (2019). Diffusion of Blockchain Technology: Insights From Academic Literature and Social Media Analytics. *Journal of Enterprise Information Management,* 32 (5), 735-757.

14. Haffke, L., Fromberger, M., Zimmermann, P. (2020). Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them. *Journal of Banking Regulation,* 21 (2), 125-138.

15. Irwin, A. S., Choo, K. R., Liu, L. (2012). An Analysis of Money Laundering and Terrorism Financing Typologies. *Journal of Money Laundering Control,* 15 (1), 85-111.

16. Koster, H. (2020). Towards Better Implementation of the European Union´s Anti-Money Laundering and Countering the Financing of Terrorism Framework. *Journal of Money Laundering Control,* 23 (2), 379-386.

17. Levi, M., Reuter, P. (2006). Money Laundering. *Crime and Justice,* 34 (1), 289-375.

18. Lucian, R. (2010). The Concept of Money Laundering in Global Economy. *International Journal of Trade, Economics and Finance,* 1 (4), 354-360.

19. Marian, O. (2013). Are Cryptocurrencies "Super" Tax Havens? *Michigan Law Review First Impressions,* 112 (38), 38-48.

20. Mendelson, M. (2019). From Initial Coin Offerings to Security Tokens: A U.S. Federal Securities Law Analysis. *Stanford Technology Law Review,* 22 (1), 52-94.

21. Middlebrook, S.T., Hughes. S.J. (2014). Regulating Cryptocurrencies in the United States: Current Issues and Future Directions. *William Mitchell Law Review,* 40 (2), 813-848.

22. Peters, G.W., Chapelle, A., Panayi, E. (2016). Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective. *Journal of Banking Regulation,* 17 (4), 239-272.

23. Preston, J. (2017). Initial Coin Offerings: Innovation, Democratization and the SEC. *Duke Law & Technology Review,* 16 (1), 318-332.

24. Raymaekers, W. (2014). Cryptocurrency Bitcoin: Disruption, challenges and opportunities. *Journal of Payments Strategy & Systems,* 9 (1), 30-40.

25. Rennock, M. J. W., Cohn, A. Butcher, J. R. (2018). Blockchain Technology and Regulatory Investigation. *Practical Law The Journal,* 4, 35-45.

26. Ryder, N. (2008). The Financial Services Authority and Money Laundering: A Game of Cat and Mouse. *Cambridge Law Journal,* 67 (3), 635-653.

27. Slattery, T. (2014). Taking a Bit out of Crime: Bitcoin and Cross-Border Tax Evasion. *Brooklyn Journal of International Law*, 39 (2), 829-873.

28. Singh, K., Best, P. (2019). Anti-Money Laundering: Using Data Visualization to Identify Suspicious Activity. *International Journal of Accounting Information Systems*, 34.

29. van Wegberg, R., Oerlemans, J., van Deventer, O. (2018). Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin. *Journal of Financial Crime*, 25 (2), 419-435.

30. Vandezande, N. (2017). Virtual Currencies Under EU Anti-Money Laundering Law. *Computer Law & Security Review*, 33 (3), 341-353.

31. Viswanathan, M. (2018). Tax Compliance in a Decentralizing Economy. *Georgia State University Law Review*, 34 (2), 283-333.

32. Woodside, J., Augustine, F., Giberson, W. (2017). Blockchain Technology Adaption Status and Strategies. *Journal of International Technology and Information Management*, 26 (2), 65-93.

33. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14 (4), 352-375.

EU and international legislation

34. Council Directive 2006/112/ EC of 28 November 2006 on the common system of value added tax, 28 November 2006, OJ L 347, 11.12.2006, p. 1-118, art. 135 (1) (e)

35. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284, 12.11.2018, p. 22-30, art. 4, 7, 8 (a), (c), (f)

36. 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)*, Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF , 8 May 2021.

37. European Parliament and Council of the European Union, Directive (EU) 2015/849 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, 20 May 2015, OJ L 141, 5.6.2015, p. 73-117, art 3.

38. European Parliament and Council of the European Union, Directive (EU) 2018/843 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, 30 May 2018, OJ L 156, 19.6.2018, p. 43-74, art. 1 (2) (d) (18), 1 (2) (d) (19), 1 paragraph 29, recital no. 8, recital no. 10.

39. European Parliament and Council of the European Union, Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 25 November 2015, OJ L 337, 23.12.2015, p. 35-127.

Other countries´ legislation

40. Foreign Account Tax Compliance Act of 2009, H.R.3933

41. Hawaii Money Transmitters Act § 489D-8 (a).

42. New York Codes, Rules and Regulations Title 23 § 200.9 (b), (c)

43. Rikoslaki 39/1889 Section 32 § 6

Court decisions

44. Complaint, United States District Court Southern District of New York, 20 Civ. 10832, *Securities and Exchange Commission v. Ripple Labs Inc., Bradley Garlinghouse, and Christian Larsen.*

45. Court decision, Skatteverket v David Hedqvist, C-264/14, EU:C:2015:718

Other sources

46. Coinfirm. (2020). *6th Anti-Money Laundering Directive: EU´s 6AMLD*, Retrieved from https://www.coinfirm.com/blog/6amld-6th-anti-money-laundering-directive/ , 8 May 2021.

47. Comply Advantage. (2020). *Crypto-Assets, Wallets, Exchanges and 6AMLD,* Retrieved from https://complyadvantage.com/knowledgebase/crypto-assets-wallets-exchanges-6amld/ , 8 May 2021.

48. Covolo, V. (2019). The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5th Anti-Money Laundering Directive. *University of Luxembourg Law Working Paper Series*, No. 2019-015.

49. di Angelo, M., Salzer, G. (2020). *Tokens, Types, and Standards: Identification and Utilization in Ethereum.* Conference Paper, 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Online Event.

50. European Central Bank. (2012). *Virtual Currency Schemes.* Retrieved from: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf , 21 November 2020.

51. Europol. (2015). *The Internet Organized Crime Threat Assessment.* Retrieved from: www.europol.europa. eu/sites/default/files/publications/europol_iocta_web_2015.pdf , 12 April 2021.

52. Houben, R., Snyers, A. (2018). *European Parliament Policy Department for Economic, Scientific and Quality of Life Policies. Cryptocurrencies and Blockchain Study: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion*. Retrieved from https://blog.elitex.ir/wp-content/uploads/2020/06/Cryptocurrencies-and-Blockchain.pdf, 8 April 2021.

53. Jafari, S., Vo-Huu, T., Jabiyev, B., Mera, A. Mirzazade, R. (2018). Cryptocurrency: A Challenge to Legal System. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172489 , 12 April 2021.

54. Nabilou, H., Prüm, A. (2019). Central Banks and Regulation of Cryptocurrencies. *Review of Banking and Financial Law (Forthcoming), University of Luxemburg Law Working Paper*, No. 2019-014.

55. Pieters, G.C. (2016). The Potential Impact of Decentralized Virtual Currency on Monetary Policy. Annual Report, Globalization and Monetary Policy Institute, Federal Reserve Bank of Dallas, p. 20-25.

56. Schneider, F., Windischbauer, U. (2010). Money Laundering: Some Facts. *Economics of Security Working Paper*, No. 25, Deutsches Institut für Wirtschaftsforschung (DIW), Berlin.

57. Sprenger, P., Balsiger, F. Anti-Money Laundering in Times of Cryptocurrencies. KPMG Compliance Matters, June 2018.

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[86]

I Tuomas Capraro

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis The 5th Anti-Money Laundering Directive in the Light of Virtual Currencies: The Exploitation of the Decentralized System and Rising Legislative Challenges

supervised by Agnes Kasper, PhD,

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.

---

9 May 2021

[86] *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.*