RIGA GRADUATE SCHOOL OF LAW

# The path to regulating cryptocurrencies in the European Union and in the Republic of Lithuania

BACHELOR THESIS


AUTHOR: Marta Ceimere
LL.B 2019/2020 year student
student number B019065

SUPERVISOR: *IEVA RĀCENĀJA*
*MBA*


DECLARATION OF HONOUR:

I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2022

## ACKNOWLEDGMENTS

This endeavor would not be possible without my supervisor Mrs. Ieva Rācenāja, therefore the author of this thesis expresses her deepest appreciation for support and assistance throughout the whole writing process.

The author would like to extend her sincere thanks to the Riga Graduate School of Law amazing library personnel for being so accommodating and understanding with regards to numerous book deadline-extensions the author requested.

Furthermore, the author is also thankful to the personnel of Riga Graduate School of Law for creating a family-like atmosphere, and for the words of encouragement, motivation when needed, as well as constructive critique, shaping students to strive to achieve more throughout these three years.

To conclude, I would be remiss for not mentioning my family, that has been my biggest support throughout this experience.

## ABSTRACT

Money laundering is regarded as being among the most serious types of financial crime, harming economy and affecting society. Along with constantly developing technological advancements, the scale of money laundering offences has also been pushed to new heights. The existing legal framework's works towards reducing the loopholes posed by current financial instruments, however those with a desire to engage in illicit activities continue to devise new strategies, creating new, possibly unforeseen threats to financial integrity.

The focus of this thesis is to comprehend and analyze the European Union's Anti-Money laundering regulatory framework towards mitigating the risks of money laundering though cryptocurrencies and reduce the regulatory scope by looking at the regulatory framework of one of the European Union's member states - the Republic of Lithuania.

**Key words:** Anti-Money Laundering, cryptocurrency, virtual currency, European Union, Lithuania, AMLD5.

## SUMMARY

Alongside investors and various companies increasingly gaining interest in cryptocurrencies, also criminals have not slept on a golden pit and cryptocurrencies have become a favorable way to launder illicitly acquired funds, due to their level of anonymity, cross-border nature, and decentralized nature. Regulators and governments, on the other hand, have not taken cryptocurrencies as seriously as they should have, and have been rather hesitant to regulate this area, leaving cryptocurrency markets and service providers in underdeveloped regulatory areas, and exposing them to possible exploitation of the colossal potential of cryptocurrencies for illicit purposes.

This thesis "The path to regulating cryptocurrencies in the European Union and in the Republic of Lithuania" seeks to answer question - 'How thorough is the European Union's Anti-Money Laundering regulatory approach to tackle money laundering (ML) through cryptocurrencies?' It looks at Anti-Money Laundering (AML) regulation requirements, mainly set out in fifth EU AML Directive, and its implementation in a national, Lithuanian, legislation. The aim is to comprehend the existing AML regulatory approach to cryptocurrencies and its future potential and approach towards regulating this fast-developing technology to eliminate risks of its exploitation.

This thesis is shaped by looking at cryptocurrency exchange service providers and crypto wallet service providers from the perspective of EU's AML requirements, later narrowing the focus to Lithuania's legislation. It must be pointed out that terms 'virtual currency' and 'cryptocurrency' are used interchangeably throughout this thesis, as in many documents and studies term 'virtual currencies' is preferred as it entails cryptocurrencies as well. Furthermore, this thesis will solely concentrate on AML requirements, hence avoiding any interaction with the any aspects, such as tax laws.

This work is structured into three main chapters with supplementing subchapters. The first chapter establishes the concepts of ML and cryptocurrencies, elaborating on the accompanying risks that are posed by cryptocurrencies', thus making them attractive to money launderers. The second chapter discusses the EU's AML regulatory framework, and more specifically, what changes fifth EU AML Directive brings with regards to cryptocurrency wallet and exchange service providers. The focus is to identify possible shortcomings of AML legislative restrictions. The understanding about, what requirements and standards are applied at EU level, logically enables the author to provide the basis for the subsequent analysis of their implementation at national, Lithuanian legislation in the third chapter. The second part of third chapter looks at the future of planned AML regulation, and what loopholes in existing regulatory approach it aims to cover.

The conclusion of the thesis provides a summary and review of the findings from the research part of thesis. Regarding the initial characteristics and the environments of the sphere of virtual assets before and after AML regulation was introduced and discussed in the first part of this thesis. The characteristics of changes taking place as well as the uncertainties they present on the way to attempting integration and harnessing the potential of virtual assets with the biggest gains according to EU policies are discussed in the second part of the thesis.

## TABLE OF CONTENTS

## INTRODUCTION

> Money laundering poses a clear and present threat to citizens, democratic institutions and the financial system. […] The scale of the problem cannot be underestimated, and the loopholes that criminals can exploit need to be closed.[1]

This statement was made by Mairead McGuiness in 2021, the Commissioner responsible for the financial services, stability, and the Capital Markets Union, during European Commission's legislative proposal for strengthening EU's AML rules.[2] This statement stresses the existing threats imposed by money laundering (hereinafter "ML"), and the legislative shortcomings need immediate attention.

In the recent years, the interest about cryptocurrencies and crypto market has been growing, and since then cryptocurrencies have become not only as a means of payment, but, due to their transaction characteristics and underlying technology, also as an ecosystem for criminals to launder funds.[3]

Initially, the fight against ML did not seem to bring any success, hence, the Risk-based approach, proposed with the adoption of third EU AML Directive,[4] was a huge step towards assessing ML risks, as it introduced risk indicators and behaviors, that usually imply possible ML threats. It allowed entities to tackle and handle more risk, as well as specified requirements, such as reporting of suspicious transactions, that financial institutions had to comply with.[5] The advancement of an unprecedented exchange system that permits irreversible, end-to-end, worldwide transactions with comparatively fast transfer speed was something revolutionary, therefore creating regulatory concerns, as immediate regulatory response would not only be impossible but, could be argued, reckless, and possibly doing more harm than good, by, let's say, violating such fundamental right as privacy of individuals.[6] Within the scope of internal market, financial flows move freely and quickly across borders between Member States, which can be exploited by criminals, allowing them to move funds undetected.

The initiative to monitor and control virtual currencies and its underlying technology can already be traced back to 2012, when the European Central Bank emphasized the need to control this sector and the potential risks it poses to financial stability. In the recent years the popularity of cryptocurrencies and other crypto assets has been growing increasingly. Some

---

[1] European Commission. Directorate-General for Communication, available on: https://ireland.representation.ec.europa.eu/news-and-events/news/commission-overhauls-anti-money-laundering-and-countering-financing-terrorism-rules-2021-07-20_en. Accessed March 10, 2022.

[2] *Ibid.*

[3] Europol. *Cryptocurrencies: Tracing the Evolution of Criminal Finances.* p.5, available on: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf. Accessed February 28, 2022.

[4] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing Text with EEA relevance, *OJ L* 309, 25.11.2014, p. 15-36. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0060. Accessed February 28, 2019.

[5] FATF. *Updated Guidance for A Risk-Based Approach. Virtual Assets and Virtual Asset Service Providers.* Available on:https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjZ3ZDhiN_3AhUmlosKHdSpAcwQFnoECA4QAQ&url=https%3A%2F%2Fwww.fatf-gafi.org%2Fmedia%2Ffatf%2Fdocuments%2Frecommendations%2FUpdated-Guidance-VA-VASP.pdf&usg=AOvVaw1mnh8Y6eTBjXsaougX7j_C. Accessed March 10, 2022.

[6] Goodell, Geoff, Aste, Tomasso. "Can Cryptocurrencies Preserve Privacy and Comply With Regulations?" Methods article. Centre for Blockchain Technologies, 28 May 2019. https://doi.org/10.3389/fbloc.2019.00004.

driven by curiosity, others driven by possible profits, and others – driven by chance to scam individuals not knowing what they do, that, of course, also attracts criminals who are constantly looking for easier ways to launder their illicitly acquired funds.

This thesis will examine the regulation of cryptocurrency sector, which is increasingly developing, and its underlying technology, as it holds great potential to become an integral part of global financial system, the same has a great potential to destroy global economy, if the reins of authority fall into the wrong hands. It lacks proper regulatory framework that would shape its development into the right path, taking a full advantage of this technological phenomenon, and eliminate its exploitation for illicit purposes.

Firstly, the historical research method is used for the purposes of examination of the history and development of ML and cryptocurrencies, as well as driving incentives of regulators for development of AML regulatory framework for financial institutions and later cryptocurrencies. Secondly, the empirical research method is used to gain necessary knowledge on the topic, through collecting relevant literature and materials, as well as utilization of secondary sources, such as various studies and recent reports relevant to the topic. Thirdly, the qualitative comparative research method is used, when reviewing, how the Republic of Lithuania implements AMLD5[7] within its national legislation and comparing transactions in crypto-exchanges and in regular banking. Lastly, throughout the process of this research, the analytical research method is used, when structuring my thesis into logical and comprehensive approach, in a way that would clearly address the following research question – 'How thorough is the European Union's Anti-Money Laundering regulatory approach to tackle money laundering through cryptocurrencies?'

This thesis consists of three chapters, complementing each other, and gradually each of the following chapters build on the stock of knowledge acquired in previous chapters.

This thesis beings with establishing the concept and phases of ML, additionally touching upon its impacts on the world's economy. It then moves on to describing the notion of 'virtual currencies', which is often preferred in laws, regulations, and documents, as it entails term 'cryptocurrency'. Next is introduced the underlying technology - blockchain, crypto market participants, as well as a comparison between crypto transactions and 'regular' banking is provided. The chapter ends with bringing cryptocurrencies within the scope of ML, by identifying the main cryptocurrency and ML related risks.

The second chapter scrutinizes EU's AML regulatory approach to cryptocurrencies and regulation of crypto service providers. There will be a detailed examination of Directive (EU) 2018/843, and what are the main changes it brings for cryptocurrency exchange platforms and custodian wallet providers. The second part of chapter introduces AML and its underlying concepts.

In The third chapter, the focus of AML regulatory framework is narrowed by examining the AMLD5 interpretation national jurisdiction of Lithuania. The Author if this thesis chose Lithuania, because it is one of EU's member states, therefore also bound to implement AMLD5 in its national legislation, and Lithuania was one of the first countries in Europe, recognizing cryptocurrencies impact on economy, and amending its AML law by bringing crypto service providers under its scope. Third chapter ends with the assessment of future regulatory

[7] 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 and terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU Text with EEA relevance, *OJ L* 156, 19.6.2018, p. 43-74. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.

framework, and what loopholes it plans to close, and what changes it means for Lithuania's AML framework.

# 1. THE PROBLEM OF MONEY LAUNDERING AND CONCEPT OF CRYPTOCURRENCIES

Money laundering (hereinafter "ML") has been recognized as a problem to economy, society, and financial sector globally for many years now. Regulators and competent authorities have been issuing guidelines and strategies for countries, companies, and different sectors, as well as conducting different type of risk assessments and analysis to evaluate the effectiveness of Anti-Money Laundering (hereinafter "AML") measures adopted. At the European Union (hereinafter "EU") level, ever since adoption of first AML legislation (hereinafter "AMLD1") in 1991[8], the regulator has been increasingly developing new strategies, expanding AML regulatory scope, and enhancing the competence and authority of competent AML agencies.

With the emerge of cryptocurrencies, and technological development, they increasingly have been exploited for the purposes of ML. Therefore, this chapter will and deeper analyse the concept of ML and cryptocurrencies, at the end indicating the cryptocurrencies' characteristics that make them attractive for criminals.

## 1.1 Concept of money laundering

ML is a criminal act, prohibited under Article 1(2) of the Directive (EU) 2015/849 (hereinafter "AMLD4"), and defined as crime under Art. 83 of TFEU. It implies the processing of fraudulently acquired funds to hide their illegal origins.[9] Article 1(3)(4) of AMLD4, in essence, indicates ML as the participation and association to transfer of property, concealment of true nature and possession and use of property, with knowledge that it derives from illegal activities.[10] As term 'funds' is often used in reference to ML, legal doctrine recons, that it should be perceived as synonym to term 'property', which also correlates with FATF recommendations.[11]

A terse definition has been provided by Her Majesty's Revenue and Customs (hereinafter "HMRC") explaining the concept of ML as "exchanging money or assets that were obtained criminally for money or other assets that are clean".[12] It is the key means for criminal organization's to maintain their operations - continuing introduction of illegally acquired cash or 'dirty money' into legal money circulation through various methods.[13] It involves

[8] Council Directive 91/308/EEC of 10 June 1991 on the prevention of use of the financial system for the purpose of money laundering, *OJ L* 166, 28/06/1991 P.0077 – 0083. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31991L0308&from=FR.

[9] FATF. *What is money laundering?* Available on: https://www.fatf-gafi.org/faq/moneylaundering/. Accessed January 1, 2022.

[10] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) OJ L 141, 5.6.2015, p. 73–117. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

[11] Niels Vandezande, *Virtual Currencies: A Legal Framework* (CiTiP, KU Leuven, Cambridge – Antwerp – Portland: Intersentia Ltd, 2018), p. 295.

[12] Lemen, Jen. "Hot Topic Highlight – Money Laundering Regulations Update." Available on: Property Elite, https://www.property-elite.co.uk/post/hot-topic-highlight-money-laundering-regulations-update. Accessed January 1, 2022.

[13] Sanz-Bas, David, Carlos del Rosal, Sergio L. Náñez Alonso, and Miguel Á. Echarte Fernández. 2021. "Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain" *Laws* 10, no. 3: 57. Available on: https://doi.org/10.3390/laws10030057. Accessed February 2, 2022.

incorporating these funds into seemingly legitimate business, for example, a restaurant, and then slowly absorbing these funds as the revenues of business activities, thus presenting them as legally earned money without raising suspicions.[14]

ML is a component of, and thus associated with various types of criminal activities including bribery, terrorist financing, theft, tax evasion, arms trafficking, drug trafficking and arms trafficking.[15] ML regulatory framework often encompasses the notion of counter - terrorist financing (hereinafter "CFT"), as the connection between cryptocurrencies and financial crimes is expanding.[16] But not to be confused, as in the case of terrorist financing, funds can be obtained from both unlawful or lawful sources, whereas in the case of ML, the funds are always illegally obtained, as ML is predicated on a crime that further gives birth to the ML at hand.[17] The EU's fifth Anti-Money Laundering directive (hereinafter "AMLD5") defines ML as:

> The conversion of the proceeds of crime into apparently clean funds, usually via the financial system, for example by disguising the sources of the money, changing its form or moving the funds to a place where they are less likely to attract attention. [18]

ML, as an idea, became more widely known in 1970, when the US President Richard Nixon passed the so-called bank secrecy act, that requires financial institutions to check every transaction which was over $10,000. The rest of the world started to criminalise ML only after 1990s, and the pressure from US became more pronounce after 2001 terrorist attack on the world trade centre in Washington DC. It is therefore rather understandable that, as the world in different countries develop at different speeds, this fight to suppress, limit or eliminate the culture of ML develops at different speeds as well.[19] Consequently, there are many places in the world, coming from different cultures, that have not received very much pressure from various instances and have not been able to fall under the scrutiny of governments or society.[20] So, it is fair to say that it is just their normal *modus operandi,* which would try to fit in today's world. Therefore, as the world starts to develop more and more, and incorporate blockchain technologies and different software's of similar characteristics to blockchain, the importance for greater clarity and ways of action for governments to protect their people, their economies, their income as well as their position as a holder of rains, becomes more urgent.[21]

---

[14] Anti-Money Laundering Centre. What is money laundering? Available on: https://www.amlc.eu/what-is-money-laundering-2/. Accessed January 1, 2022.
[15] DeltaNet International. 5 Basic Money Laundering Offences, available on: https://www.delta-net.com/compliance/anti-money-laundering/faqs/5-basic-money-laundering-offences. Accessed January 1, 2022.
[16] FATF. *Report to the G20 Finance Ministers and Central Bank Governors.* p.2. July 2018, available on: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.
[17] Robbie Houben and Alexander Snyers. *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, Policy Department for Economic, Scientific and Quality of Life Policies (2018). Available on: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.
[18] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on the information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 text with EEA relevance, *OJ L* 141, 5.6.2015, p. 1-18. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R0847.
[19] CoinDesk. Opinion. Crypto Should Disrupt Current Anti-Money Laundering Practices, Not Adopt Them, available on:https://www.coindesk.com/layer2/2022/03/31/crypto-should-disrupt-current-anti-money-laundering-practices-not-adopt-them/. Accessed February 26, 2022.
[20] *Ibid.*
[21] *Ibid.*

According to Dr Ron Pol, a financial crime specialist, very little are the results of the, so to say, policy experiment carried out until now to fight against and limit ML.[22] The current rules in our financial systems do not stop the great majority of money that is being laundered. As stated in the United Nations (hereinafter "UN") estimates, the result of current policies in place is only 1%, meaning that more than 99% of all the ML in the world, as well as assets acquired through criminal means, do not end up being found out about.[23] The value of the annually seized assets globally is from 1 to $2 billion, while the worldwide spending on anti-money laundering (AML) and sanctions compliance is estimated to exceed $180 billion.[24] Plus, AML departments in financial services institutions are more concerned about, and focused on complying with AML legislation than working on stopping the process of ML as such.[25] It is understandable and good to enforce the rules, but it is more necessary to achieve the result to protect the people and reduce the social costs caused by those criminal activities carried out around the world which result in financial gains which are not legally and morally supported and or permitted.[26]

To conclude on the concept, criminals are developing new and more hidden ways to launder money, one could say, more effectively through finding new under-regulated areas, where to freely manifest themselves, and 'clean' the dirty money more. Therefore, it is crucial to eliminate these grey areas with an AML legislation that is thorough and constant - development–oriented, and even though new, not already too old to tackle ML.

### 1.1.1 Money laundering phases

The process of 'cleaning' the money is immensely complex. Theory divides these operations into three phases - placement, layering and integration or investment, where each of the phases involve different illegal activities.[27] However, because of growing sophistication of ML procedures, direct division into these phases may look unrecognizable at times, as they might be overlapping, take place concurrently, or repeat one of the following phases again and again:[28]

1) The phase of placement is the introduction of illegally obtained funds into the financial system, but outside the authorities' jurisdiction, or in exchanges, where there are weaker AML requirements and where cryptocurrencies can be purchased using either fiat currency or another cryptocurrency.[29]
2) The second phase or 'layering' is where the criminals use complex transactions to conceal the illegal origin of funds.[30] The funds are then mixed and integrated into different businesses and placed in different nations and financial institutions, and scattered into different accounts to hide their origin.[31] By employing cryptocurrency exchanges, criminals may exchange one cryptocurrency for another or, by using an Initial Coin Offering (hereinafter "ICO"), use one form of cryptocurrency to pay for

[22] EffectiveAML. PhD, LLB (Hons), BCom (Econ). Ron, available on: https://www.effectiveaml.org/ron/. Accessed May 3, 2022.
[23] *Supra* note 19.
[24] United Nations. *Money Laundering*. Available on: https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed February 26, 2022.
[25] *Supra* note 19.
[26] *Supra* note 22.
[27] St Paul's Chambers. "Stages of Money Laundering Explained." Available on: https://www.stpaulschambers.com/stages-of-money-laundering-explained/. Accessed February 1, 2022.
[28] *Supra* note 13.
[29] *Supra* note 27.
[30] Tookitaki. Money Laundering via Cryptocurrencies: All You Need to Know, available on: https://www.tookitaki.ai/news-views/moneylaundering-via-cryptocurrencies/. Accessed February 1, 2022.
[31] *Supra* note 13.

another. At this stage it is common for criminals to transfer their crypto assets to other jurisdictions.[32]

3) The phase of investment or 'integration' is where the funds are used for lawful financial transactions, such as, granting of loans, corporate investments, investments in assets.[33] All these transactions are recorded in reports, thus justifying their legality, and making it harder to oversight and discover the real origin of funds.[34]

## 1.2 Cryptocurrencies

After being introduced with ML concept and its process in the previous sub-chapter, further the history and development of virtual currencies will be established, to be able to comprehend what are virtual currencies, and what are the key aspects that make them as a financial instrument from an AML standpoint, as well as their weak points that allow them to be exploited for ML purposes. It must be noted, however, that for the example purposes, the bitcoin transactions and nature will be used as standard, as other cryptocurrencies, even though very similar, may have small deviations from example.

### 1.2.1 Background and development of virtual currencies

Imagine seeing your dream car being sold on the internet, and the price set is 5 cows, but you are not a cattle farmer, but sheep farmer. The problem will then be whether the seller will agree on price in terms of sheep, otherwise, you won't be able to buy this car, or, if the seller is in another country, difficulties may arise with regards to transportation of animals, creating additional costs.

Historically, the bedrock for trade was barter system, in which one party of transaction traded goods or services with other party of transaction, which they perceived as equally valuable. Barter system was later replaced by introducing physical currency and measuring goods and services value in terms of money.[35] However, the development of technology and internet, lead to introduction of electronic fund transfer (EFT) by Western Union in 1871.[36] EFTs refer to now-standard electronic bank transfers, where an individual or a company has a bank account in their name, and, by using credit or debit card linked to that bank account, or in an online environment, can transfer money to other person's bank account.[37]

A further rise of information society provided new opportunities for developing e-commerce – services and goods were now available online, which would be quite impossible and unimaginable without the ability to also pay for these services and goods electronically.[38] Consequently, a distinction between electronic money and virtual currency must be established. Electronic money, even though having a non-physical form, is tied to a physically existing currency in one's bank account and can be withdrawn in cash from an ATM[39]. The division between concepts of electronic money and virtual currencies is also provided in the Article

[32] *Supra* note 30.
[33] *Supra* note 13.
[34] *Ibid.*
[35] CSGForte. Electronic Payments: A Brief History, available on: https://www.forte.net/electronic-payments-a-brief-history/. Accessed March 4th, 2022.
[36] *Ibid.*
[37] *Supra* note 11. pp. 26-27.
[38] *Supra* note 11. pp. 26-27.
[39] *Supra* note 11. p. 27.

1(d)(18) of AMLD5,[40] as the definition for the concept of virtual currencies, that states 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 exchange and which can be transferred, stored and traded electronically.[41]

In other words, virtual currencies e.g., Litecoin or Ripple, cannot be withdrawn from an ATM, as they exist only in a digital form.

Virtual currencies can be centralized and decentralized. Centralized virtual currency transactions involve a third-party - repository, who is the central administrator and, typically, also the issuer of the currency, and who aids in the completion of transactions.[42] Bidders both entrust their assets to the central administrator, expecting that their transactions will be securely processed, and, by leveraging the exchange's user network, also new trade-partner connections will be established. Moreover, as the central administration protects these assets, it eliminates the risk of individual investor losing access to his or her virtual currency stored in digital wallet, which could happen in case an individual forgets the key to digital wallet.[43]

Decentralized virtual currencies, unlike centralized currencies, do not involve a third-party intervention - central administrator processing their transactions.[44] These are peer-to-peer (hereinafter "P2P") exchanges on based blockchain network, where transactions are completed using smart contracts.[45] Blockchain uses very clear organization of system – cryptography, to store a list of transaction records, called blocks, and when one transaction takes place, it is routed across a network of many computers, also known as nodes, as everyone owning the particular currency has the same ledger, and when each and every new transaction takes place, this ledger is updated, so it would be the same on all nodes.[46] Before each transaction takes place, it is approved by all the other ledgers, which eliminates the risk of hackers tempering with these ledgers, because, in case a hacker hacks onto someone's computer and decides to change some numbers on a computer for one's benefit, then all the other ledgers will detect that something suspicious is going on.

To provide comparison between the two types, centralized currencies are more regulated, do not provide user anonymity, and control over transactions lies in the hands of central authority, meaning that, before a transaction takes place, it must be authorized from a central administration. They require higher exchange fees, and are more prone to being hacked, as they have single point of failure, meaning that, to leak data and get access to many wallets, one is required to hack into the central administration only, which also shows the level of security that can be provided with having all the control in the hands of one central authority.[47]

---

[40] *Supra* note 7. Article 3(16)(18).
[41] *Supra* note 7. Article 3(18).
[42] CFI. Virtual Currency, available on: https://corporatefinanceinstitute.com/resources/knowledge/other/virtual-currency/. Accessed March 10, 2022.
[43] Nathan Reiff. What are Centralized Cryptocurrency Exchanges? Available on: https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/. Accessed March 10, 2022.
[44] *Supra* note 42.
[45] *Supra* note 43.
[46] *Supra* note 42.
[47] 101 Blockchain. Decentralizes Vs. Centralized: A Detailed Comparison, updated on May 29, 2021., Available on: https://101blockchains.com/decentralized-vs-centralized/. Accessed March 17, 2022.

In the case of decentralized currencies, on the other hand, full control over their transactions lies in the hands of its users, and it provides higher level of security over transactions, as each holder of currency holds a copy of the ledger. However, as the main disadvantages must be noted the virtual currency volatility, and crime, as the users are anonymous, and the blockchain network can be used as a platform for ML,[48] which creates the perception of "thrustless" environment.[49]

Virtual currencies, likewise, can be divided into two following sub-categories. Convertible (open) virtual currencies can be converted into real currency and vice versa. Under this category also falls cryptocurrencies, for example, Bitcoin and Litecoin, which is worthy of attention for the purposes of this paper.[50] Virtual currencies that are non-convertible (closed), rationally, are the opposite of convertible virtual currencies and are designed for internal use withing the specific system, such as, gaming environment as in case of World of Warcraft Gold or in pure cryptocurrency exchanges[51].[52]

### 1.2.2 Brief history of cryptocurrencies

It was important to understand the origins and characteristics of virtual currencies, as cryptocurrencies, despite being a type of virtual currency, has gained greater popularity, and these concepts, also in the scope of this thesis, are frequently used interchangeably.

European Parliament in its study on Cryptocurrencies and blockchain[53] looked at different watch-dog's perspectives and definitions on what is a cryptocurrency, at the end providing the combined definition, including all the key features of cryptocurrency as:

> a digital representation of value that (i) is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa.[54]

This indicates key properties that help to identify and distinguish most cryptocurrencies from other types of virtual currencies, namely, its decentralized operation manner, the use in P2P transactions, non/convertibility into a money, and, rather than relying on third parties – financial institutions, cryptocurrencies operate using distributed ledger technology, that is based on a math-based algorithmic logic (using encryption) to establish an environment that works for every cryptocurrency market participant.[55]

The above indicated definitions clear the air regarding the status of legal tender of cryptocurrencies, clearly establishing that they are not legal tender, due to their price volatility and not general acceptance as a means of payment. This comes as a result of ECB's opinion[56]

---

[48] Ibid.
[49] Supra note 43.
[50] FATF Report. Virtual Currencies, Key Definitions and Potential AML/CFT Risks (June 2014), p.4. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Accessed March 25, 2022.
[51] World of Warcraft Gold, available on: https://www.g2g.com/categories/wow-gold?region_id=166fbf02-6d9a-45a0-9f74-ac3ba5a002b4. Accessed on March 15, 2022.
[52] Supra note 50.
[53] Supra note 17. p.23.
[54] Ibid.
[55] Supra note 11. p. 52.
[56] Council of the European Union. Opinion. Proposal for a Directive of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. [COM(2016) 450 final – 2016/0208

on the European Commission's proposed amendments to AMLD4[57] in October 2016, stressing the need to make a stronger distinction between legal tender and virtual currencies, and, aiming no to promote their use, alleviated the potential benefits of virtual currencies and emphasising the legislative proposal's restrictions on ML/FT.[58] Nevertheless, they are increasingly being used as a payment instrument by businesses,[59] providing the benefits of almost no transaction costs, and, due to their cross-border nature, provides fast transactions transnationally. Therefore, over banks and financial institutions in the conventional sense, it can be argued, that the cryptocurrency transactions provide greater advantage for conducting foreign transactions.[60]

It may be perceived that cryptocurrencies contain necessary qualities and potential, such as better payment system efficiency, and reduced transaction costs, aligned with currency transfers and payments[61], to qualify as an effective alternative for trading value, that can bypass undesirable attention from the State and other actors, who could be well-placed to be able to create a profile on one's activities.[62]

As a result of many failed attempts in the 90s to create, under centralized system, digital currencies, cryptocurrencies are thought to be as spiritual descendants of crypto - anarchism[63], patiently 'waiting' almost 20 years for tech anarchism to arise, and, only after the latter eroded in 2008, the doors for innovation and further development of cryptocurrencies and other virtual alternative currencies opened.[64] The significance was put on the following key areas that, to varying degrees, shape the concept and idea behind cryptocurrencies. These are the anonymity of transactions, privacy of parties to transaction and cryptographic security, which is based on cryptographic schemes aimed at sustaining security and fidelity.[65]

In 2008, the world was introduced with the idea of the first ever cryptocurrency - bitcoin, which was proposed by Satoshi Nakamoto in his whitepaper, addressing the issue of double – spending problem and providing a solution through the use of timestamp server in peer-to-peer transactions.[66] This was a breakthrough, as was achieved, presumably, the impossible – freedom from third parties intermediaries, financial institutions, interference, and manipulation with currencies, meanwhile, providing the same security of transactions and preventing double-spending of the same currency.[67] The idea of Bitcoin network came to realization in 2009,

(COD)], available on: https://data.consilium.europa.eu/doc/document/ST-13666-2016-INIT/en/pdf. Accessed May 5, 2022.

[57] *Ibid.*

[58] *Supra* note 11. p. 288.

[59] Gowa Nandan and Chakravort Chandrani, "Comparative study on cryptocurrency transaction and banking transaction," Global Transitions Proceedings Vol.2, Issue 2. (2021), p.531, accessed March 17, 2022, available on: https://doi.org/10.1016/j.gltp.2021.08.064.

[60] Datinsky P. "European Legal Regulation of Cryptocurrencies through the AML Scope", *Public Governance, Administration and Finance Law Review* Vol. 5. No. 1. (2020): p.41. Available on: Academic Search Complete Hein Online. Accessed February 10, 2022.

[61] *Supra* note 50.

[62] Goodell G and Aste T (2019) "Can Cryptocurrencies Preserve Privacy and Comply With Regulations?", available on: Frontiers in Blockchain, pdf. p. 2., doi: 10.3389/fbloc.2019.00004. Accessed March 20, 2022.

[63] *Supra* note 11. p. 51.

[64] Konstantin Robin. *What is crypto-anarchism and how it evolved?* (May 5, 2020). Available on: https://www.finextra.com/blogposting/18729/what-is-crypto-anarchism-and-how-it-evolved. Accessed March 25, 2022.

[65] *Ibid.*

[66] Satoshi Nakamoto, (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Available on: https://bitcoin.org/bitcoin.pdf. Accessed March 25, 2022.

[67] *Ibid.*

however, its value stayed close to zero, up until 2010, when there appeared bitcoin exchanges, providing the possibility to exchange bitcoins for money.[68] This resulted in the growth of bitcoin's value, and, following achievement of initial parity with the US dollar in 2011, also the first market bubble appeared, where the value of bitcoin went up to 32 US dollars.[69] The following years, a steady growth in popularity continued, by virtue to an increase in the number of retailers accepting bitcoin as a means of payment[70], before, in 2017, the cryptocurrency market underwent sudden dramatic rise of 1204 % in value, consequently rising also bitcoin's value by 700%.[71] Therefore, it is important to note that in cryptocurrency trading, the currency's value is solely based on the willingness of buyer to pay for it, meaning that, it is all based on speculations.[72]

### 1.2.3 Blockchain technology

This section will elaborate on the concept of blockchain technology and its connection to cryptocurrencies. Term 'blockchain' is quite often used in relation to cryptocurrency exchanges, and it indeed is an essential technical component, as blockchain technology, with its notably forward-looking cryptographic technology[73], is the building block for the most cryptocurrencies existing in the market.[74] Having said that, blockchain is not limited to only cryptocurrency market, but it has a much greater capabilities already, and more potential, when looking at future of data, than other existing technological systems.

In essence, blockchain should be understood as decentralized method of record-keeping, that can hold a wide range of information, from financial transactions to digital profiles of individuals, in a cryptographically protected database. This information is put on a joint ledger, which is constantly updated across all the computers by the users themselves (also known as nodes) and verified every time the information is updated.[75] Blockchain is viewed as the leading distributed ledger technology ("DLT"), that serves as the bedrock of the cryptocurrency market.[76]

Before looking at the process of how the transactions on the cryptocurrency exchange market are performed, it's important to get familiar with some of the main concepts, such as 'keypairs' and 'basic authentication process'.[77] A keypair consists of 2 keys – private, that can be created by oneself or generated automatically, and a public key, that is created using Elliptic Curve Digital Signature Algorithm (ECDSA). These keypairs are cryptographically protected and are necessary in order to encrypt and decrypt data, or to secure access to certain data by locking it with the private key, consisting of 256-bit number, where only the holder of private key can unlock it.[78] These keypairs serve as security provider for creating digital signatures, used in the second important concept - basic authentication process, that ensure the verification

[68] *Supra* note 11. p. 52.
[69] *Supra* note 11. p. 53.
[70] *Supra* note 11. p. 53.
[71] Charles Bovaird, (2017). *Why the crypto market has appreciated more than 1,200% this year,* available on: https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/?sh=136a0dd36eed. Accessed March 26, 2022.
[72] *Supra* note 6.
[73] *Supra* note 11. p. 54.
[74] *Supra* note 17. p. 24
[75] *Supra* note 11. p. 5.
[76] Ed. by Philipp Hacker, Ioannis Lianos, Gergios Dimitropoulos, and Stefan Eich 2019. *Regulating Blockchain, Techno-Social and Legal Challenges.* Available on: Academic Search Complete OXFORD University Press, p.3.
[77] Deltec. Author: Outten S. Bitcoin Transaction Validation, What Exactly Goes on Under the Hood? Available on: https://www.deltecbank.com/2021/10/05/bitcoin-transaction-validation-what-exactly-goes-on-under-the-hood/?locale=en. Accessed May 6, 2022.
[78] *Ibid.*

of amount of funds to be sent; wallet, where it should be directed, as well as the accuracy of data provided by the cryptocurrency sender.[79] These keys are stored in a file, therefore, in case this file gets lost, stolen and/ or deleted, also all the cryptocurrency, that is connected to this file containing the keypair, is, consequently, also irretrievably lost.[80]

To provide a more structural point of view on how a transaction in cryptocurrency exchange market, based on blockchain technology, take place, the author will provide a simple example of cryptocurrency bitcoin transaction that can be divided into the following steps:

1) The future owner $P_1$ decides to initiate transaction with first owner $P_0$. $P_1$ must send his/her public key to $P_0$.[81]

2) This transaction is portrayed as a block on the network, by P0 transferring bitcoins by digitally signing a hash of the previous transaction and the P1's public key, thereby verifying the integrity of data[82].[83]

3) This transaction block is then shared with all the miners and nodes on the network.

4) Miners, process of verification with Signature Script using PubKey, will confirm that the requested transaction block is valid, if it runs back "true", or invalid in case it runs back as "false."[84]

5) The verified block is then added to the blockchain or public ledger and validated.

6)The Bitcoins are then moved from User's 1 wallet to User's 2 wallet.[85]

### 1.2.4 Comparison of cryptocurrency transactions with transactions of banking in its conventional sense

Cryptocurrencies only during the last few years have been enjoying an increasing acceptance and interest in the global financial markets. While many individuals, investing in cryptocurrencies, have little to no understanding of the concept, and knowledge about crypto market is shallow[86], consequently also financial criminals are gaining interest in this sector and using gaps in AML legislations and supervision to commit financial crimes.[87] Moreover, the growing interest and demand of cryptocurrencies consequently also drive their prices up, attracting speculators to invest believing, that the prices will further increase.[88] This section therefore is dedicated to highlighting some of the main aspects and characteristics that distinguish cryptocurrency transactions and addresses from 'traditional banking', thus hoping

[79] Ibid.
[80] European Central Bank. Virtual Currency Schemes, October 2012. p. 23. Available on: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Accessed May 11, 2022.
[81] Ibid.
[82] Simplicable. What is a Hashcode? Available: https://simplicable.com/new/hashcode. Accessed May 11, 2022.
[83] Supra note 80.
[84] Supra note 77.
[85] Northeastern University, What is Cryptocurrency? Available on: https://onlinebusiness.northeastern.edu/masters-in-finance-msf/knowledge/guide-to-the-rise-of-cryptocurrency-digital-currency-and-bitcoin/. Accessed April 17, 2022.
[86] CNBC make it. Author: Vega N. More than 1 in 3 cryptocurrency investors know little to nothing about it, survey finds. Published March 4, 2021. Available on: https://www.deltecbank.com/2021/10/05/bitcoin-transaction-validation-what-exactly-goes-on-under-the-hood/?locale=en. Accessed May 13, 2022.
[87] Supra note 3. p.5.
[88] Supra note 59. p.41-42.

to accentuate the possible gaps in cryptocurrency characteristics that make crypto exchange market more appealing to crooks.[89]

As first of key differences in features between transactions in traditional banking system and cryptocurrency exchanges is the anonymity of addresses, which more in-depth analysis will be discussed. In short, while cryptocurrencies can be divided into being anonymous or pseudo-anonymous, no such option is in the banks, as each bank account must be tied to real-life identifiable individual.[90]

Cryptocurrencies also do not keep in their possession the personal data of cryptocurrency owners, thus avoiding the risk of one's personal data being leaked and misused.[91] Consequently, simplify things for criminals to conceal their illegally acquired funds. Therefore, it comes as no surprise that they quickly become the preferable means of cybercriminals, from purchasing illicit items with bitcoin to ransomware campaigns, that require bitcoin payments.[92]

Decentralized cryptocurrencies are not backed or guaranteed by any bank or other central authority, and, by providing peer-to-peer transactions, they avoid the long process of payment processing, that, in traditional banking is done by banks acting like middleman and collecting transaction costs. The 'middleman' function is fulfilled by internal underlying network that governs the system's operation and enables system's members to autonomously verify transactions.[93] Bank accounts are tied to an individual account owner, who goes through the process of financial identification and validation through financial institutions.[94]

Furthermore, according to Statista, figures show that the transaction speed in cryptocurrency exchange, on average, can take up to 10 minutes, excluding situations, where, due to different system imperfections, such as network traffic causing delays, transactions can take up to a few hours[95]. The significance of transaction speed lies in fact that it reveals the efficiency of each cryptocurrency, meaning, the higher the efficiency score, the more it indicates, that the blockchain, underlying the cryptocurrency, is stronger equipped to move the data between parties and validate transactions.[96] Further, the sub-chapter 1.4. introduces 5 of the most popular cryptocurrencies, that, depending on their transaction speed, are arranged as follows. In the first place, with the longest average time of 40 minutes, is Bitcoin, followed by Litecoin and Monero with 30 minutes, Ethereum with 5 minutes, and lastly, Ripple, which has a near-instant transaction time.[97]

Transactions are irreversible, and transaction costs in cryptocurrency exchanges are zero or close to zero. However, as transaction speed is influenced by various factors, including the size and time of the block, and previously mentioned, network traffic. In case the user has

[89] Ibid.
[90] Supra note 59.
[91] Lansky J. "Possible State Approaches to Cryptocurrencies", p.23. Available on: https://pdfs.semanticscholar.org/c14a/cbbb00b5baee7f10b24d224d429ee6b39e0e.pdf. Accessed May 8, 2022.
[92] Bakertilly. Author: Marks T. J. Cryptocurrency and money laundering: why understanding fraud is critical, available on: https://www.bakertilly.com/insights/cryptocurrency-and-money-laundering. Accessed March 24, 2022.
[93] Supra note 59.
[94] Cryptomathic. Authors: Sharma G. April 2018. Digital Identity and eIDAS in Banking, available on: https://www.cryptomathic.com/news-events/blog/digital-identity-and-eidas-in-banking. Accessed May 8, 2022.
[95] Supra note 59.
[96] Statista. Transaction speed ranking of 66 crypto – including DeFi and metaverse – in 2022, available on: https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/. Accessed April 27, 2022.
[97] Ibid.

willingness to speed up the transaction time, one can increase his or her transaction fee, that way speeding up the blockchain.[98] Banks, on the contrary, are monitored and governed by government.[99] International bank wire transfers take on average 3 days to process, due to the process itself being complex, as the bank accounts involved must be reconciled. Banks have a single point of failure because they are based on a centralized system, whereas cryptocurrencies, due to their decentralised nature, can avoid this single point of failure. This provides some level of security for people that choose to do transactions using cryptocurrency exchange over traditional banking.[100] Therefore it is believed that a decentralized system holds a future and is to bring changes also in the banking industry.[101]

## 1.3 Crypto market participants

To gain a perception of how the "ecosystem" of the cryptocurrency market works, the key participants and their signature role within the market will be delved into further.

Before identifying key crypto-market participants, it must be noted that 'obliged entities,' within the scope of AMLD4, have a responsibility to implement policies, controls, and procedures, such as customer due diligence measures, to be able to identify, mitigate, and effectively monitor and eliminate, and inform about suspicious activities or ML/TF related risks, considering customer, transaction, and other relevant risk factors. The introduction of AMLD5 extended the EU's AML Directives personal scope of virtual currency service providers, introducing new obligated entities under the AMLD5, thus making them subject to the same regulations as banks, payment institutions, and other financial institutions.[102]

There are too many cryptocurrency market participants to be able to count them, however, the following ones, describes in this chapter, are the main ones, and most important within the AML regulatory scope.

### 1.3.1 Users

'User' can be both natural and legal persons, that acquires cryptocurrencies available in the exchange market.[103] Under the AMLD5, users are not obligated entities, as EU's AML framework's focus is on setting requirements, that intermediaries must comply with.[104]

The acquirement of cryptocurrencies can take various forms, such as purchase using fiat money; through P2P exchange platforms, where cryptocurrency is bought from other users; directly from the coin issuer; mining and through the purchase of goods or services, where cryptocurrencies are acceptable means of payment,[105] as was the case with Tesla and bitcoin up

[98] Ibid.
[99] Supra note 59.
[100] Ibid.
[101] Gosha R. Central Banking – Capitalism's Single Point of Failure, avaailable on: https://ryangosha.medium.com/central-banking-capitalisms-single-point-of-failure-e4804a4e0ae. Accessed April 18, 2022.
[102] Supra note 17. p.24.
[103] Ibid. p.76.
[104] Ibid. p.23.
[105] Supra note 50.

until May 2021, when Tesla suspended bitcoin as an acceptable means of payment for its vehicles, due to high fossil fuel consumption used in bitcoin mining process.[106]

### 1.3.2 Miners

'Miners' can be an individual, or a group of individuals, who voluntarily engages with their computers, thereby becoming a 'node', in the process of verifying transactions, called 'blocks', on the blockchain, making the important process of computer processing possible.[107] This infuses the system with newly issued cryptocurrency, and facilitates the cryptocurrency scheme's decentralised operation.[108] Miners are crucial players, as without them the problem of double-spending would be very much ongoing.[109] For their engagement miners can request a transaction fee, or, usually, they receive a portion from the newly minted cryptocurrency. It is common for miners to create "mining business", where they profit from generating and trading cryptocurrency for fiat currency or other virtual currencies.[110] There is a murky area in EU's AML rules because of the absence of 'miners' from AMLD regulation. Unser AMLD5 also miners are not identified as obliged entities due to the reason that miners are rather regarded as technological service providers by validating cryptocurrency transactions, not as the intermediaries between the virtual and physical worlds.[111] However, miner's exclusion from EU's AML regulation creates a murky area, creating a possible issue for new ways of exploiting cryptocurrencies for ML purposes by criminals.[112]

### 1.3.3 Cryptocurrency exchanges

'Cryptocurrency exchanges' confer the cryptocurrency exchange services to cryptocurrency market participants. Exchanges mainly quote the exchange rates at which the exchange is ready to buy/sell cryptocurrencies against major fiat currencies or other cryptocurrencies. Some cryptocurrency exchanges even offer a wider range of services - provide e.g., volatility statistics, act as wallet providers, as well as provide conversion services for agents, who also accept cryptocurrencies as a means of payment for their goods or services. In exchange for their service, these exchanges receive commission[113].[114] Article 1(2) of AMLD5[115] also stipulates that cryptocurrency exchanges, which allow users to sell or purchase new cryptocurrency using fiat cash, now classifies as obliged entities under AMLD5, meaning that, so called, pure cryptocurrency exchanges, where payments only using cryptocurrencies are accepted, fall outside of the scope of regulation.[116] Therefore, there is still a grey area with regards to regulating purely cryptocurrency exchanges that are exclusively crypto to crypto exchanges, as they are not obliged to provide identification requirements to FIUs, thus possibly allowing illicitly acquired funds to subsequently pass either through an

[106] Lora Kolodny, Elon Musk says Tesla will stop accepting bitcoin for car purchases, citing environmental concerns (2021), available on: https://www.cnbc.com/2021/05/12/elon-musk-says-tesla-will-stop-accepting-bitcoin-for-car-purchases.html. Accessed March 31, 2022.
[107] *Supra* note 80.
[108] *Supra* note 59.
[109] *Supra* note 17. p.24.
[110] *Ibid.* pp.24-25.
[111] European Commission. Commission Staff Working Document. *Impact Assessment.* Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=GA. Accessed May 11, 2022.
[112] *Supra* note 17. p.76.
[113] *Supra* note 80.
[114] *Supra* note 17. p.26.
[115] *Supra* note 7. Article 1(2) (d).
[116] *Supra* note 17. p.23.

obligated entity or simply allow cryptocurrencies to be used totally beyond the monitored system.[117] For example atomic swap[118], due to the absence of an intermediary, makes it challenging to establish appropriate legislative response if, over time, this platform is utilized by criminals; also cyberattacks and the lack of insurance for crypto assets.[119]

### 1.3.4 Trading platforms

'Trading platforms' serve and function like markets, where the market is the place, or in this case, a platform for trade, giving opportunity to the seller to meet the buyer. To recall what has been said before, the exchange can be both pure cryptocurrency exchange, and exchange involving fiat currencies[120].[121] Like with pure cryptocurrency exchanges, P2P trading platforms, that are managed purely by software, are hard to regulate due to their decentralized nature, again leaving a grey spot, making them extremely difficult to govern them, let alone include them on the list of obliged entities.[122]

### 1.3.5 Wallet providers

'Wallet providers' just like virtual currencies, before introduction of AMLD5, had no unified definition, the concept was clear, but every entity and financial institution provided its viewpoint on what are the wallet providers and what are the key functions they fulfil. AMLD5[123] amended AMLD4's Article 3 by adding the term 'custodian wallet provider' as being:

> […] an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.[124]

Wallet providers are entities that fulfil functions comparable to a safe, but instead of amassing securities and jewellery[125], it provides customers with digital wallets for storing, transferring, and preserving their funds, cryptographic keys, as well as transaction verification codes and overview of the past transaction reports.[126] To authorize access and exchanges from the personal wallet, one needs a master key (also referred to as private key), which is in digital format and consists of hexadecimal codes, thus they do not embody standard perception of 'key', but rather look like this – 80nsd6lafj7ht937wsbfpu40of83rn9aq0li18ng.[127]

By registering with the wallet provider, one can quite simply obtain a crypto wallet, in whichever of the following forms seems most suitable. Desktop wallets, considered as one of the safest forms of wallet, can only be accessed through one's PC, on which it is downloaded.[128]

---

[117] *Supra* note 17. p.24.
[118] CFI. What are Atomic Swaps? Available on: https://corporatefinanceinstitute.com/resources/knowledge/other/atomic-swaps/. Accessed May 12, 2022.
[119] *Supra* note 17. p.77.
[120] *Supra* note 80.
[121] *Supra* note 17. p.26.
[122] *Supra* note 17. p.77.
[123] *Supra* note 7. Article 1(2)(d)(19).
[124] *Supra* note 7.
[125] Martin Quest, *Cryptocurrency Master Bundle; The Art of HOLDING; The Crypto Mining Mindset; The ICO Approach; Cryptocurrency 101; Blockchain Dynamics*, ch.4. Available on: https://www.pdfdrive.com/cryptocurrency-master-everything-you-need-to-know-about-cryptocurrency-and-bitcoin-trading-mining-investing-ethereum-icos-and-the-blockchain-e184666203.html. Accessed February 2, 2022.
[126] *Supra* note 80.
[127] *Supra* note 125.
[128] *Supra* note 11. pp. 54-55.

The downside is hacker attacks or viruses, that might hinder computer's performance and compromise the safety of the crypto wallet.[129] Other form of wallet is custody wallets - a more convenient form, as they are not 'tied' to one computer device, but can be accessed from any location with access of internet. The user's cryptographic key for online wallets is also stored online, thus being more attractive and vulnerable to hacker attacks.[130] Furthermore, there are a form of hardware wallets, that provide high security, as everything else, other than transactions, is stored offline on hardware like USB, thus it is hacker–attack resistant.[131] And lastly, there are software wallets, that can be installed as application on one's mobile device and used for transactions involving Initial Coin Offering (ICO) tokens.[132] However, it is not obliged for users to have a wallet provider, as, with an adequate knowledge, they can set up a wallet themselves.[133]

Like with fiat-to-crypto (and vice versa) cryptocurrency exchanges, custodian wallet providers or 'custodian virtual currency wallet operators' in Lithuania, fall within the concept of obliged entity under AMLD5. They now must comply with the registration and customer due diligence requirements, including monitoring transactions and reporting of suspicious activities to national authorities, which is Financial Crime Investigation Service in Lithuania,[134] [135] and is defined as:

> […] a legal person who is established in the Republic of Lithuania or a branch, established in the Republic of Lithuania, of a legal person of a Member State of the European Union or a foreign state and who provides services of management of custodian virtual currency wallets on behalf of the customers.[136]

Other crypto market participants involved include web administrators, merchants, e.g., Wikipedia and Microsoft, who accept bitcoin as a means of payment, and payment facilitators, who is a payment processor, who allows merchants to accept cryptocurrency as payment, and instantly, in return, receive fiat currency[137].[138]

## 1.4 Top five cryptocurrencies

According to CoinMarketCap, the most trusted cryptocurrency price tracking website in the world right now, as of March 2022, there are issued more than 18000 cryptocurrencies.[139] However, there are some that have gained more popularity and importance than others, including the cryptocurrency pioneer – bitcoin.[140]

---

[129] *Supra* note 125.
[130] *Ibid.*
[131] *Ibid.*
[132] *Ibid.*
[133] *Supra* note 50.
[134] Financial Crime Investigation Service. *Information for legal entities carrying out the activities of virtual currency exchange operators and (or) depository virtual currency wallet operators in the Republic of Lithuania*. Available on: https://www.fntt.lt/en/money-laundering-prevention/information-for-legal-entities-carrying-out-the-activities-of-virtual-currency-exchange-operators-and-or-depository-virtual-currency-wallet-operators-in-the-republic-of-lithuania/4115. Accessed May 1, 2022.
[135] *Supra* note 17. p.77.
[136] *Supra* note 134.
[137] *Supra* note 17. p.26.
[138] Investopedia. What is a Cryptocurrency Payment Gateway? Available on: https://www.investopedia.com/tech/bitcoin-payment-services-introduction/. Accessed April 7, 2022.
[139] CoinMarketCap. Available on: https://coinmarketcap.com. Accessed April 17, 2022.
[140] Investopedia. 10 Important Cryptocurrencies Other Than Bitcoin, available on: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/#citation-1. Accessed April 10, 2022.

### 1.4.1 Bitcoin

It is the largest crypto currency still in existence it is also the original crypto currency.[141] It is a standalone cryptocurrency.[142] Similarly to most cryptocurrencies, bitcoin is based on a blockchain network, which is sometimes called a letter of login transactions. These transactions are distributed across network of computers, created by all the participants of bitcoin cryptocurrency market. Each of those computers compare the information with all the other computers and verify it with the goal of allowing only the true information to exist so as to prevent hacks and scams, and similar type of manipulations with the systems' code in one place. This eliminates the chance or possibility of somehow manipulating with the data that has passed and been through in the bitcoin system.[143] Its anonymity aspect comes from the fact that transactions are not linked to one's personal information, but to a person's wallet.[144] To hide the history, bitcoin creators encourage its users to use new links or addresses for doing every new transaction. To increase their anonymity, they are considering pulling different and random transactions together, so that it would be even harder to trace the origins of transactions in the future.

Currently it is considered that bitcoin has a fast transaction time - up to 10 minutes for transactions to go through. Sometimes though it can take a couple of days. Bitcoins transaction speed is 3 to 6 transactions per second.[145]

### 1.4.2 Ether

If there is both a cryptocurrency and a blockchain platform, this is a cryptocurrency that is most favored by program developers, because of its potential for application in contracts called non-fungible tokens or NFTs.[146] The smart contracts or what they call 'decentralized applications 'or 'DAPPS' are contracts, that the users can make by coding and releasing them. These contracts automatically enforce their clauses. Its plus point is that it brings economic value and can be used beyond just cryptocurrency. Ethereum is the name of the network. Cryptocurrency based on it is called Ether. Evidently these two parts have their own roles. Which also means, if one part is important and brings economic value, the other one also grows.[147] The idea for the smart contract was to bring the growing field of decentralized finance (hereinafter "DeFi") into play as it was a growing field and could bring economic value to its participants.

Theoretically these types of contracts do not need trust from the other party. They call this phenomenon 'trustless P2P financial transactions. These transactions cut out the third parties, save time money, and omit the hurdles.[148] According to Statista, it is also the third most

[141] Forbes Advisor. 10 Of The Best Cryptocurrencies in May 2022, available on: https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/. Accessed April 17, 2022.
[142] IG. Cryptocurrency comparison, available on: https://www.ig.com/en/cryptocurrency-trading/cryptocurrency-comparison. Accessed April 17, 2022.
[143] *Supra* note 141.
[144] *Supra* note 77.
[145] CMC markets. What is ripple? Available on: https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-ripple. Accessed April 17, 2022.
[146] *Supra* note 141.
[147] *Supra* note 142.
[148] Money. 7 of the Best Cryptocurrencies to Buy Now, available on: https://money.usnews.com/investing/cryptocurrency/slideshows/whats-the-best-cryptocurrency-to-buy?slide=3. Accessed April 17, 2022.

traded currency in 2022, just behind bitcoin and ether.[149] Seeing how NFTs have come out of nowhere and become this big news that many are trying to take part in, really shows the importance of being able to bring economic value. [150]

### 1.4.3 Ripple

The underpinning of ripple is a payment network called RippleNet. This payment network is used by major banks, and financial institutions, some of which include American Express and Santander. It is supposedly a decentralized cryptocurrency, because of the very different way it operates when compared to other cryptocurrencies, some therefore question, whether it is truly a decentralized cryptocurrency. One of the reasons for it is that RippleNet can be used without its underlying cryptocurrency - ripple.[151]

This cryptocurrency is praised for its lightning-fast transaction speeds.[152] In a similar way to ether (Ethereum's cryptocurrency), ripple exists as a part of wider network, which also has different applications. That means, if the popularity of those use cases, but their network increases and it is adopted by businesses, ripple will also grow[153]. The value of the report is not in its Ripple XRP token but in its network. With the ripple token or XRP on the platform it can be exchanged to any currency or digital asset. The value comes from the ability to transfer assets quickly around the world. It operates as a competitor to the popular payment system of our financial System called Swift. It does not act as a competitor to different Fiat currencies as currencies like bitcoin aim to do, it just facilitates the transfer of assets on its network. With swift financial institutions need to have accounts in different countries but with a ripple they just need to use the ripple software. Also, it allows currencies to be exchanged using rebel as a mediator currency which results in much lower fees. Currently for some currencies US dollar needs to be the mediator currency as not all currencies can be directly exchanged with other currencies. This directly affects the fees. The costs are lower than for fiat currency exchanges, plus there is no requirement for double fees per intended exchange. ripple is not based on Blockchain technology, it is their own technology known as 'the ripple protocol consensus algorithm' or RPCA. Also, there is no possibility for mining as all their 100 billion tokens are pre-mined. Transaction speeds are 1500 transactions per second impossible to scale up to 50000 transactions per second, which is comparable to Visa.[154]

### 1.4.4 Litecoin

A Cryptocurrency that according to its founder Charlie Lee in its conception was designed to be 'Silver to bitcoin's gold'. Its biggest pro is its fast transaction speed.[155] It is also based on bitcoins original codebase, but not on bitcoin's blockchain, therefore there is no parental node.[156] During its creation it was developed to be faster than bitcoin and be more scalable.[157] So, in a lot of ways it is comparable to bitcoin, but it is mined faster than bitcoin, which allows

[149] Statista. The 100 most traded cryptocurrencies in the law 24 hours as of April 2022, available on: https://www.statista.com/statistics/655511/leading-virtual-currencies-globally-by-purchase-volume/. Accessed April 17, 2022.
[150] *Supra* note 148.
[151] *Supra* note 142.
[152] *Ibid.*
[153] *Ibid.*
[154] *Ibid.*
[155] *Ibid.*
[156] CMC Markets. What is Litecoin? Available on:https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-litecoin. Accessed April 17, 2022.
[157] https://www.coindesk.com/price/litecoin/.

for transfers to be cheap and fast.[158] It is a standalone cryptocurrency[159]. Just like bitcoin, it is a form of digital money which utilizing blockchain technology allows for peer-to-peer (P2P) transactions leaving out controlling institutions censorship and government.

### 1.4.5 Monero

It is a decentralized cryptocurrency, that gained its popularity and acceptance mainly for its privacy-oriented features. The feature advancing its privacy level is that its blockchain is opaque, making transaction details as well as amounts anonymous.[160] It differs from bitcoin in the aspect of anonymity. It is much more anonymous, as it doesn't allow to see the deeper underlying information about the transaction, like, time zones, patterns, locations, wallet size and other key pieces of data that would pose a security risk to persons anonymity or having their identity found out. It is a coin that addresses privacy concerns that bitcoin users might have plus it does not need expensive and specifically designed equipment for the crypto currency to be mined.[161]

## 1.5 Money Laundering risks through cryptocurrencies

As a first step in assessing the risks posed by cryptocurrencies as potential ML instruments for AML. Therefore, this chapter examines the characteristics of cryptocurrencies, that encourage criminals to exploit them for ML purposes, and aims to gain understanding of the underlying risks for AML approaches.

### 1.5.1 Anonymity

In their early days, it was widely believed that all cryptocurrencies provide a high level of anonymity and were perceived as preserving one of basic human rights – privacy. Therefore, anonymity and pseudonymity are one of the key risks underlying cryptocurrencies, that varies in degrees for different cryptocurrencies, making them attractive to criminals for ML purposes. Participants of the cryptocurrency market use anonymity for security and privacy reasons, as well as to move toward individual sovereignty.

To start with pseudonymity, let us take the bitcoin as an example. As one creates a bitcoin wallet, he or she automatically acquires a unique keypair, which allows them to trade bitcoin publicly on the blockchain, using their public key, where other users see this pseudonym, but they are not required to disclose any personality identifying information[162]. But since the financial forensic data about one's public key may be connected to their actual identity, and, as the blockchain records all the transactions, someone with relevant technical knowledge can track bitcoin transactions.[163] Moreover, through network analysis, this key may be linked back to the digital wallet or IP address, therefore disclosing the identity of

[158] *Supra* note 142.
[159] *Ibid.*
[160] Investopedia. Monero (XRM) Cryptocurrency, available on: https://www.investopedia.com/tech/introduction-monero-xmr/. Accessed April 17, 2022.
[161] Genesis Mining. Monero and Bitcoin: What's the Difference? Available on: https://www.genesis-mining.com/monero-vs-bitcoin. Accessed April 17, 2022.
[162] Cryptopedia. Anonymity vs. Pseudonymity In Crypto, available on: https://www.gemini.com/cryptopedia/anonymity-vs-pseudonymity-basic-differences. Accessed on April 20, 2022.
[163] Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). "Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain." *Journal of Management Information Systems*, *36*(1), 37–73. https://doi.org/10.1080/07421222.2018.1550550.

the user or provide information, which crypto wallets are transferring bitcoins to other crypto wallets.[164]

When referring to anonymity, it can be described as a way of concealing one's personal identification, that, unlike with pseudonymous cryptocurrencies, is estimated to be untraceable, providing high level of secrecy, and absence of distinctive character from other market participants.[165] Monero[166] with its strongly decentralized network, offers the highest level of privacy and anonymity among all cryptocurrencies, as its transactions are untraceable, and by virtue of Ring Confidential Transactions, the amounts sent or received - unknown. It employs ring signatures and stealth addresses that hides the real identities of parties to transaction.[167] Recital No.9 of AMLD5[168] identifies anonymity as potential threat to financial integrity stating that "[t]he anonymity of virtual currencies allows their potential misuse for criminal purposes. […] because users can also transact without such (exchange service and wallet) providers."[169] Anonymity hinders the monitoring process of cryptocurrency transactions, thus making it way harder to trace shady transactions and hide illegal source of funds, making it easier for ML operations to be conducted.[170] Lithuania has identified the 'anonymity', or lack of reliable customer identification as high risk with regards to money laundering.[171]

According to study done by TAX3 committee[172] in 2018, as one of main issues regarding ML through cryptocurrencies was identified the level of anonymity of cryptocurrencies, emphasizing that, even though some cryptocurrencies enjoy pseudonymity, meaning that with investing adequate effort, the authorities can trace the identities of users, it is still a burden for law enforcement to effectively catch the criminals, as the detection, investigation and persecution of cryptocurrency ML cases is a very complex and costly process.[173]. Other cryptocurrencies are claimed to enjoy utter anonymity, which was the case with bitcoin, that had a reputation of preserving anonymity and privacy of users[174]. This myth was broken with the recent cases of Colonial Pipeline hack,[175] and a case involving conspiracy to launder money through bitcoin in Manhattan, where the two users were tracked down and

---

[164] CryptoMag. Bitbay Crypto Exchange Full Review & Step by Step Guide, available on: https://cryptomag.me/bitbay-review/. Accessed on March 21, 2022.

[165] Susan V. Scott and Wanda J. Orlikowski. (September 2014). "Entanglements in Practice: Performing anonymity Through Social Media." *MIS Quaterly,* Vol.38, No.3, p.875. Available on: https://www.jstor.org/stable/26635004?seq=11. Accessed April 18, 2022.

[166] Investopedia. Monero (XRM) Cryptocurrency, available on: https://www.investopedia.com/tech/introduction-monero-xmr/. Accessed April 17, 2022.

[167] Kanstrén T. (2021). "Maping Ring Signatures and Stealth addresses in Monero," available on: https://medium.com/coinmonks/mapping-ring-signatures-and-stealth-addresses-in-monero-a5543a434684. Accessed March 23, 2022.

[168] Noether S., Mackenzie A., The Monero Research Lab. "Ring Confidential Transactions." Available on: https://www.researchgate.net/publication/311865049_Ring_Confidential_Transactions. Accessed May 1, 2022.

[169] *Supra* note 7. Recital No. 9.

[170] IMF Staff Discussion Note. *Virtual Currencies and Beyond: Initial Considerations.* p.27 Available on: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf. Accessed May 3, 2022.

[171] *Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing.* p.60. https://www.fntt.lt/data/public/uploads/2020/05/final-nra_eng_v3.pdf. Accessed May 5, 2022.

[172] *Supra* note 17. p.53.

[173] *Ibid.*

[174] CNET. Is Bitcoin Really Anonymous? Available on: https://www.cnet.com/personal-finance/crypto/is-bitcoin-really-anonymous/. Accessed April 26, 2022.

[175] Reuters. U.S. seizes $2.3 mln in bitcoin pai to Colonial Pipeline hackers, available on: https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/. Accessed May 8, 2022.

arrested.[176] These investigations took, however, a lot of time and resources, thus, this type of approach to combat ML in cryptocurrency sector would not qualify as an effective fighting mechanism. However, KYC / AML requirements are now imposed on leading crypto exchanges, for example, the largest crypto exchange in Europe Bitbay[177], requiring them to match the digital wallet address to the user's real-world identity, therefore, there is a hope to possibly see some positive changes in efforts to de-anonymization of cryptocurrency users.[178]

### 1.5.2 Traceability

As hereinbefore stated, on the one hand cryptocurrencies are completely anonym, allowing to possess a key pair, also referred to as address, where other users transfer funds to you, without it containing any information that would help to trace back to users' identity.[179] In principle, therefore, if one person owns numerous key pairs, thus different addresses, then there is no connection between them, that could possibly lead to tracing down the owner of them.[180] This approach was suggested in the original bitcoin whitepaper, where the bitcoin inventor Satoshi Nakamoto said that:

> […] an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belong to the same owner.[181]

This suggests that, on the other hand, cryptocurrency – bitcoin is very traceable, transparent, and public. Processing transactions with cryptocurrency is comparable to writing anonymously and using pseudonym, meaning that decentralised cryptocurrencies based on blockchain technology algorithm ecosystem is traceable. For example, if an author's pseudonym is ever connected to his or her real identity, everything that has ever been written under that pseudonym, can lead to them revealing their identity.[182]

Due to the fact that all transactions on blockchain are irreversible and with public addresses being transparent, a large map is being generated over time, allowing analytical tools to put puzzle pieces together, creating a vision as to where cryptocurrencies are moving.[183] To conclude about the traceability aspect, its complete protection is provided from cryptocurrency service providers' part, and the rest is left up to the owners' attentiveness and precision not to create a detectable link between his or her real identity and key pair. This anonymity, thus untraceability of identity of the wallet owner and true beneficiary, is the aspect that allows criminals to hide their identity behind numerous wallets, conducting scam transactions, thus misleading government, as, to be able to seize the illicitly acquired funds, they, in the first place, must know, who the criminal is, and that he or she has these funds in their possession. This

[176] Department of Justice. *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency.* Available on: https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency. Accessed May 8, 2022.
[177] *Supra* note 164.
[178] ULAM LABS. Is Cryptocurrency Anonymous? The Myth of Anonymity Debunked, available on: https://www.ulam.io/blog/is-cryptocurrency-anonymous/. Accessed April 26, 2022.
[179] Acuant. How Anonymous Is Cryptocurrency? Available on: https://www.acuant.com/blog/how-anonymous-is-cryptocurrency/. Accessed April 26, 2022.
[180] Supra note 174.
[181] Nakamoto S. "Bitcoin: A Peer-to-Peer Electronic Cash System," p.6. Available on: https://bitcoin.org/bitcoin.pdf. Accessed May 5, 2022.
[182] *Supra* note 179.
[183] *Ibid.*

might be opening an interesting edge that, in the future, it will be even easier to oversee the cryptocurrency market and transactions.[184]

Cryptocurrencies are easy to access, everyone with willingness can set up a crypto wallet, and exchange cryptocurrencies. This makes them more appealing transnationally for moving and storing funds that can further be used for criminal purposes, including ML.[185] The element, creating challenges to policymakers, is the cross-border nature of cryptocurrencies,[186] and, according to Lithuania's National Risk Assessment (2020)[187], aimed at evaluation and identification of ML/TF risks and vulnerabilities affecting Lithuania's internal market, the traceability aspect, which is argued to give room for criminals to launder money. The problem with traceability has been identified as high risk with regards to ML.[188] Many cryptocurrency issuers choose to establish outside national jurisdiction, making traceability problematic. Moreover, significant technological solutions are required to identify virtual currency receivers. Due to the inability to track funds, it is difficult to assess risks and extent of cryptocurrencies role in ML. It has been identified by the Lithuania supervisory authority that it lacks unified legislative framework with regards to reduction of ML risks.[189]

### 1.5.3 Decentralized system

The underlying decentralized system of cryptocurrencies is a blessing on the one hand, and a curse on the other, making them vulnerable to anonymity risks for the purposes of identification and verification for suspicious transactions. Taking a pseudonymous cryptocurrency bitcoin as an example – it has no requirements to market participants with regards to providing their real-life identity for verification purposes. Nevertheless, in cases where participants themselves, due to lack of technical knowledge or negligence, have not taken precautionary steps, thus leaving links between their crypto addresses and their real-life identity or IP address, law enforcement authorities and individuals with adequate technical knowledge are able identify these users.[190]

[184] *Ibid.*
[185] FATF. *Report to the G20 Finance Ministers and Central Bank Governors.* p.2. July 2018, available on: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.
[186] *Supra* note 170.
[187] *Supra* note 171.
[188] *Ibid.*
[189] *Ibid. pp.39-40.*
[190] FATF. *Guidance for a Risk-based Approach Virtual Currencies.* p. 31. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Accessed April 17, 2022.

## 2. EUROPEAN UNION ANTI-MONEY LAUNDERING REGULATORY FRAMEWORK OF CRYPTOCURRENCIES

The overall knowledge about cryptocurrencies and crypto market is rising, yet still low across EU Member States, hence it is pressing that a strong foundation blocks, an effective measures and regulations are implemented at both EU and national levels, to be able to co-develop with technological developments, and to know how to adapt to new ML risks, when they arise. The core aim of AML regulations is to strengthen financial institution integrity and increase transparency.[191]

The lack of regulation of cryptocurrencies with regards to their degree of anonymity, underlying technology, and decentralized system, may create challenges and burden economy through the unregulated area's exploitation for criminal activities, including ML.

### 2.1. European Union Anti-Money Laundering approach to cryptocurrencies

To better comprehend the present situation of the legal framework for cryptocurrencies in Lithuania, first it is important to review the approach for identifying the composition and distinguishable characteristics of cryptocurrencies at the EU level. There are number of international bodies in various areas of expertise, who contribute with recommendations and guidelines paving the way of more comprehensive regulation at EU and national level, in addition conducting risk assessments and evaluating the efficiency of adopted measures.

The Financial Action Task Force (FATF) was established in 1989 as a result of transnational agreement to combat ML related to drug trafficking.[192] It since has introduced FATF recommendations, consisting of set of standards that help to fight ML/TF through harmonized reaction to organized crime and other threats on global financial integrity. These recommendations set the international standards in the field of ML/FT are being improved from time to time, with the latest version being introduced in March 2022; *and* strengthened to cover new risk areas and emerging methods of financial crime.[193]

Taking a few steps back in EU ML regulatory history, when cryptocurrencies had not yet appeared at the horizon, EU introduced AMLD1 in 1991, aimed at strengthening financial system across different EU Member States, which was later amended with introduction of second Anti-Money Laundering Directive (hereinafter "AMLD2")[194]. But as the environment of ML evolved, FATF updated its Recommendations, resulting in European Commission's

---

[191] European Commission. *Statement By First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourova on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive*. Available on: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3429. Accessed May 11, 2022.

[192] *Supra* note 80. p.29.

[193] FATF. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* Available on: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. Accessed May 13, 2022.

[194] Amended Proposal for a Council Decision on the signing, on behalf of the European Union, and provisional application of the Cooperation Agreement between the European Union and its Member States, of the one part, and the Principality of Liechtenstein, of the other part, to combat fraud and any other illegal activity to the detriment of their financial interests and to ensure exchange of information on tax matters /COM/2009/0644 final/. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0644:FIN. Accessed May 9, 2022.

proposal for third Anti-Money Laundering Directive (hereinafter "AMLD3"), which introduced RBA and customer due-diligence requirements. In 2013, the Commission published proposal for AMLD4, which did not explicitly apply to virtual currencies, including cryptocurrencies and crypto-related service providers, however, European Banking Authority (hereinafter "EBA", 2014) in its opinion on virtual currencies, prompted regulators to include virtual currencies under its scope of AML regulation.[195] The Commission in its Action Plan (February 2016)[196] highlighted the non-existence of regulation of virtual currencies, clarifying that the referral to anonymous electronic money[197] in AMLD4, cannot be speculated as also being applicable to virtual currencies. The European Commission's proposal on amendments to AMLD4 (July 2016) intended at addressing anonymity of transactions, once again highlighting the absence of regulation on cash and anonymous prepaid cards, as well as virtual currency transactions.[198]

Concerning virtual currency transactions EU financial authorities specifically emphasised two areas which were devoid of regulation under EU law. Exchanges or the place of trade for currencies, as well as digital wallets, where currencies are held, stored, or transferred to and from, were pointed out as needing regulation.[199]

AMLD5, which will be analysed more thoroughly in the following sub-section, sets out to enforce all the AMLD4 requirements on cryptocurrency exchanges as well as all their service providers. Particularly, those include customer identity checks, beneficial owners as well as reporting of suspicious transactions with the aim of reducing anonymity associated with these types of transactions.[200] It means that under AMLD5, instead of users only holding their cryptocurrencies using wallet provider services or use cryptocurrency exchange platforms for their transactions, AMLD5 introduces customer due diligence requirements that wallet providers and exchange platform service providers must comply with.[201]

Users that employ software or hardware wallets and trade over P2P networks are still able to trade anonymously,[202] as there are presently no regulations in the EU that permit the tracing of blockchain - based transactions or provide data on the originator/recipient of these transactions.[203] These shortcomings in regulation have been recognized by the Members of European Parliament (MEPs). Hence, at the end of March 2022, members from the Committee on Economic and Monetary Affairs (ECON) and the Committee on Civil Liberties, voted in favour of proposal on regulation to enhance EU regulations against ML/TF, which also covers the traceability aspect of crypto – assets, and rules governing transactions of users with privately - created wallets. These rules will supplement the EU AML package.[204]

---

[195] *Supra* note 11. p. 283.
[196] *Supra* note 194.
[197] *Supra* note 10. Article 12 (d).
[198] *Supra* note 7.
[199] ESMA. *Warning. ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies.* Available on: https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf. Accessed May 5, 2022.
[200] A&L Goodbody. EU regulation of cryptocurrency, available on: https://www.algoodbody.com/insights-publications/eu-regulation-of-cryptocurrency-exchanges-5amld-ups-the-ante. Accessed May 12, 2022.
[201] *Supra* note 17. pp.79-80.
[202] *Supra* note 17. pp.79-80.
[203] European Parliament. *Crypto Assets: new rules to stop illicit flows in the EU.* Available on: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-tt-flows-in-the-eu. Accessed May 9, 2022.
[204] European Parliament. *Initial Appraisal of the European Commission Impact Assessment. Anti-money-laundering package.* Available on:

Cryptocurrency exchanges in the territory of EU have certain requirements that are crucial for facilitating ML combating. For example, they are obligated to fulfil customer due diligence (CDD) requirements, as, due to providers of cryptocurrency exchange platform services are being regulated in the same way banks and other financial institutions are. They have to have KYC requirements in place, and, in case any suspicious activity is identified, they must report that to Financial Intelligence Units (FIUs), which in Lithuania is Lithuanian Financial Intelligence Unit.[205] Sixth Anti – Money Laundering Directive (AMLD6) extends the liability for ML offenses to legal entities as well as people.[206] Consequently, requiring the top management of cryptocurrency wallet and exchange service providers must perform significantly more supervision over their internal AML systems.[207]

### 2.1.1. Directive (EU) 2018/843 (AMLD5)

AMLD5 was introduced because of a rise in the exploitation of cryptocurrencies for ML purposes, EU legislators attempted to control this issue and bring a beam of transparency light with AMLD5, as AMLD4 did not include cryptocurrency exchanges and markets, wallet-providers, or tumbler services as obliged entities,[208] consequently also excluding them from compliance with AML requirements and obligations that obliged entities are subject to.[209]

The scope of AMLD5 covers situations when virtual currency services are provided in a business-to-customer relationship not a business-to-business relationship. This stems from the FATF's incentive providing that virtual currency service providers must be seen as people who operate in a manner of financial institutions, as defined by FATF.[210] Therefore, including only the crypto exchangers, where cryptocurrencies can be converted into fiat currency.

Referring to the definition of virtual currencies under AMLD5 in the subchapter 1.2.1., it introduced unified definition of 'virtual currencies.' The part stating that virtual currencies are accepted as a means of exchange, implies that what counts is the cryptocurrency's *de facto* use as a means of payment, as due to lacking required characteristics to obtain the status of legal tender, individuals using it as a means of exchange, still treat it like one.[211] It further also specifies 'custodian wallet providers', which are entities that offer services to safeguard their client's private encryption keys to hold or exchange cryptocurrencies.[212]

As indicated previously, wallet providers and exchange platforms were not subjects to KYC requirements or obligation to notify competent authorities about potential ML cases, therefore criminals were able to transfer funds into the EU's financial system or inside virtual

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/699467/EPRS_BRI(2021)699467_EN.pdf. Accessed May 2, 2022.

[205] *Supra* note 3. p.7.

[206] EUR-Lex. Proposal for DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM/2021/423 final. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0423. Accessed April 20, 2022.

[207] Comply Advantage. Cryptocurrency Regulations Around The World, available on: https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/. Accessed May 12, 2022.

[208] *Supra* note 191.

[209] *Supra* note 11. pp. 286, 298-303, 309-310.

[210] FATF. *Designated categories of offences.* Available at https://www.fatf-gafi.org/glossary/d-i/. Accessed on May 11, 2022.

[211] DE VIDO, Sara. "All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive." DPCE Online, [S.l.], v.38, n.1, April 2019. Available on: http://www.dpceonline.it/index.php/dpceonline/article/view/643. Accessed May 6, 2022.

[212] *Supra* note 7. Article 1(d)(19).

currency platforms, where sufficient degree of anonymity is provided, being able to hide the illicit origins of funds. AMLD5 subjected virtual currency service providers under 'obliged entities', making them subject to these previous requirements. KYC requirements applies to not only new customers, but also existing ones.[213] It implies that obliged entities are obliged to know their users and perform record-keeping of the relevant data, meaning that they must avoid anonymous accounts. For pseudonymous accounts, AML standards are met without compromising with the partial anonymity of cryptocurrencies as long as the data on the clients are maintained by the obliged entities.[214]

AMLD5 also brought changes for users of crypto service providers, specifically targeting anonymity - one of the key benefits that cryptocurrencies possess. This was a big regulatory step taken as users obtaining their virtual currencies through exchanges or custodial wallet providers, consequently, are obliged to now identify themselves to their crypto service providers.[215] AMLD5 also sets reporting requirements by authorizing FIU's to identify the users and their addresses, hence combating the anonymity characteristic of cryptocurrencies.[216] However, EU acknowledges that existing AMLD's scope which includes crypto-service providers will not completely resolve the challenge of anonymity, since transactions can be conducted without using their services.[217]

## 2.2. Key elements of Anti-Money laundering in the context of cryptocurrencies

In the context of cryptocurrencies and the malpractice of criminals exploiting these exchanges to launder money through anonymous wallets, practical AML plans and programs are crucial for strengthening and maintaining mechanisms fighting all kinds of financial crimes, and to be able to comply with intensifying regulations. The main objectives of AML framework are increased transparency in the financial sector institutions.[218]

An effective AML plan includes three main key elements - 'Know Your Customer' procedure, Transparency framework and Risk - based approach.

### 2.2.1. Know Your Customer procedure

Know Your Customer ("KYC") is one of the cornerstone requirements of due diligence that financial institutions, subject to international AML/CTF standards, are bound to comply with,[219] to hinder the malpractice of criminals in crypto world, such as money laundering,

[213] *Supra* note 11. pp. 303-304.
[214] *Supra* note 211.
[215] *Supra* note 11. p. 304.
[216] Comply Advantage. 5th Anti-Money Laundering Directive (5AMLD): What You Need To Know, available on: https://complyadvantage.com/insights/5mld-fifth-anti-money-laundering-directive/. Accessed April 7, 2022.
[217] *Supra* note 7. Recital 9.
[218] FATF. *Opportunities and Challenges of New Technologies for AML/CFT.* p.42. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf. Accessed April 7, 2022.
[219] GLI. *Blockchain & Cryptocurrency Laws and Regulations 2022 | 10 Cryptocurrency compliance and risks: A European KYC/AML perspective.* Available on: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/10-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective#chaptercontent1. Accessed April 7, 2022.

terrorist financing and tax evasion.[220] The requirements of customer due diligence (CDD) and KYC is specified under Art.13(1)(a)(b) of fourth EU AML Directive (AMLD4) with amendments introduced in fifth EU AML Directive (AMLD5) and states the following:

> (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities;[221]
>
> (b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer, [w]here the beneficial owner identified is the senior managing official as referred to in Article 3(6)(a) (ii), obliged entities shall take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process.[222]

KYC requires from the financial institutions, as well as cryptocurrency exchanges and crypto wallets[223], to assign consumer a risk value based on their tendency to commit financial crime.[224] With regards to countries identified as high-risk sue to their inadequate AML regulations, EU companies are expected to execute more thorough examination of customer due diligence, with the addition of Source of Wealth (SWO) investigations in some cases.[225]

The verification procedure consists of two main steps – collection of all the necessary data and documents that administer the identification of the customer holding the funds, also known as Personal Identifiable Information (PII) and a thorough examination of these documents to verify whether the users indeed are who they say they are[226].[227]

### 2.2.2. Transparency

---

[220] Martin Quest. Cryptocurrency Master Bundle; The Art of HOLDING; The Crypto Mining Mindset; The ICO Approac; Cryptocurrency 101; Blockchain Dynics. Source: https://www.pdfdrive.com/cryptocurrency-master-everything-you-need-to-know-about-cryptocurrency-and-bitcoin-trading-mining-investing-ethereum-icos-and-the-blockchain-e184666203.html., ch.4. Accessed on November 28, 2021.

[221] *Supra* note 7.

222 Supra note 7.

223 Getid. AML and KYC for Crypto Exchanges & Wallets, The 2022 Guide, available on:https://getid.com/aml-kyc-crypto-exchanges-wallets/. April 13, 2022.

224 Ibid.

225 https://www.refinitiv.com/en/risk-and-compliance/eu-anti-money-laundering-directive#fourthaml. April 14, 2022.

226 Martin Quest. Cryptocurrency Master Bundle; The Art of HOLDING; The Crypto Mining Mindset; The ICO Approac; Cryptocurrency 101; Blockchain Dynics. Source: https://www.pdfdrive.com/cryptocurrency-master-everything-you-need-to-know-about-cryptocurrency-and-bitcoin-trading-mining-investing-ethereum-icos-and-the-blockchain-e184666203.html., ch.4. Accessed on November 28, 2021.

227 Supra note 223.

Transparency means that the transactions are traceable. It means that a third-party or somebody besides the one doing a transaction can find out about the contents of a transaction without the person making the transaction even knowing about it at the time or at all.[228]

It is a tool for verifying where the money is coming from and a way to trace where it's originated from. It helps to eliminate illegal activities, such as paying for drugs, human trafficking, and paying for illegal acts like corruption and money laundering et cetera. On a grander scale, the notion of transparency helps to see where the money is in the world and where it flows locally and globally. Moreover, it improves governments' understanding and thus capacity to better regulate the markets.

Governments can see where the money flows and which products and services people spend their resources on. Therefore, some areas' products and services can end up having a higher tax rate. Taxes can be introduced because of preventative measures or to discourage acquiring certain things or buying things of certain type or foreign origin. As a result, this visible flow of money provides information to governments which enable them to see what areas, products, or services should or could be taxed based on the goals they're trying to achieve. When the governing authorities can see what the transaction is about, who the sender is and who is the receiver, they can then decide how to act or react. Without this insight governments are losing control and losing the role of impacting the economic systems in place. Governments are being left out and are losing control, as well as the overseeing role. If, and when that happens, it means, that that role of checking and monitoring has been given to someone else. In the case of bitcoin, it is given to the users and individual parties. It provides the context that the foreseeable risks of a transaction, having a negative or bad outcome to the person willing to do the transaction are greatly reduced. These types of conditions provide a fertile soil for all kinds of unlawful creativity. Thus, when the aforementioned conditions are present, it provides encouragement for all kinds of unlawful activities to fill the unmonitored space.

The logical conclusion is that the more one knows or the more a government agency, authority or body knows about transactions and the origins of money, the better they can locate instances of law being overstepped. Easy access to this type of information makes their job much easier.

Nevertheless, there is another side to transparency or protecting a person's privacy with regards to transactions. It would be a case like Facebook's[229], but probably could end up revealing even much more. It is one thing to check whether the person trying to buy something has enough funds for the transaction to take place, but it is a whole another thing to be able to see peoples' balances in their wallets. That information can be easily considered as well as combined with information about spending habits to play with the price of goods in order to maximize profit. This type of visibility can also serve as a tool to separate people into real groups. Logically that aids in spending less on advertising and having a more laser beamed focus. In that case one should consider what type of impact will people's materialism, internal corruption as well as different outside pressures on moral standard result in. What type of economic atmosphere or even economic cannibalism it will create? Not all organizations in that type of environment would have aggressive policies that people would be aggressively against.

228 Bijsterveld van S. "Transparency in the European Union: A crucial link in Shaping the New Social Contract Between the Citizen and the EU," Faculty of Law. p.10. Available on: https://www.ip-rs.si/fileadmin/user_upload/Pdf/clanki/Agenda__Bijsterveld-Paper.pdf. Accessed April 20, 2022.

229 The Guardian. Judge approves $650m settlement of privacy lawsuit against Facebook, available on: https://www.theguardian.com/technology/2021/feb/27/facebook-illinois-privacy-lawsuit-settlement. Accessed April 20, 2022.

Still, it could be argued that many seemingly innocuous actions, policies, and codes would appear or would try to exist even when people would not agree with something that is or is not against the law. It is said that knowledge is power[230] and if people understand that that holds true, and that knowledge gives power to the one who has it, then it is only a logical conclusion that all the available possibilities giving way to achieving the goal one is striving for will cross one's mind. Especially, if the pressure is not legal but only moral which many could attest is subject to pressure. For instance, if a person who is building some automated systems has a goal or is helping somebody whose sole focus is topline revenue, they will first consider the knowledge and understanding they have, which in the case of transparency might be a lot of intimate data. Then, because of the plethora of seemingly possible and legitimate ways of achieving the desired goal, the actions immoral to some, will seem doable, reasonable or even the best opportunities to act upon.

### 2.2.3. Risk-based approach

The third key AML element is the risk-based approach (hereinafter "RBA"), which is established as a cornerstone of EU AML/CTF system under the fourth EU Anti-Money Laundering Directive (AMLD4).[231] When analyzing the term 'risk', FATF highlights three main components: threat, vulnerability, and consequence. In relation to ML, a threat includes the criminals, their facilitators as well as their money laundering activities. 'Vulnerabilities' consist of the areas and things that can be exploited by threat due to their specificities, loopholes, or shortcomings in their features, or managing systems. the last component 'consequence' indicates the harmful outcome that may occur in case the threat successfully exploits the vulnerabilities.[232]

AMLD4 acknowledging that the levels of money laundering risks differ in different countries, as well as specific sectors due to various factors, including national specificities, and, within the scope of this work, the level of understanding and participation in the cryptocurrency exchanges by both private individuals and financial institutions. RBA refers to a comprehensive, evidence-based decision-making that enables the Union and those acting within it to address the ML risks more effectively.[233] Therefore, each Member State's competent authorities must assess the risks that are most relevant and topical for them, to be able to provide effective regulation and money laundering management strategy.[234]

According to FATF's ML/TF risk assessment in 2014, identifying the following risks as potential AML/CFT risks: anonymity of trade; limited verification and identification procedure of market participants; lack of supervision with regards to AML compliance in cross-border transactions; decentralization is seen as a disadvantage and lack of one central authority that monitors everything.[235]

RBA enables responsible supervisory authorities to optimize their concern and expertise in response to the risks assessed through conducting risk assessment procedure and helps to develop potential risk-based supervision strategies, that offers comprehensive nexus

[230] Francis Bacon (1597).
[231] *Supra* note 7.
[232] FATF. AML/CTF Measures and Financial Inclusion. 2014. pp.19-20. Available on: https://www.fatfgafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf. Accessed on May 8, 2022.
[233] *Supra* note 211.
[234] Zhang Fan, "The "Risk – Based" Principle of AML Management", (September 19, 2017), available on: https://www.acamstoday.org/the-risk-based-principle-of-aml-management/. Accessed February 3, 2022.
[235] *Supra* note 50.

between the money laundering risks indicated for the specific sector on the one hand and proposed supervision strategies for managing these risks.[236] It emphasises the need to identify, understand and evaluate the risks that arise as a result from complicated relationships between AML compliance requirements and cryptocurrency market characteristics. FATF's Recommendation 1[237] is dedicated to application of risk-sensitive measures and implementation of management strategies through RBA.[238]

FATF, as the general principle of RBA recognizes that there are different risk levels - higher risk and lower risk countries, therefore, the latter should not be burdened with unnecessary regulatory requirements, as more simplified measures will consummate the goal of mitigating money laundering though cryptocurrencies, allowing to exempt measures that are excessive and unnecessary. Consequently, in the countries, where the problem is identified as higher risk, there should be adopted more stricter regulatory measures.[239] RBA technique allows countries to develop a more inclusive financial system that is not based on cookie cutter approach, and put their resources, energy and focus only in the areas where needed, assisting in reducing the grey area, where transactions can easily avoid the eyes of regulators, or other supervisory authorities.[240]

[236] FATF. Guidance for a risk-based approach, Supervisors. p.25. Available on: https://www.fatf-gafi.org/media/fatf/documents/Risk-Based-Approach-Supervisors.pdf. Accessed on May 12, 2022.
[237] FATF. Public consultation of FATF's Recommendation 1 and its Interpretive Note. Available on: https://www.fatf-gafi.org/publications/financingofproliferation/documents/consultation-recommendation-1.html. Accessed May 8, 2022.
[238] *Supra* note 232.
[239] *Supra* note 232.
[240] *Ibid.*

## 3. ANTI-MONEY LAUNDERING FRAMEWORK OF CRYPTOCURRENCIES IN THE REPUBLIC OF LITHUANIA, AND WAY FORWARD

The choice to analyze this specific jurisdiction was because the Republic of Lithuania was one of the first European nations to establish comprehensive rules for the financial market actors that operate with crypto assets.[241] Thereby, as Lithuania is a part of EU, it is beneficial to see, how it implements EU AML rules in its national legislation. This chapter will focus on the regulatory framework of cryptocurrencies in the Republic of Lithuanian through the lenses of AML, consequently looking at secondary regulatory framework, guidelines, and studies, as well as changes that are to be brought by upcoming regulations. Lastly, the future regulation, and the main changes it will bring for EU and Lithuania, will be closer observed.

### 3.1. The case of Lithuania

Current AML law regulating cryptocurrencies in the Republic of Lithuania is the Republic of Lithuania Law on The Prevention of Money Laundering and Terrorist Financing (hereinafter "Lithuanian AML Law")[242], with the most recent amendments made on April 15, 2021. It sets general requirements and compliance standards for the subjects of this law and implements relevant EU legal acts.[243]

ML as criminal offence is defined under Article 216 of t Criminal Code of the Republic of Lithuania,[244] stating that legalization of money or property, that has derived from criminal activity. Article 7 of the Criminal Code imposes criminal liability for ML – up to 7 years imprisonment.[245] The Financial Crime Investigation Service (hereinafter "FCIS") provided its interpretation of ML, including notion "assets" instead of "property."[246] This interpretation seems more inclusive with regards to application of cryptocurrencies, as there have been various debates involving cryptocurrencies being considered as "property."[247]

Lithuanian AML Law has implemented provisions of AMLD5 and FATF standards, therefore, under Art. 2($22^2$) of Lithuanian AML Law defining virtual currencies as follows:

> Virtual currencies shall mean a digital representation of value that does not possess a legal status of currency or money, that is not issued or guaranteed by a central bank or any other public authority, is not necessarily attached to a currency, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.[248]

---

[241] Lietuvos Bankas. *V. Vasiliauskas: Clear 'rules of the game' needed for the boomig crypto sector.* Available on: https://www.lb.lt/en/news/v-vasiliauskas-clear-rules-of-the-game-needed-for-the-booming-crypto-sector. Accessed April 20, 2022.

[242] Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing. (Amended on 15 April 2021). Available on: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2c647332ba5111eb91e294a1358e77e9?jfwid=twcznlk4w. Accessed May 1, 2022.

[243] *Ibid.* Article 1.

[244] Criminal Code of the Republic of Lithuania. Availabe on: https://www.derechos.org/intlaw/doc/ltu1.html.

[245] *Ibid.* Article 7.

[246] Financial Crime Investigation Service. *Legal Acts of the Republic of Lithuania.* Available on: https://www.fntt.lt/en/money-laundering-prevention/legal-acts/legal-acts-of-the-republic-of-lithuania/347. accessed May 10, 2022.

[247] Lexicology. "Cryptocurrency – Is it "property" and why does it matter?" Available on: https://www.lexology.com/library/detail.aspx?g=fa95822c-49ae-4701-9288-ed2b49d63d3b. Accessed May 10, 2022.

[248] *Supra* note 7.

Lithuanian AML law goes hand in hand with AMLD5 and makes both custodian virtual currency wallet operator and virtual currency exchange operators as obliged entities, and thus subject to AML rules. Moreover, Lithuania has taken a step further by defining not only wallet provider, as in AMLD5,[249] but also 'public key,'[250] 'custodian virtual currency wallet operator,'[251] 'virtual currency address,'[252] 'virtual currency exchange operator'[253].

On 2017, the BoL demonstrated its position on Virtual Currencies and Initial Coin Offering (ICO). In short, BoL stated that national financial services must not engage in any type of operations and activities involving cryptocurrencies, for example, trading, doing transactions, promote acquiring of cryptocurrencies.[254]

To combat ML/TF, Lithuania supervises exchanges and wallet provider services through licensing and authorisation procedures. Both national Lithuanian enterprises, as well as Lithuanian branches of EU and non-EU companies, can also file for crypto licensing, which means – informing competent authorities. To get authorization to provide cryptocurrency exchange or wallet services, the enterprise must be established in Lithuania (not necessarily physical establishment), with the required minimum share capital of EUR 2500.[255] If authorized, enterprise must perform the necessary AML/KYC requirements, such as customer identification and verification procedures, documentation and record keeping, reporting of suspicious activities, withing the meaning of Art. 17. of the Law, to the Lithuanian FIU. It is therefore important to have an internal AML officer in place before beginning crypto-related activity.[256]

ICOs[257] are also subject to AML regulations, in 2018, Lithuania's Ministry of Finance published 'Guidelines for ICO's'. In short, these guidelines provide a 15% personal income tax rate for buyers and sellers of cryptocurrency. In addition to that, until the tokens are sold, founders of ICOs who get tokens without remuneration will not be taxed.[258] Entities conducting ICO's are not obliged entities, but they must comply with AML/CFT requirements provided under Art.25[1] of Lithuanian AML Law.

Moneywall, in its mutual evaluation report (hereinafter "MER") on Lithuania (2018), discovered that, despite all these virtual asset service providers (hereinafter "VASPs") having AML/CFT measures in place and presenting low AML/CFT risks within their sector, some of them demonstrated poor understanding of these ML risks and core AML measures that must be applied. Moreover, they comply with all AML regulations applicable to financial institutions, even though majority of them are not legally required to do so[259], which, could be argued, is not an effective allocation of resources, and does not comply with the RBA, aiming to regulate

[249] *Supra* note 7. Article 1(2)(d)(19) ; *Supra* note 242. Article 2(3[1]).

[250] *Supra* note 242. Article 2(22[1]).
[251] *Supra* note 242. Article 2(3[2]).
[252] *Supra* note 242. Article 2(22[3]).
[253] *Supra* note 242. Article 2(22[4]).
[254] *Supra* note 242
[255] Cryptonews. Crypto regulatory Environment in Lithuania, available on: https://cryptonews.com/news/crypto-regulatory-environment-lithuania.htm. Accessed May 12, 2022.
[256] *Supra* note 242. Article 9.
[257] *Supra* note 242. Article 17[1] .
[258] ICO Guidelines. 2018. Available on: https://finmin.lrv.lt/uploads/finmin/documents/files/ICO%20Guidelines%20Lithuania.pdf. Accessed May 9, 2022.
[259] Moneywall. "Anti-money laundering and counter-terrorist financing measures Lithuania, Fifth Round Mutual Evaluation Report," p.101.December 2018. Available on: https://rm.coe.int/09000016809247ed. Accessed May 2, 2022.

the higher-risk spheres more, at the same time not overregulating other spheres unnecessary. According to Art. 5(1) (9) of the Law Financial Crime Investigation Service (hereinafter "FCIS") is supposed to provide obliged entities with methodological guidance and evaluation, that includes also training, conceptual framework and guidelines.[260]

Moneywall's both Follow-up Reports (hereinafter "FUR") of 2020[261] and 2021[262] on MER Report of 2018 on Lithuania, showed improvements and steps taken by Lithuania to comply with the FATF Recommendations and identified deficiencies in the MER. There were still identified deficiencies with regards to sanctions and persecution of criminals.

As a lead in the European digital domain, the BoL says that solutions must be developed to diminish the difference in attitudes towards digital securities and financial innovations throughout Europe, as it recognised that quite often technological developments surpass the adaption of regulatory framework, thus threatening to impede growth, and create shortcomings that criminals can exploit. This aspect is recognised as critically important with regards to all virtual assets. BoL stresses the need for clear definitions for digital securities and urges EU to pave the way for progress by shifting from directives to directly applicable European-wide laws.[263]

### 3.1.1. Supervisory authorities

Bank of Lithuania (hereinafter "BoL"), with the merging of three entities monitoring banking, insurance, and capital markets, has been the sole financial market regulator in Lithuania since 2012.[264] Its main operational spheres are Economics and Financial Stability; Banking; Organisation and Supervision.[265] The Financial Stability Service department of the BoL, which comes under the Economics and Financial Stability Service, is responsible for macroprudential supervision, and Supervision Service is responsible for both economic and financial market supervision. [266]

Operational activities of cryptocurrency exchanges and wallet service providers, which also fall under the notion of obliged entities, are regulated by the FCIS as stipulated in Art. 5, 7 and 8 of the Lithuanian AML Law.[267] Article 4(9) of the Lithuanian AML Law stipulates that FCIS is obliged to 'approve instructions together with BoL[268], 'supervise the activities', 'provide methodological assistance' aimed at preventing ML/FT as laid down in the law, for

[260] *Ibid.*
[261] Moneywall. "Anti-money laundering and counter-terrorist financing measures Lithuania, 1st Enhanced Follow-up Report & Technical Compliance Re-Rating Round," p.101. June 2020. Available on: https://rm.coe.int/moneyval-2020-7-sr-5th-round-fur-mer-lithuania/16809ef774. Accessed May 3, 2022.
[262] Moneywall. "Anti-money laundering and counter-terrorist financing measures Lithuania, 2st Enhanced Follow-up Report & Technical Compliance Re-Rating Round," p.101. June 2020. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/fur/MONEYVAL-FUR-Lithuania-Nov-2021.pdf. Accessed May 3, 2022.
[263] Blockchain News. Bank of Lithuania Calls For Uniform Regulation for Digital Financial Innovation Across Europe. Available on: https://blockchain.news/insight/bank-of-lithuania-calls-for-uniform-regulation-for-digital-financial-innovation-across-europe. Accessed May 5, 2022.
[264] OECD. *Lithuania: Review of the Financial System.* p. 16. 2017. Available on: https://www.oecd.org/finance/Lithuania-financial-markets-2017.pdf. Accessed May 12, 2022.
[265] *Ibid.*
[266] Lietuvos Bankas. *Economics and Financial Stability Service established at the Bank of Lithuania.* Available on: https://www.lb.lt/en/news/economics-and-financial-stability-service-established-at-the-bank-of-lithuania. Accessed May 13, 2022.
[267] Cryptonews. Crypto regulatory Environment in Lithuania, available on: https://cryptonews.com/news/crypto-regulatory-environment-lithuania.htm. Accessed May 12, 2022.
[268] *Supra* note 242. Aricle 4(1).

obliged entities and financial institutions.[269] In case obliged entities and/or financial institutions violate the Lithuanian AML Law, the FCIS and BoL may impose sanctions, including fines, suspensions and annulment of licence, as stipulated in Article 36 of the Law.

As the latest step towards strengthening AML supervision, in 2019 BoL established an altered supervisory structure, with separate AML/CFT supervisory body being introduced, which focused solely on the ML/FT related supervision.[270]

## 3.2. Way forward – EU and Lithuanian perspective

On September 24, 2020, European commission launched a proposal on markets in crypto assets (hereinafter "MiCA"). The package of measures proposed was to further enable and support the innovation and potential of digital finance, while at the same time mitigating the risks. One of the main priority areas is to ensure that the EU regulatory framework for financial services does not pose obstacles for innovation and application of new technologies.[271] In February 2021, during the fifth annual conference on Fintech and regulation Commissioner McGuinness illustrated, what environment will be enabled by make up regulation, stating that MiCA regulation will provide authorized enterprises, who are crypto-assets issuers and service providers, with a European passport.[272] This way, issuers and crypto-asset service providers will be able to expand their operations across the Digital Single Market, at the same time mitigating market fragmentation in the crypto sector, currently caused by divergent national regimes.[273] That means that a coin authorized in one EU country can be used across EU countries, without needing registration or notification in each of the countries separately.[274]

The regulation is now moved to discussions between the European Parliament, European Commission and Ministers of Finance.[275] Stefan Berger, the lead member of Parliament commented on the move, saying that MiCA report may set global standards for crypto regulation, as it is unprecedented in terms of innovation, protection of consumer rights and legal certainty.[276] Once established, it will act as a comprehensive solutions package concerning virtual assets. While the provisions on stablecoins will start to apply in the beginning of 2024, the rest of the provisions are expected to come in force from early 2025.[277]

Financial services regulation is based upon four pillars. These are - customer protection; financial market integrity; financial stability and countering of financial crime. Customer protection deals with transparency of the risks and costs involved responsible publicity and different assessments for investors. Financial market integrity is responsible for preventing

[269] *Ibid.* Article 4 and 30.
[270] *Supra* note 261.
[271] *Supra* note 206.
[272] European Commission. *Keynote speech by Commissioner McGuiness at the 5th Annual Conference on FinTech and Regulation: New Challenges and New Solutions.* Available on: https://ec.europa.eu/commission/commissioners/2019-2024/mcguinness/announcements/keynote-speech-commissioner-mcguinness-5th-annual-conference-fintech-and-regulation-new-challenges_en. Accessed May 11, 2022.
[273] *Ibid.*
[274] ING. Regulation and the coming of age of Europe's crypto markets, available on: https://think.ing.com/articles/regulation-and-the-coming-of-age-of-europes-crypto-markets#a8. Acessed May 12, 2022.
[275] *Ibid*.
[276] News, European Parliament. *Cryptocurrencies in the EU: new rules to boost benefits and curb threats.* Available on: https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats. Accessed May 11, 2022.
[277] *Supra* note 274.

market manipulation through trade monitoring and includes trade execution obligations. Financial stability deals with micro-Prudential regulations, that help maintain financial stability and health of institutions and macro prudential rules which help maintain the stability of the whole financial system. Under the latter, cybersecurity rules are also included. The countering of financial crime deals with due diligence, recordkeeping, and obligation to report suspicious transactions. Under MiCA, all four of these pillars will be regulated.[278]

MiCA has distinguished a few categories that will be regulated:

1. Issuance of classic crypto currency. Issuers are required to publish a white paper which contains "mandatory disclosures". Existing crypto assets are exempted from some requirements. Proof-of-work cryptocurrencies will have to publish an energy consumption report.[279]
2. Stable coins. MiCA distinguishes two types - "Asset-Referenced tokens" (hereinafter "ART's") and "E-Money Tokens" (hereinafter "EMT's"). ART's are currencies that are not denominated in any EU currency. ECB has the power to limit their scope, if they risk endangering the operation of payment systems, monetary sovereignty, or transmission of monetary policy. If they are not stable with regards to their external assets, they will not qualify as ART's. EMT's are denominated in Euro, and will function like bank deposits, thus stricter requirements will be applicable. Generally, both stable coins should be assets of high-quality, low risk and liquid, meaning, immediately redeemable at par value.[280]
3. Crypto asset service providers (hereinafter "CASP's"). CASP's include brokers, exchanges custodians and others. They need to be an EU-based legal entity, and assess their clients based on suitability and fitness, and always act in the best interest of the client. CASP's will also have a high degree of liability in case a client falls victim to a hack or some other similar type of loss. Concerning decentralized assets, decentralized autonomous organizations and foreign issuers and service providers, solutions are not yet clear.[281]

It is evident that going forward there are still many things to solve. The whole system needs to adapt to. The EP, Commission and European Council officials need to decide, who will supervise and police these digital assets as they cannot yet decide, if these systems will work more like securities markets, in which case the ESMA (European Securities and Markets Authority) should be responsible, or if these assets work like payments in which case the EBA should be the watchdog.[282] Banks will also need to rethink their business models, how they can work together with currencies like EMT's. Similarly, the environment and things seem more nuanced as the focus gets more localized and issues seem less general, less overarching, and more temperamental or more depending on local sentiments. EU member states are eager to know, how the requirements, that will be imposed on crypto asset service providers, will help local authorities to mitigate the risks threatening financial stability.

In the case of Lithuania cryptocurrencies and their activities are still considered underregulated. Only on March 23, 2022, the draft for amendments to AML law was presented.

[278] *Ibid.*
[279] *Ibid.*
[280] *Ibid.*
[281] *Ibid.*
[282] Politico. Brussels split over who will be crypto watchdog, available on: https://www.politico.eu/article/brussels-split-over-who-will-be-crypto-watchdog/. Accessed May 12, 2022.

Although the amendment has not yet been made public, one of the expected changes is the following. Crypto asset service providers must conduct all parts of their business in the country and Lithuania employs an AML officer; make sure the mandatory requirements for customer identification are met and no anonymous accounts are opened. With regards to MiCA it is not yet publicly known whether Lithuanian authorities will introduce the capital range requirements for CSAP activities laid out in MiCA.[283]

[283] Sorainen. *Stricter regulation of the cryptocurrency sector is under consideration in Lithuania.* Available on: https://www.sorainen.com/publications/stricter-regulation-of-the-cryptocurrency-sector-is-under-consideration-in-lithuania/. Accessed May 13, 2022.

## CONCLUSIONS

As cryptocurrencies are seen as attractive from a criminal's perspective and exploitable for the means of ML, they pose a threat to the fight against ML. Thereby, this thesis focused on the EU's and the Republic of Lithuania's incentives to regulate this fast technologically developing sector and minimize their favorability to be used as ML instrument in the eyes of criminals, as cryptocurrencies hold a great potential in global financial markets, if regulated properly.

After setting the contextual framework, the first chapter introduced the overview of the concepts of ML and cryptocurrencies, as well as the underlying risks of cryptocurrencies that can and are used for ML purposes. The main risks indicated were anonymity/ pseudonymity, cross-border nature and traceability and decentralized nature of cryptocurrencies.

The second chapter focused on the assessment of a more global, EU-wide AML regulatory framework, introducing the currently main AML regulatory instrument – AMLD5, that sets EU-wide standards for regulating virtual currencies. As the main changes it must be indicated that AML imposed regulatory requirements on virtual asset wallet service providers and cryptocurrency exchanges that provide exchange services involving fiat-to-crypto and vice versa transactions, including them under the notion of obliged entities.

Third chapter narrowed the focus by looking at the Republic of Lithuania's AML regulatory framework. It was established that ML risks imposed by cryptocurrencies are not regulated separately but fall under the regulation of their national AML law[284]. Lithuania was between the first countries in Europe that recognized crypto-asset impact on financial markets and enhanced its AML framework including VASPs under its provisions.

The second part of third chapter was devoted for the planned future approach regarding regulation of crypto assets. It provides overview of the big plans EU is aiming to achieve in terms of regulation of crypto assets and the spheres that it is planning to cover, that currently are unregulated or there exist some uncertainties and grey areas on the knowledge or an adequate approach which leave room for criminal's to further exploit cryptocurrencies

The EU's existing AML framework for combating ML currently could be more accurately presented as a collection of laws and regulations than as a homogeneous entity. It lacks legal certainty in certain spheres and the failure of businesses to recognize certain crimes and security breaches. AMLD5 was a big step towards setting the foundation for AML regulatory framework in the sphere of cryptocurrencies. The 5AMLD brought the term "virtual currencies" under which certain virtual assets are currently covered in the EU.

MiCA will introduce a harmonized approach to the term "virtual assets" across all countries in the European Union. Consequently, that means we can expect harmonized sets of rules and for crypto-related services and products across EU countries by the end of 2024. MiCA is aimed to regulate all issues regarding Digital Finance Strategies on a EU level and establish legal certainty across EU member countries.[285] Arguably, the notion of "passporting" of crypto currencies is the most embodying and the most visible illustration of the MiCA's

[284] Republic of Lithuania law …

[285] Bird&Bird. Road to MiCAR: The European Crypto-assets Regulation, available on: https://www.twobirds.com/-/media/new-website-content/pdfs/2022/articles/road-to-micar_en.pdf. Accessed May 14, 2022.

approach to harmonizing the workings of the virtual asset sphere in the EU.[286] On a local perspective, in this case, Lithuania, some of the changes expected are for example, for CASP's to handle all parts of their business in Lithuania, have a manager residing in Lithuania and employ an AML officer. Also, stricter requirements concerning the reputation of the managers, supervisory persons and beneficiaries are expected to be introduced. What is uncertain is whether Lithuania will follow MiCA's recommendations concerning the range of capital requirements (50 000 - 150 000) depending on the specific CASP's activity. Other than these few and some others, it is not yet if some other (if any) supervisory requirements will be introduced that will reduce the risks of money laundering and terrorist financing.[287] As the EU tries to get a handle on the sphere of virtual assets, the fact that DeFi is global and has emerged only after the MiCA was proposed remains to be seen how it will be regulated. Still, the EU's facade desire to remain competitive and take advantage of the innovations these technologies have brought and can bring has already been put into strict guidelines and shown how important part the authorities have positioned themselves to play. The fact that governments are not prepared to give up control, can be deducted from the EU's move to develop their own virtual currency and from the regulation one Asset-Referenced Tokens or ART's which although being high quality and stable will be at the mercy of ECB if it sees that they can potentially pose a risk and to the transmission of monetary policy, monetary sovereignty or pose a danger to payment systems. Obviously, these changes will curb the potential of many service providers and asset providers who will have to adjust or completely pivot their strategy in the face of the EU's desire to limit the potential and scale of illicit activities.

[286] ING. Regulation and the coming of age of Europe's crypto markets, available on: https://think.ing.com/articles/regulation-and-the-coming-of-age-of-europes-crypto-markets. Accessed May 14, 2022.
[287] *Supra* note 283.

## BIBLIOGRAPHY

### Primary sources:


1. Council Directive 91/308/EEC of 10 June 1991 on the prevention of use of the financial system for the purpose of money laundering, OJ L 166, 28/06/1991 P.0077 – 0083. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31991L0308&from=FR.
2. Criminal Code of the Republic of Lithuania. Availabe on: https://www.derechos.org/intlaw/doc/ltu1.html.
3. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) OJ L 141, 5.6.2015, p. 73–117. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.
4. 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 and terrorist financing and amending Directives 2009/138/EC and 2013/36/EU Text with EEA relevance, OJ L 156, 19.6.2018, p. 43-74. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.
5. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing Text with EEA relevance, OJ L 309, 25.11.2014, p. 15-36. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0060. Accessed February 28, 2019.
6. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on the information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 text with EEA relevance, OJ L 141, 5.6.2015, p. 1-18. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R0847.
7. Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing. Available on:https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2c647332ba5111eb91e294a1358e77e9?jfwid=twcznlk4w. Accessed February 20, 2022.


### Secondary sources:


1. /COM/2009/0644 final/. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2009:0644:FIN. Accessed May 9, 2022.
2. 101 Blockchain. Decentralizes Vs. Centralized: A Detailed Comparison, updated on May 29, 2021., Available on: https://101blockchains.com/decentralized-vs-centralized/. Accessed March 17, 2022.
3. A&L Goodbody. EU regulation of cryptocurrency, available on: https://www.algoodbody.com/insights-publications/eu-regulation-of-cryptocurrency-exchanges-5amld-ups-the-ante. Accessed May 12, 2022.

4. Acuant. How Anonymous Is Cryptocurrency? Available on: https://www.acuant.com/blog/how-anonymous-is-cryptocurrency/. Accessed April 26, 2022.
5. Amended Proposal for a Council Decision on the signing, on behalf of the European Union, and provisional application of the Cooperation Agreement between the European Union and its Member States, of the one part, and the Principality of Liechtenstein, of the other part, to combat fraud and any other illegal activity to the detriment of their financial interests and to ensure exchange of information on tax matters
6. Anti-Money Laundering Centre. What is money laundering? Available on: https://www.amlc.eu/what-is-money-laundering-2/. Accessed January 1, 2022.
7. Bakertilly. Author: Marks T. J. Cryptocurrency and money laundering: why understanding fraud is critical, available on: https://www.bakertilly.com/insights/cryptocurrency-and-money-laundering. Accessed March 24, 2022.
8. Bakertilly. Author: Marks T. J. Cryptocurrency and money laundering: why understanding fraud is critical, available on: https://www.bakertilly.com/insights/cryptocurrency-and-money-laundering. Accessed March 24, 2022.
9. Bijsterveld van S. "Transparency in the European Union: A crucial link in Shaping the New Social Contract Between the Citizen and the EU," Faculty of Law. p.10. Available on: https://www.ip-rs.si/fileadmin/user_upload/Pdf/clanki/Agenda__Bijsterveld-Paper.pdf. Accessed April 20, 2022.
10. Bird&Bird. Road to MiCAR: The European Crypto-assets Regulation, available on: https://www.twobirds.com/-/media/new-website-content/pdfs/2022/articles/road-to-micar_en.pdf. Accessed May 14, 2022.
11. Blockchain News. Bank of Lithuania Calls For Uniform Regulation for Digital Financial Innovation Across Europe. Available on: https://blockchain.news/insight/bank-of-lithuania-calls-for-uniform-regulation-for-digital-financial-innovation-across-europe. Accessed May 5, 2022.
12. CFI. Virtual Currency, available on: https://corporatefinanceinstitute.com/resources/knowledge/other/virtual-currency/. Accessed March 10, 2022.
13. CFI. What are Atomic Swaps? Available on: https://corporatefinanceinstitute.com/resources/knowledge/other/atomic-swaps/. Accessed May 12, 2022.
14. Charles Bovaird, (2017). Why the crypto market has appreciated more than 1,200% this year, available on: https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/?sh=136a0dd36eed. Accessed March 26, 2022.
15. CMC markets. What is ripple? Available on: https://www.cmcmarkets.com/en/learn-cryptocurrencies/what-is-ripple. Accessed April 17, 2022.
16. CNBC make it. Author: Vega N. More than 1 in 3 cryptocurrency investors know little to nothing about it, survey finds. Published March 4, 2021. Available on: https://www.deltecbank.com/2021/10/05/bitcoin-transaction-validation-what-exactly-goes-on-under-the-hood/?locale=en. Accessed May 13, 2022.
17. CNBC make it. Author: Vega N. More than 1 in 3 cryptocurrency investors know little to nothing about it, survey finds. Published March 4, 2021. Available on: https://www.deltecbank.com/2021/10/05/bitcoin-transaction-validation-what-exactly-goes-on-under-the-hood/?locale=en. Accessed May 13, 2022.

18. CNET. Is Bitcoin Really Anonymous? Available on: https://www.cnet.com/personal-finance/crypto/is-bitcoin-really-anonymous/. Accessed April 26, 2022
19. CoinDesk. Opinion. Crypto Should Disrupt Current Anti-Money Laundering Practices, Not Adopt Them, available on:https://www.coindesk.com/layer2/2022/03/31/crypto-should-disrupt-current-anti-money-laundering-practices-not-adopt-them/. Accessed February 26, 2022.
20. CoinMarketCap. Available on: https://coinmarketcap.com. Accessed April 17, 2022.
21. Comply Advantage. 5th Anti-Money Laundering Directive (5AMLD): What You Need To Know, available on: https://complyadvantage.com/insights/5mld-fifth-anti-money-laundering-directive/. Accessed April 7, 2022.
22. Comply Advantage. 5th Anti-Money Laundering Directive (5AMLD): What You Need To Know, available on: https://complyadvantage.com/insights/5mld-fifth-anti-money-laundering-directive/. Accessed April 7, 2022.
23. Comply Advantage. Cryptocurrency Regulations Around The World, available on: https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/. Accessed May 12, 2022.
24. Council of the European Union. Opinion. Proposal for a Directive of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. [COM(2016) 450 final – 2016/0208 (COD)], available on: https://data.consilium.europa.eu/doc/document/ST-13666-2016-INIT/en/pdf. Accessed May 5, 2022.
25. CryptoMag. Bitbay Crypto Exchange Full Review & Step by Step Guide, available on: https://cryptomag.me/bitbay-review/. Accessed on March 21, 2022.
26. Cryptomathic. Authors: Sharma G. April 2018. Digital Identity and eIDAS in Banking, available on: https://www.cryptomathic.com/news-events/blog/digital-identity-and-eidas-in-banking. Accessed May 8, 2022.
27. Cryptomathic. Authors: Sharma G. April 2018. Digital Identity and eIDAS in Banking, available on: https://www.cryptomathic.com/news-events/blog/digital-identity-and-eidas-in-banking. Accessed May 8, 2022.
28. Cryptonews. Crypto regulatory Environment in Lithuania, available on: https://cryptonews.com/news/crypto-regulatory-environment-lithuania.htm. Accessed May 12, 2022.
29. Cryptopedia. Anonymity vs. Pseudonymity In Crypto, available on: https://www.gemini.com/cryptopedia/anonymity-vs-pseudonymity-basic-differences. Accessed on April 20, 2022.
30. CSGForte. Electronic Payments: A Brief History, available on: https://www.forte.net/electronic-payments-a-brief-history/. Accessed March 4th, 2022.
31. Datinsky P. "European Legal Regulation of Cryptocurrencies through the AML Scope", Public Governance, Administration and Finance Law Review Vol. 5. No. 1. (2020): p.41. Available on: Academic Search Complete Hein Online. Accessed February 10, 2022.
32. DE VIDO, Sara. "All that Glitters is not Gold: The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive." DPCE Online, [S.l.], v. 38, n. 1, apr. 2019. http://www.dpceonline.it/index.php/dpceonline/article/view/643.
33. DeltaNet International. 5 Basic Money Laundering Offences, available on: https://www.delta-net.com/compliance/anti-money-laundering/faqs/5-basic-money-laundering-offences. Accessed January 1, 2022.

34. Deltec. Author: Outten S. Bitcoin Transaction Validation, What Exactly Goes on Under the Hood? Available on: https://www.deltecbank.com/2021/10/05/bitcoin-transaction-validation-what-exactly-goes-on-under-the-hood/?locale=en. Accessed May 6, 2022.

35. Deltec. Author: Outten S. Bitcoin Transaction Validation, What Exactly Goes on Under the Hood? Available on: https://www.deltecbank.com/2021/10/05/bitcoin-transaction-validation-what-exactly-goes-on-under-the-hood/?locale=en. Accessed May 6, 2022.

36. Department of Justice. Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency. Available on: https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency. Accessed May 8, 2022.

37. Ed. by Philipp Hacker, Ioannis Lianos, Gergios Dimitropoulos, and Stefan Eich 2019. Regulating Blockchain, Techno-Social and Legal Challenges. Available on: Academic Search Complete OXFORD University Press, p.3.

38. EffectiveAML. PhD, LLB (Hons), BCom (Econ). Ron, available on: https://www.effectiveaml.org/ron/. Accessed May 3, 2022.

39. ESMA. Warning. ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies. Available on: https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf. Accessed May 5, 2022.

40. EUR-Lex. Proposal for DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM/2021/423 final. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0423. Accessed April 20, 2022.

41. EUR-Lex. Proposal for DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM/2021/423 final. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0423. Accessed April 20, 2022.

42. European Central Bank. Virtual Currency Schemes, October 2012. p. 23. Available on: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Accessed May 11, 2022.

43. European Central Bank. Virtual Currency Schemes, October 2012. p. 23. Available on:https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Accessed April 1, 2022.

44. European Commission. Commission Staff Working Document. Impact Assessment. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=GA. Accessed May 11, 2022.

45. European Commission. Keynote speech by Commissioner McGuiness at the 5th Annual Conference on FinTech and Regulation: New Challenges and New Solutions. Available on: https://ec.europa.eu/commission/commissioners/2019-2024/mcguinness/announcements/keynote-speech-commissioner-mcguinness-5th-annual-conference-fintech-and-regulation-new-challenges_en. Accessed May 11, 2022.

46. European Commission. Statement By First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourova on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive. Available on:

https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3429. Accessed May 11, 2022.

47. European Parliament. Crypto Assets: new rules to stop illicit flows in the EU. Available on: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-tt-flows-in-the-eu. Accessed May 9, 2022.
48. European Parliament. Initial Appraisal of the European Commission Impact Assessment. Anti-money-laundering package. Available on: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/699467/EPRS_BRI(2021)699467_EN.pdf. Accessed May 2, 2022.
49. Evaluation Report," p.101.December 2018. Available on: https://rm.coe.int/09000016809247ed. Accessed May 2, 2022.
50. FATF Report. Virtual Currencies, Key Definitions and Potential AML/CFT Risks (June 2014), p.4. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Accessed March 25, 2022.
51. FATF. Designated categories of offences. Available at https://www.fatf-gafi.org/glossary/d-i/. Accessed on May 11, 2022.
52. FATF. AML/CTF Measures and Financial Inclusion. 2014. p.18. Available on: https://www.fatfgafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf. Accessed on May 8, 2022.
53. FATF. AML/CTF Measures and Financial Inclusion. 2014. pp.19-20. Available on: https://www.fatfgafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf. Accessed on May 8, 2022.
54. FATF. Guidance for a Risk-based Approach Virtual Currencies. p. 31. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Accessed April 17, 2022.
55. FATF. Guidance for a risk-based approach, Supervisors. p.25. Available on: https://www.fatf-gafi.org/media/fatf/documents/Risk-Based-Approach-Supervisors.pdf. Accessed on May 12, 2022.
56. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Available on: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. Accessed May 13, 2022.
57. FATF. Opportunities and Challenges of New Technologies for AML/CFT. p.42. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf. Accessed April 7, 2022.
58. FATF. Public consultation of FATF's Recommendation 1 and its Interpretive Note. Available on: https://www.fatf-gafi.org/publications/financingofproliferation/documents/consultation-recommendation-1.html. Accessed May 8, 2022.
59. FATF. Report to the G20 Finance Ministers and Central Bank Governors. p.2. July 2018, available on: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.
60. FATF. Report to the G20 Finance Ministers and Central Bank Governors. p.2. July 2018, available on: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.

61. FATF. What is money laundering? Available on: https://www.fatf-gafi.org/faq/moneylaundering/. Accessed January 1, 2022.
62. Financial Crime Investigation Service. Information for legal entities carrying out the activities of virtual currency exchange operators and (or) depository virtual currency wallet operators in the Republic of Lithuania. Available on: https://www.fntt.lt/en/money-laundering-prevention/information-for-legal-entities-carrying-out-the-activities-of-virtual-currency-exchange-operators-and-or-depository-virtual-currency-wallet-operators-in-the-republic-of-lithuania/4115. Accessed May 1, 2022.
63. Financial Crime Investigation Service. Legal Acts of the Republic of Lithuania. Available on: https://www.fntt.lt/en/money-laundering-prevention/legal-acts/legal-acts-of-the-republic-of-lithuania/347. accessed May 10, 2022.
64. Forbes Advisor. 10 Of The Best Cryptocurrencies in May 2022, available on: https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/. Accessed April 17, 2022.
65. Francis Bacon (1597).
66. Genesis Mining. Monero and Bitcoin: What's the Difference? Available on: https://www.genesis-mining.com/monero-vs-bitcoin. Accessed April 17, 2022.
67. Getid. AML and KYC for Crypto Exchanges & Wallets, The 2022 Guide, available on: https://getid.com/aml-kyc-crypto-exchanges-wallets/. April 13, 2022.
68. GLI. Blockchain & Cryptocurrency Laws and Regulations 2022 | 10 Cryptocurrency compliance and risks: A European KYC/AML perspective. Available on: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/10-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective#chaptercontent1. Accessed April 7, 2022.
69. Goodell G and Aste T (2019) "Can Cryptocurrencies Preserve Privacy and Comply With Regulations?", available on: Frontiers in Blockchain, pdf. p. 2., doi: 10.3389/fbloc.2019.00004. Accessed March 20, 2022.
70. Gosha R. Central Banking – Capitalism's Single Point of Failure, avaailable on: https://ryangosha.medium.com/central-banking-capitalisms-single-point-of-failure-e4804a4e0ae. Accessed April 18, 2022.
71. Gosha R. Central Banking – Capitalism's Single Point of Failure, avaailable on: https://ryangosha.medium.com/central-banking-capitalisms-single-point-of-failure-e4804a4e0ae. Accessed April
72. Gowa Nandan and Chakravort Chandrani, "Comparative study on cryptocurrency transaction and banking transaction," Global Transitions Proceedings Vol.2, Issue 2. (2021), p.531, accessed March 17, 2022, available on: https://doi.org/10.1016/j.gltp.2021.08.064.
73. ICO Guidelines. 2018. Available on: https://finmin.lrv.lt/uploads/finmin/documents/files/ICO%20Guidelines%20Lithuania.pdf. Accessed May 9, 2022.
74. IG. Cryptocurrency comparison, available on: https://www.ig.com/en/cryptocurrency-trading/cryptocurrency-comparison. Accessed April 17, 2022.
75. IMF Staff Discussion Note. Virtual Currencies and Beyond: Initial Considerations. p.27 Available on: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf. Accessed May 3, 2022.

76. ING. Regulation and the coming of age of Europe's crypto markets, available on: https://think.ing.com/articles/regulation-and-the-coming-of-age-of-europes-crypto-markets. Accessed May 14, 2022.
77. ING. Regulation and the coming of age of Europe's crypto markets, available on: https://think.ing.com/articles/regulation-and-the-coming-of-age-of-europes-crypto-markets#a8. Accessed May 12, 2022.
78. Investopedia. 10 Important Cryptocurrencies Other Than Bitcoin, available on: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/#citation-1. Accessed April 10, 2022.
79. Investopedia. Monero (XRM) Cryptocurrency, available on: https://www.investopedia.com/tech/introduction-monero-xmr/. Accessed April 17, 2022.
80. Investopedia. Monero (XRM) Cryptocurrency, available on: https://www.investopedia.com/tech/introduction-monero-xmr/. Accessed April 17, 2022.
81. Investopedia. What is a Cryptocurrency Payment Gateway? Available on: https://www.investopedia.com/tech/bitcoin-payment-services-introduction/. Accessed April 7, 2022.
82. Kanstrén T. (2021). "Maping Ring Signatures and Stealth addresses in Monero," available on: https://medium.com/coinmonks/mapping-ring-signatures-and-stealth-addresses-in-monero-a5543a434684. Accessed March 23, 2022.
83. Konstantin Robin. What is crypto-anarchism and how it evolved? (May 5, 2020). Available on: https://www.finextra.com/blogposting/18729/what-is-crypto-anarchism-and-how-it-evolved. Accessed March 25, 2022.
84. Lansky J. "Possible State Approaches to Cryptocurrencies", p.23. Available on: https://pdfs.semanticscholar.org/c14a/cbbb00b5baee7f10b24d224d429ee6b39e0e.pdf. Accessed May 8, 2022.
85. Lansky J. "Possible State Approaches to Cryptocurrencies", p.23. Available on: https://pdfs.semanticscholar.org/c14a/cbbb00b5baee7f10b24d224d429ee6b39e0e.pdf. Accessed May 8, 2022.
86. Lemen, Jen. "Hot Topic Highlight – Money Laundering Regulations Update." Available on: Property Elite, https://www.property-elite.co.uk/post/hot-topic-highlight-money-laundering-regulations-update. Accessed January 1, 2022.
87. Lexicology. "Cryptocurrency – Is it "property" and why does it matter?" Available on: https://www.lexology.com/library/detail.aspx?g=fa95822c-49ae-4701-9288-ed2b49d63d3b. Accessed May 10, 2022.
88. Lietuvos Bankas. Economics and Financial Stability Service established at the Bank of Lithuania. Available on: https://www.lb.lt/en/news/economics-and-financial-stability-service-established-at-the-bank-of-lithuania. Accessed May 13, 2022.
89. Lietuvos Bankas. V. Vasiliauskas: Clear 'rules of the game' needed for the boomig crypto sector. Available on: https://www.lb.lt/en/news/v-vasiliauskas-clear-rules-of-the-game-needed-for-the-booming-crypto-sector. Accessed April 20, 2022.
90. Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing. p.60. https://www.fntt.lt/data/public/uploads/2020/05/final-nra_eng_v3.pdf. Accessed May 5, 2022.
91. Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing. p.39. https://www.fntt.lt/data/public/uploads/2020/05/final-nra_eng_v3.pdf. Accessed May 5, 2022.

92. Lora Kolodny, Elon Musk says Tesla will stop accepting bitcoin for car purchases, citing environmental concerns (2021), available on: https://www.cnbc.com/2021/05/12/elon-musk-says-tesla-will-stop-accepting-bitcoin-for-car-purchases.html. Accessed March 31, 2022.

93. Martin Quest. Cryptocurrency Master Bundle; The Art of HOLDING; The Crypto Mining Mindset; The ICO Approac; Cryptocurrency 101; Blockchain Dynics. Source: https://www.pdfdrive.com/cryptocurrency-master-everything-you-need-to-know-about-cryptocurrency-and-bitcoin-trading-mining-investing-ethereum-icos-and-the-blockchain-e184666203.html., ch.4. Accessed on November 28, 2021.

94. Money. 7 of the Best Cryptocurrencies to Buy Now, available on: https://money.usnews.com/investing/cryptocurrency/slideshows/whats-the-best-cryptocurrency-to-buy?slide=3. Accessed April 17, 2022.

95. Moneywall. "Anti-money laundering and counter-terrorist financing measures Lithuania, 1st Enhanced Follow-up Report & Technical Compliance Re-Rating Round," p.6. June 2020. Available on: https://rm.coe.int/moneyval-2020-7-sr-5th-round-fur-mer-lithuania/16809ef774. Accessed May 3, 2022.

96. Moneywall. "Anti-money laundering and counter-terrorist financing measures Lithuania, 2st Enhanced Follow-up Report & Technical Compliance Re-Rating Round," p.101. June 2020. Available on: https://www.fatf-gafi.org/media/fatf/documents/reports/fur/MONEYVAL-FUR-Lithuania-Nov-2021.pdf. Accessed May 3, 2022.

97. Nathan Reiff. What are Centralized Cryptocurrency Exchanges? Available on: https://www.investopedia.com/tech/what-are-centralized-cryptocurrency-exchanges/. Accessed March 10, 2022.

98. News, European Parliament. Cryptocurrencies in the EU: new rules to boost benefits and curb threats. Available on: https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats. Accessed May 11, 2022.

99. Niels Vandezande, Virtual Currencies: A Legal Framework (CiTiP, KU Leuven, Cambridge – Antwerp – Portland: Intersentia Ltd, 2018), p. 304.

100. Noether S., Mackenzie A., The Monero Research Lab. "Ring Confidential Transactions." Available on: https://www.researchgate.net/publication/311865049_Ring_Confidential_Transactions. Accessed May 1, 2022.

101. Northeastern University, What is Cryptocurrency? Available on: https://onlinebusiness.northeastern.edu/masters-in-finance-msf/knowledge/guide-to-the-rise-of-cryptocurrency-digital-currency-and-bitcoin/. Accessed April 17, 2022.

102. Northeastern University, What is Cryptocurrency? Available on: https://onlinebusiness.northeastern.edu/masters-in-finance-msf/knowledge/guide-to-the-rise-of-cryptocurrency-digital-currency-and-bitcoin/. Accessed April 17, 2022.

103. OECD. Lithuania: Review of the Financial System. p. 16. 2017. Available on: https://www.oecd.org/finance/Lithuania-financial-markets-2017.pdf. Accessed May 12, 2022.

104. Politico. Brussels split over who will be crypto watchdog, available on: https://www.politico.eu/article/brussels-split-over-who-will-be-crypto-watchdog/. Accessed May 12, 2022.

105. Reuters. U.S. seizes $2.3 mln in bitcoin pai to Colonial Pipeline hackers, available on: https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/. Accessed May 8, 2022.

106. Satoshi Nakamoto, (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available on: https://bitcoin.org/bitcoin.pdf. Accessed March 25, 2022.

107. Simplicable. What is a Hashcode? Available on: https://simplicable.com/new/hashcode. Accessed May 11, 2022.

108. Sorainen. Stricter regulation of the cryptocurrency sector is under consideration in Lithuania. Available on: https://www.sorainen.com/publications/stricter-regulation-of-the-cryptocurrency-sector-is-under-consideration-in-lithuania/. Accessed May 13, 2022.

109. St Paul's Chambers. "Stages of Money Laundering Explained." Available on: https://www.stpaulschambers.com/stages-of-money-laundering-explained/. Accessed February 1, 2022.

110. Statista. The 100 most traded cryptocurrencies in the law 24 hours as of April 2022, available on: https://www.statista.com/statistics/655511/leading-virtual-currencies-globally-by-purchase-volume/. Accessed April 17, 2022.

111. Statista. Transaction speed ranking of 66 crypto – including DeFi and metaverse – in 2022, available on: https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/. Accessed April 27, 2022.

112. Statista. Transaction speed ranking of 66 crypto – including DeFi and metaverse – in 2022, available on: https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/. Accessed April 27, 2022.

113. Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). "Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain." Journal of Management Information Systems, 36(1), 37–73. https://doi.org/10.1080/07421222.2018.1550550.

114. Susan V. Scott and Wanda J. Orlikowski. (September 2014). "Entanglements in Practice: Performing anonymity Through Social Media." MIS Quaterly, Vol.38, No.3, p.875. Available on: https://www.jstor.org/stable/26635004?seq=11. Accessed April 18, 2022.

115. The Guardian. Judge approves $650m settlement of privacy lawsuit against Facebook, available on: https://www.theguardian.com/technology/2021/feb/27/facebook-illinois-privacy-lawsuit-settlement. Accessed April 20, 2022.

116. ULAM LABS. Is Cryptocurrency Anonymous? The Myth of Anonymity Debunked, available on: https://www.ulam.io/blog/is-cryptocurrency-anonymous/. Accessed April 26, 2022.

117. United Nations. Money Laundering. Available on: https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed February 26, 2022.

118. World of Warcraft Gold, available on: https://www.g2g.com/categories/wow-gold?region_id=166fbf02-6d9a-45a0-9f74-ac3ba5a002b4. Accessed on March 15, 2022.

119. Zhang Fan, "The "Risk – Based" Principle of AML Management", (September 19, 2017), available on: https://www.acamstoday.org/the-risk-based-principle-of-aml-management/. Accessed February 3, 2022.