TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Jaanika Ansip

DECENTRALISED FINANCE EXCHANGE SERVICES THROUGH ESTONIAN AND EUROPEAN UNION LEGAL PERSPECTIVE

Master's thesis

Programme HAJM, specialisation Law and Technology

Supervisor: Aleksi Oskar Johannes Kajander

LL.M., MA

Tallinn 2023

I hereby declare that I compiled this thesis independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not been presented previously for grading.

The document's length is 17,638 words, from Introduction to end of Conclusion.

Jaanika Ansip

09.05.2023

TABLE OF CONTENTS

ABSTRACT

Decentralised finance exchange (DeFi) is a new technology that is similar to traditional finance, but is built on blockchain and does not use intermediaries like banks. The research problem addressed in the thesis is the challenge faced by fully decentralised finance services in complying with legal and regulatory requirements, given the absence of a central authority or an intermediary to facilitate compliance. The scope of the EU proposal for a Regulation on Markets in Crypto-Assets (MiCA) does not include fully decentralised financial services that operate without any form of central control or provision. Thus, the present study wants to provide an understanding of the regulatory challenges and opportunities faced by the DeFi industry in Estonia and the EU.

The paper presents three research inquiries that served as a framework for the analysis: the extent to which MiCA governs financial services related to decentralised exchange; the existing legal regulations governing decentralised exchange financial services in Estonia; and what needs to be done in areas with no regulations. The analysis showed that the hybrid exchange DeFi is covered by regulation to a significant extent, but does not cover complete decentralisation. Under the current legal framework in Estonia, there are no corresponding legislative criteria applicable to full DeFi. Consequently, when there are no regulations, setting minimum technical standards for setting up DeFi platforms can help protect consumers and make sure that AML and KYC rules are followed.

Keywords: MiCA, DeFi, DApps, DEX.

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
AMLD5	AML Directive 2018/843
CASPs	Crypto Asset Service Providers
CTF	Combating Terrorist Financing
DAO	Decentralised Autonomous Organisations
DApps	Decentralised Applications
DeFi	Decentralised Finance
DEX	Decentralised Exchange
DLT	Distributed Ledger Technology
FATF	Financial Action Task Force
FinTech	Financial Technology
FIU	Financial Intelligence Unit
FSA	Financial Supervision Authority
ICO	Initial Coin Offerings
KYC	Know Your Customer
MiCA	Regulation on Markets in Crypto-Assets
MLTFPA	Estonian Money Laundering and Terrorist Financing Prevention Act
NCA	National Competent Authority
PIEIA	Estonian Payment Institutions and E-money Institutions Act
SEC	United States Securities and Exchange Commission
SMA	Estonian Securities Market Act
STO	Security Token Offerings
VASPs	Virtual Asset Service Providers

INTRODUCTION

The world of cryptocurrencies has experienced explosive growth, becoming a huge industry that has also had an impact on global finance. The emergence of Bitcoin in 2009 was a significant event as it was the first cryptocurrency to operate without a centralised governing body and lacking government support.[1] The financial sector experiences noteworthy influences from novel technologies, with blockchain technology increasingly revolutionising the way money is exchanged and stored as an alternative to traditional financial services. The European Commission acknowledges the financial sector as the foremost consumer of digital technology, which contributes significantly to digitization of the economy and society.[2]

In the ever-evolving crypto space, one of the prevailing developments is the emergence of decentralised finance (DeFi). This decentralised blockchain-based service serves as an alternative to traditional centralised finance, providing similar services.[3] DeFi exchange facilitates direct cryptocurrency and other crypto-asset exchange between individuals, eliminating the need for intermediaries such as banks.[4] The protocol leverages smart contracts, mostly based on Ethereum, to create and execute financial transactions, with the terms of agreement between buyer and seller directly coded into the system.[5] By 2021, the number of users utilising DeFi protocols had steadily increased, with approximately three million unique addresses recorded.[6] Furthermore, by 2023, the total value of cryptocurrency and assets locked in DeFi protocols exceeded fifty billion US dollars.[7]

This remarkable growth can be attributed to increasing acceptance and evolution of DeFi protocols and applications, including decentralised exchanges (DEX). Professional and

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Satoshi Nakamoto Institute*, Bitcoin.Org, 1–9. https://bitcoin.org/bitcoin.pdf.
[2] COM(2018) 109 final. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the regions. FinTech Action plan: For a more competitive and innovative European financial sector, p 2.
[3] Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance. *ArXiv.org*, p 1.
[4] Jensen, J., Von Wachter, V., & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). Complex Systems Informatics and Modeling Quarterly, (26), 46-54, p 48.
[5] Kim, H., Kim, H., & Park, Y. (2022). Perpetual Contract NFT as Collateral for DeFi Composability. IEEE Access, 10, 126802-126814, p 126802.
[6] OECD (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications, OECD Paris, p 26.
[7] The value is determined by using Coinmarketcap. *Top DeFi Tokens by Market Capitalization. CoinMarketCap*. https://coinmarketcap.com/view/defi/.

institutional investors from several European countries, such as the Netherlands and France, have contributed to the growth of DeFi, making Central North-Western Europe the world's largest cryptocurrency market.[8] Despite the Financial Action Task Force (FATF)[9] informing us that it is difficult to determine the precise impact of DeFi growth on illicit financing, open source information indicates that a risk of criminal misuse persists.[10]

The European Commission unveiled a Digital Finance Strategy package[11] in 2020, which included a digital finance strategy and legislative proposals pertaining to crypto-assets.[12] One of the proposals propagated is the Regulation on Markets in Crypto-Assets (MiCA), which aims to establish a consistent regulatory framework for crypto-assets and related service providers throughout the European Union.[13] The scope of MiCA encompasses services pertaining to crypto-assets, including those that are partially decentralised, while fully decentralised services are excluded according to recital 12a. Thus, DeFi services that are only partially decentralised may be subject to regulatory oversight, regardless of whether they are offered or managed by individuals or entities. Nevertheless, MiCA's scope does not encompass completely decentralised finance services that operate without any form of control or provisions from a central entity. Another proposal concerns distributed ledger technology (DLT).[14] It intends to establish a system through which market infrastructures can obtain exemptions from financial regulations in order to use DLT for trading and settling securities transactions, according to recital 3.

In October 2022, the European Union recognised the importance of evaluating DeFi in materials it published pertaining to this topic.[15] At present, a precise definition or explanation pertaining to

---

[8] Roukny, T. (2022). *Decentralized finance: information frictions and public policies: approaching the regulation and supervision of decentralized finance.* Luxembourg: Publications Office of the European Union. http://doi.org/10.2874/444494.

[9] *Who we are*. Financial Action Task Force (FATF) . https://www.fatf-gafi.org/en/the-fatf/who-we-are.html.

[10] FATF (2022), *Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs,* FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.

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

[12] *Digital finance: agreement reached on European crypto-assets regulation (MiCA).* (2022, June 30). [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/.

[13] *Ibid*.

[14] COM(2020) 594 final. Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology.

[15] Roukny, T. (2022), *supra nota* 8.

the differentiation between partial and full DeFi is not available. However, partial or hybrid DeFi can be described as a financial system that combines elements from traditional and autonomous mechanisms, as it may have features such as centralised control, intermediaries and/or compliance obligations. Such as a company which has certain operations controlled by a centralised authority, whilst other operations are automatised and operate on a peer-to-peer network or blockchain. On the other hand, there is full DeFi that can be described as a financial system entirely based on blockchain without features of partial DeFi. Full DeFi has features such as peer-to-peer transactions, transparency of the transactions and open access, as they are available on the blockchain, no central authority and independent governance, which means that users are involved in the decision-making process, but decisions are made through a consensus mechanism.

Effective supervision and regulation of fully decentralised finance exchange services to ensure compliance with anti-money laundering (AML) and combating terrorist financing (CTF) poses significant challenges for regulators. The aforementioned task may involve creating innovative regulatory structures and technological solutions that are proficient in overseeing and controlling DeFi services in their entirety. Regulatory entities need to find an appropriate balance between promoting progress and expansion within the realm of crypto-assets and DeFi, while simultaneously guaranteeing protection for and stability of the financial system, through suitable AML protocols.

AML Directive 2018/843 (AMLD5) of the European Union imposes AML and Know Your Customer (KYC) obligations on Virtual Asset Service Providers (VASPs) prior to the implementation of the MiCA. Throughout past events, Estonia has made an effort to attract cryptocurrency companies to establish themselves within the country's borders. The reason for this can be ascribed to the issuance of operating licences, with 381 licences for provision of virtual currency services having been issued in Estonia up until 2021, which amounts to approximately 55% of all licences in the world.[16] Considering the swift expansion of the DeFi sector and prospective regulatory obstacles it will confront, it is logical to examine the Estonian regulatory structure, which continues to look comparatively favourably on blockchain and

[16] Estonian Financial Intelligence Unit (2022). *Rahapesu Andmebüroo väliskoostöö ülevaade 2021*. https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#rahapesu-andmeburoo-

cryptocurrency affiliated enterprises. Examining the regulatory framework can help guarantee that DeFi exchange services function in compliance with legal requirements and furnish a secure and coherent environment for users and investors.

The study on hand identifies a research problem pertaining to the absence of a central authority or intermediary in fully decentralised finance services, which poses challenges in complying with legal and regulatory requirements. The absence of a third-party entity to assume accountability for non-compliance presents a significant obstacle. The objective of this paper is to analyse the MiCA proposal and existing legislation in Estonia regarding the relationship between decentralised finance systems and due diligence laws, including anti-money laundering laws. The objective of this study is to evaluate the adequacy of the legal framework in Estonia and the EU with regards to DeFi and identify any changes required to the legal framework in order to improve its effective implementation. The research paper will focus on the analysis of the exchange DeFi service, as it represents a significant component of the DeFi ecosystem.

The increasing adoption of DeFi services around the world has prompted inquiries regarding the regulatory framework in Europe that oversees this developing industry. This research delves into the legal framework governing DeFi in Estonia and evaluates the applicability of the recently introduced MiCA regulation to this novel technology. This paper presents three research questions that will serve as a framework for the analysis.

1. To what extent does MiCA govern financial services related to decentralised exchange?
2. What are the existing legal regulations governing decentralised exchange financial services in Estonia?
3. What must be done in areas with no regulations, whether any additional or stronger regulations are required in the DeFi technology?

The objective of this paper is to offer significant insights into regulatory obstacles and prospects encountered by the DeFi industry in Estonia and the EU by answering the questions provided. The research paper presented here is of considerable academic value, as it presents a thorough examination of the regulatory framework governing the DeFi industry. Additionally, it

scrutinises the applicability of the MiCA regulation recently introduced for this burgeoning and developing sector. The study delves into the difficulties that emerge in regulating decentralised services such as DeFi. It offers significant insights into how MiCA tackles these challenges, its association with partially decentralised services, and the due diligence obligations it imposes. The analysis on hand aims to provide policymakers and regulators with insights into regulatory obstacles that arise in connection with decentralised services, and to suggest optimal approaches for tackling them.

The approach selected for investigating the research question in the thesis will be qualitative, with the objective of presenting a comprehensive depiction and explanation of the DeFi phenomenon. The proposed legal research methodology entails an examination of the MiCA and Estonian laws pertaining to DeFi. The study will involve a comprehensive review and analysis of relevant literature to gain insights into DeFi technology, its historical context, the current regulatory landscape, and associated obstacles. This study will primarily examine the existing legislation on MiCA and its correlation with decentralised finance exchange services, alongside the legal framework in Estonia and academic publications.

The research paper is organised into four distinct chapters. The first chapter provides an overview of the historical context and difficulties associated with the subject matter. The second chapter focuses on an examination of MiCA legislation pertaining to DeFi, while the third chapter examines the state of DeFi in Estonia. The final chapter explores the topic of complete financial decentralisation and its potential future implications.

1. DEFI THEORETICAL PART

This chapter investigates developments that led to the emergence of DeFi services and provides an overview of the risks and legal challenges that are associated with these services. Innovation and disruption in financial technology are not merely a recent occurrence; they have existed for centuries.[17] The revolutionary type of financial system, characterised by decentralisation, developed with the advent of blockchain technology and the release of the Bitcoin White Paper[18] in 2008.[19] Blockchain architecture and technology enables the secure and transparent storage and transmission of data.[20] This technology operates without a centralised storage system or controlling authority using crypto assets and algorithmic techniques.[21] Because a blockchain is a type of decentralised ledger with the additional capability of cryptographically connecting information into distinct "blocks" that comprise a sequential, immutable chain, the concept of a blockchain is frequently perceived as a classification or subdivision of Distributed Ledger Technology (DLT).[22]

DeFi has evolved as a result of Web 3.0, the most recent version of the Internet that employs blockchain technology, decentralisation, and a token-based economy, specifically through use of permissionless public blockchains such as Bitcoin and Ethereum.[23] The DeFi movement may be traced back to 2014, when Vitalik Buterin developed Ethereum, a smart contract framework that allows structuring of decentralised applications (dApps).[24] Ethereum currently has the second-largest market capitalisation among crypto assets, valued at around $207 billion.[25] DeFi is a collection of financial apps built on blockchain networks, with the goal of creating a

[17] Kiviat, T. (2015). Beyond bitcoin: issues in regulating blockchain transactions. Duke Law Journal, 65(3), 569-608, p 581.
[18] Nakamoto (2008), *supra nota* 1.
[19] Harvey, C., Ramachandran, A., Santoro, J., Ehrsam, F., & Buterin, V. (2021). *DeFi and the Future of Finance*. Newark: John Wiley & Sons, Incorporated.
[20] Pavlidis, G. (2021). Europe in the digital age: Regulating digital finance without suffocating innovation. Law, Innovation and Technology, 13(2), 464-477, p 465.
[21] *Ibid*, p 465.
[22] Motsi-Omoijiade, I.D. (2022). Cryptocurrency Regulation: A Reflexive Law Approach (1st ed.). Routledge. https://doi.org/10.4324/9781003254164, p 4.
[23] Trotz, E. (2022). Million dollar bash: a nuanced approach for calculating tax liability for participants in decentralized finance. Texas Tech Law Review, 54(3), 575-593, p 576.
[24] Harvey *et al.* (2021), *supra nota* 19.
[25] *Ethereum price today, ETH to USD live, marketcap and chart.* CoinMarketCap. https://coinmarketcap.com/currencies/ethereum/.

financial system that is transparent, open source, and permissionless, and that operates without the intervention of a central authority.[26]

1.1 DeFi pillars

DeFi is considered as a progressive phase that goes beyond financial technology (FinTech). It involves not only the development of financial services in the form of software but also the reconstruction of the entire financial ecosystem through implementation of innovative techniques.[27] Automation and blockchain technologies are significant factors in shaping the production, distribution, and utilisation of financial services.[28] DeFi can be classified as comprising of four fundamental technologies, namely artificial intelligence, cloud computing, data analytics, and blockchain technology, which includes distributed ledgers and smart contracts.[29] Unlike traditional financial systems, DeFi protocols are maintained by a group of anonymous agents as opposed to a single legal entity.[30] Universal access, transparent and deterministic rules, non-custodial services, and interoperable and composable protocols distinguish DeFi from traditional finance.[31] The primary distinction between centralised finance and DeFi is found in three key areas: who controls the assets, the level of transparency and accountability, and the level of protection of privacy provided to the end user.[32]

The primary component of DeFi is blockchain technology. Due to its ability to enable verifiable, monitored, and enforceable exchanges of value over a computer network without the need for a trusted third party or central institution, blockchain technology can be described as a "trustless" mechanism.[33] Each block contains a hash, the hash of the previous block, and a timestamp, which ensures the order of events and promotes transparency.[34] Implementing multiple nodes

[26] Salami, I. (2021). Challenges and approaches to regulating decentralized finance. AJIL Unbound, 115, 425-429, p 1.
[27] Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: New challenges for compliance. *Journal of Financial Crime, 30*(1), 97-113.
[28] Schueffel, P. (2021). DeFi: Decentralized Finance - An Introduction and Overview. Journal of Innovation Management, 9(3), I-XI, p 11.
[29] Zetzsche, D., Arner, D., & Buckley, R. (2020). Decentralized finance. *Journal of Financial Regulation, 6*(2), 172-203. https://doi.org/10.1093/jfr/fjaa010.
[30] Roukny, T. (2022), *supra nota* 8.
[31] *Ibid*.
[32] Qin *et al.* (2021), *supra nota* 3, p 13.
[33] Kiviat (2015), *supra nota* 17, p 574.
[34] Sai, B., Nikhil, R., Prasad, S., & Naik, N. (2023). A decentralised KYC based approach for microfinance using blockchain technology. Cyber Security and Applications, 1, 100009, p 2.

serves to preserve data integrity and provide redundancy.[35] In response to the addition of blocks, each node updates its respective chain.[36] Consensus protocols decide which blocks can be added to the chain and become "truth".[37] Once the transaction has been validated by a consensus protocols system, it is recorded in the immutable public ledger.[38]

Two distinct classifications of blockchain networks exist, namely permissioned and permissionless. Permissionless blockchains are inclusive and accessible to all users, whereas permissioned blockchains are exclusive and only accessible to authorised parties identified by a system administrator.[39] There is also a hybrid version - Consortium composite blockchains that present the potential for centralised control.[40] Integration of public and private blockchains creates a semi-decentralised network by distributing the majority of responsibilities among multiple entities.[41] The private segment of a consortium blockchain is managed by a recognised entity, while the public segment is accessible to all.[42]

The majority of decentralised financial services are affiliated with or constructed on the Ethereum blockchain,[43] which is considered permissionless. Ethereum functions as a decentralised blockchain network that is not under the ownership of any singular entity, but rather is supervised by the Ethereum Foundation, a non-profit organisation.[44] The Ethereum Foundation operates as a non-traditional non-profit entity and does not adhere to a typical corporate structure.[45] The Foundation's primary objective is not to oversee or manage the Ethereum platform.[46] DeFi services can be combined and programmed in numerous ways. DeFi's primary financial services are stablecoins, decentralised exchanges, loans and credit, derivatives

[35] *Ibid*, p 2.
[36] *Ibid*, p 2.
[37] Harvey *et al.* (2021), *supra nota* 19, p 13.
[38] Kiviat (2015), *supra nota* 17, p 578.
[39] Jensen, J., Von Wachter, V., & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). Complex Systems Informatics and Modeling Quarterly, (26), 46-54, p 47.
[40] *Ibid* p 12.
[41] *Ibid*, p 12.
[42] *Ibid* , p 12.
[43] OECD (2022), *supra nota* 6, p 9.
[44] *Ethereum Foundation.* Ethereum.org. https://ethereum.org/en/foundation/.
[45] *Ibid.*
[46] *Ibid.*

and insurance, and portfolio management.[47] Yield farming utilises smart contracts to maximise returns from pledging crypto assets.[48]

The second component of DeFi is crypto assets. The term crypto asset refers to a cryptographically secured and transferable token.[49] A public key representing the address to receive tokens and a private key used to spend them are utilised by cryptography to secure cryptocurrency accounts.[50] Despite the fact that crypto assets represent value, their construction and structure is not uniform, as they may have their own blockchain like Bitcoin, be built on other blockchains, or be utilised on different blockchains, each with their own unique purpose and value.[51] The leading cryptocurrency Bitcoin has gained global recognition and is now transacted on major exchanges.[52] Anyone can obtain the crypto asset software and create an account to transfer digital currency to other accounts, allowing for limitless global transactions.[53] Due to the decentralised nature of crypto assets, they are not subject to the same rules and regulations as traditional currencies.[54] In contrast, they form a new and distinct asset class that requires its own regulatory framework to ensure proper use and management.[55]

In addition to Bitcoin, it is important to recognise the significance of stablecoins as a type of digital currency. Stablecoins are a distinct classification of digital assets that are designed with the specific purpose of maintaining a stable market value.[56] Cryptocurrencies, exemplified by Bitcoin, have been recognised for their notable instability, leading to implementation of stabilising mechanisms.[57] Stablecoins play a crucial role in facilitating and sustaining diverse financial operations, including exchange, lending, and borrowing, within the decentralised finance framework.[58] Certain stablecoins, including USDT and USDC, have integrated a

[47] Roukny, T. (2022), *supra nota* 8.
[48] Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi) (National Bureau of Economic Research Working Papers No. 30006). https://doi.org/10.3386/w30006.
[49] Harvey *et al.* (2021), *supra nota* 19, p 14.
[50] *Ibid*.
[51]Ojog, S. (2021). The Emerging World of Decentralized Finance. Informatica Economica, 25(4/2021), 43-52, p 43.
[52] Cumming, D., Johan, S., & Pant, A. (2019). Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty. Journal of Risk and Financial Management, 12(3), 126, p 3.
[53] Teomete Yalabik, F., & Yalabik, I. (2019). Anonymous Bitcoin v enforcement law. International Review of Law, Computers & Technology, 33(1), 34-52, p 37.
[54] *Ibid*, p 37.
[55] Cumming et al (2019), *supra nota* 52, p 5.
[56] Salami, (2021), *supra nota* 26, p 425.
[57] *Ibid*, p 425.
[58] Trotz (2022), *supra nota* 23, p 582.

blacklist mechanism in order to adhere to regulatory mandates,[59] which means that blacklist mechanisms have a feature to block or freeze certain accounts or transactions to comply with regulatory requirements or mitigate the risks. This action has the potential to negatively impact the decentralised finance ecosystem.[60]

Smart contracts are the third fundamental component of DeFi. Blockchains enable the creation of smart contracts that extend the capabilities of a basic payment network, such as Bitcoin.[61] A smart contract is a piece of code that can generate and modify any data or token type supported by the blockchain.[62] Given that DeFi is a clear illustration of the "code is law" thesis, the law is a set of rules that are written and enforced using immutable code.[63] Prior to DeFi's widespread adoption, however, concerns regarding liability for incorrect input or compiler errors must be resolved.[64] Smart contracts are not legally binding contracts, despite their name.[65] They are primarily responsible for executing predefined business logic in order to complete specific tasks, processes, or transactions.[66] To attach the parties' execution to legally binding agreements, legal action is required.[67] Moreover, thanks to smart contracts, dApps are created, which are applications that resemble traditional software applications, with the key advantage of being permission-free and uncensorable.[68]

1.2 DeFi Exchange service

The three distinct categories of exchanges are centralised, decentralised, and partial or hybrid. The first category, centralised exchanges, exhibit no decentralisation at all. The second category, partial or hybrid DeFi, can be described as a financial system that combines elements from traditional and decentralised finance, as it may have features such as centralised control, intermediaries and compliance obligations. An example of this is a company which has certain operations controlled by a centralised authority, whilst other operations are automatised and

[59] Qin *et al.* (2021), *supra nota* 3, p 5.
[60] *Ibid*, p 6.
[61] Harvey *et al.* (2021), *supra nota* 19, p 14.
[62] *Ibid,* p 15.
[63] Frajtova Michalikova, K., Poliakova, A. (2021). Decentralized finance. *SHS Web of Conferences, 129*, 3008, p 7.
[64] *Ibid*, p 7.
[65] Sai *et al* (2023), *supra nota 34*, p 2-3.
[66] *Ibid*, p 2-3.
[67] *Ibid*, p 2-3.
[68] Harvey *et al.* (2021), *supra nota* 19, p 17.

operate on a peer-to-peer network or blockchain. Thirdly, full DeFi is a financial system that operates entirely on the blockchain and does not rely on any features of partial DeFi. Full DeFi exchanges have features such as peer-to-peer transactions, transparency of the transactions and open access, as they are available on the blockchain, with no central authority and decentralised governance. This means that users participate in the decision making process and the decision is made by a consensus mechanism. The term "fully decentralised" pertains to services that function without any central authority or provider, whereas "no intermediary" denotes a self-executing, self-providing, self-performing, and self-governing service.

Numerous applications that are supposedly decentralised in nature actually exhibit a hybrid composition of centralised (*off-chain*) and decentralised (*on-chain*) components, such as custody, listing, liquidity, and trade execution.[69] DEXs hold reserves (*liquidity pools*) against which users may trade at any time at market prices, and when smart contracts receive trade orders, they resolve transactions on the blockchain immediately, without waiting for a counterparty to accept the order.[70] Therefore, DEXs are platforms that apply the fundamental features of traditional stock exchanges within a self-governing ecosystem.[71] To ensure equitable conditions, these transactions replace centralised websites with protocols.[72] DEXs differ from traditional exchanges in that they lack a central custodian and have less stringent listing requirements, as assets must only meet formal requirements to be listed.[73] Typically, the term "exchange" leads people to believe that cryptocurrency exchanges match sell and buy orders in a manner similar to traditional stock exchanges.[74] Despite this, users of decentralised exchanges create an account and deposit funds, similar to how banking services are utilised.[75]

The DEX platform facilitates provision of various services. Swapping is the noncustodial and atomic exchange of one token for another in DeFi, meaning that clauses in a smart contract have

[69] Kim, J. (2021). Regulation of decentralized systems: a study of Uniswap. Harvard Journal of Law & Technology, 35(1), 335, p 339.
[70] *Ibid*, p 340.
[71] Stepanova, V., & Eriņš, I. (2021). Review of Decentralized Finance Applications and Their Total Value Locked. TEM Journal, 10(1), 327-333, p 329.
[72] *Ibid*.
[73] Qin *et al.* (2021), *supra nota* 3, p 6.
[74] Suga, Y., Shimaoka, M., Sato, M., & Nakajima, H. (2020). Securing Cryptocurrency Exchange: Building up Standard from Huge Failures. *Financial Cryptography and Data Security, 12063*, 254-270.
[75] *Ibid.*

the power to cancel a transaction and reverse all of its previous actions.[76] The exchange is called atomic, because funds are stored in a smart contract with withdrawal rights that can be exercised prior to completion of the swap, and if the swap fails, the funds are returned to the parties.[77] In addition, crypto assets can be stored in specialised digital wallets, commonly referred to as 'crypto asset wallets', through encryption mechanisms within 'exchanges'.[78]

Automated Market Makers (AMMs) constitute a fundamental function of DEX. These are smart contracts based on a blockchain that facilitate exchange between two assets. These contracts hold assets on both sides of an exchange pair and provide continuous buying and selling price quotes.[79] AMMs facilitate trade execution without requiring buyers and sellers to be present at the same time.[80] Individuals can engage in asset exchange through AMMs without needing a large number of counterparties. As is customary in traditional marketplaces, pricing is determined by a computer program, eliminating the need for human intervention in matching of orders.[81] Furthermore, the concept of a decentralised exchange pertains to execution of exchange operations, particularly arbitrage, which entails the utilisation of automated exchange techniques to profit from momentary market fluctuations. Arbitrage refers to the act of buying a financial instrument in one market and selling it at a higher price in another market.[82]

1.3 DeFi challenges and risks

DeFi presents ample opportunities for transparency and integrity; however, it also poses significant threats to the economy. Despite the potential benefits of DeFi, such as preventing market power abuse, fostering innovation, and enhancing financial accessibility, its pseudonymous nature, absence of formal leadership, and limited control over contracting processes may increase the likelihood of illicit activities, jeopardise customer safety, and

[76] Harvey *et al.* (2021), *supra nota* 19, p 30.
[77] *Ibid*, p 29-31.
[78] Cumming et al (2019), *supra nota* 52, p 7.
[79] Harvey *et al* (2021), *supra nota* 19, p 29-31.
[80] Jensen *et al* (2021), *supra nota* 39.
[81] Mohan, V. (2022). Automated market makers and decentralized exchanges: A DeFi primer. Financial Innovation (Heidelberg), 8(1), 1-48.
[82] Qin *et al.* (2021), *supra nota* 3, p 6.

generate new forms of financial instability.[83] The cryptocurrency market is known for being very volatile, and even surprising things like social media coverage can have a big effect on it.[84]

As with any novel market, the classification of DeFi presents regulatory challenges.[85] Due to its reliance on decentralisation, DeFi faces difficulties operating in a regulated environment, which can contribute to "the tragedy of the commons",[86] in which nobody has a direct stake in maintaining or improving the technology.[87] The uncertainty surrounding the categorisation of both the platform and its users as either providers or recipients of financial services poses a challenge in the application of current regulatory frameworks.[88]

There are two distinct types of risks associated with crypto assets: private-law risks that pertain to cryptocurrency consumers and public-law risks that affect society as a whole; private-law risks include the possibility of tax law violations, whereas public-law risks are associated with the use of cryptocurrencies for illegal purposes, such as the procurement of illegal goods and financing of terrorism.[89] The "cyber laundering" of criminal funds is a regular practise in finance industries.[90] Those who engage in this unlawful behaviour, which entails hiding money through digital transactions, usually adopt creative and different strategies to cover their tracks.[91] Moreover, as banking becomes increasingly digital and cryptocurrencies seek to become a part of the mainstream financial system, it is crucial for banks and regulators to collaborate as gatekeepers to prevent money laundering in the financial industry.[92]

---

[83] Roukny, T. (2022), *supra nota* 8.
[84] Wronka (2023), *supra nota* 27.
[85] *Ibid*.
[86] Hardin, G. (1968). The Tragedy of the Commons. Science (American Association for the Advancement of Science), 162(3859), 1243-1248.
[87] Zetzsche *et al* (2020), *supra nota* 29.
[88] Avgouleas, E. & Marjosola, H. (2022). *Digital Finance in Europe: Law, Regulation, and Governance*. Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110749472, p 6.
[89] Datinsky, P. (2020). European Legal Regulation of Cryptocurrencies through the AML Scope. *Public Governance, Administration and Finances Law Review,5*(1), 38-47.
[90] Nizovtsev, Y., Parfylo, O., Barabash, O., Kyrenko, S., & Smetanina, N. (2022). Mechanisms of money laundering obtained from cybercrime: The legal aspect. *Journal of Money Laundering Control, 25*(2), 297-305.
[91] *Ibid.*
[92] Yeoh, P. (2020). Banks' vulnerabilities to money laundering activities. *Journal of Money Laundering Control, 23*(1), 122-135.

The anonymity, ease of worldwide transfer, and low transaction fees associated with crypto assets make them attractive for use in unlawful financial transactions such as money laundering.[93] It is possible to launder money using cryptocurrencies in two ways: by purchasing tokens with cash obtained through unlawful means, or through token purchases used in illegal activity.[94] The laundering process typically comprises three distinct stages, namely placement, layering, and integration.[95] Placement denotes the initial step of introducing illicit funds into the financial system, while layering pertains to the act of concealing the origin of such funds.[96] Lastly, integration refers to the process of reintroducing the funds into the economy without disclosing their source.[97] Furthermore, tumblers and mixing services have the capacity to gather coins from various individuals into a singular transaction, thereby strengthening the difficulty of tracking financial movements within the crypto assets network.[98] Wallets are used to store the crypto asset keys required for purchase and exchange of cryptocurrencies, whereas tumbler services are used to conceal the origin of tokens.[99] Uncovering and accessing crypto assets pose noteworthy challenges for law enforcement. Nonetheless, it is possible to obtain access to owners of Bitcoin via pseudonyms and track their assets.[100]

An additional obstacle within the realm of DeFi pertains to technical concerns. A significant obstacle faced by blockchain protocols pertains to their insularity from extraneous information sources, thereby restricting the efficacy of smart contract services solely to their respective contracts and tokens. The aforementioned issue is commonly referred to as the oracle problem. Oracles are considered as data sources that facilitate communication of information beyond the network with minimal trust, particularly in the context of smart contract services.[101] The trustless quality of blockchain technology is ascribed to its immutability, transparency, and the ability to programme smart contracts. Establishing trust algorithmically requires users to rely on the

[93] Haffke, L., Fromberger, M., & Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation, 21*(2), 125-138, p 129.
[94] *Ibid*, p 129.
[95] Datinsky (2020), *supra nota* 89.
[96] *Ibid*.
[97] *Ibid.*
[98] Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity (Oxford), 5*(1), 1-11, p 10.
[99] Haffke *et al* (2020), *supra nota* 93.
[100] Teomete Yalabik *et al* (2019), *supra nota*, p 53.
[101] Harvey *et al.* (2021), *supra nota* 19, p 15-16.

accuracy of smart contract code, as well as socio-technical factors such as adherence to institutional norms and transparency.[102]

Blockchain technology is also associated with security concerns. Despite the significant potential of DeFi, its rapid growth has resulted in persistent infrastructure challenges, security breaches, and fraudulent activities.[103] The escalating volume of financial transactions has resulted in a scenario where even minor fluctuations in pricing or data protection can lead to significant monetary losses for purchasers.[104] The absence of trust in the state-space aspect of DeFi has garnered the interest of cybercriminals who may exploit the lack of verification and connection to real-world identities to partake in unlawful activities for their own benefit. The absence of traceability poses a challenge to law enforcement endeavours and potentially creates an avenue for cyber-attacks.[105] In the year 2020, a group of unauthorised individuals gained access to 15 distinct DeFi protocols and embezzled a sum exceeding $120 million. Regrettably, only a portion of the funds stolen were eventually retrieved.[106]

An important challenge in the context of decentralised autonomous organisations (DAOs) pertains to determination of the rules of operation, which are encoded in smart contracts and dictate the eligibility of individuals to execute specific actions or updates. DAOs frequently incorporate a governance token that confers voting rights to the holder, enabling them to participate in forthcoming decision-making processes.[107]

FATF Guidelines identify a number of risk factors that increase the likelihood of noncompliance with AML/CFT regulations, including the use of anonymity-enhancing features in technology and network architecture, unregistered and unlicensed crypto asset service providers, disintermediation of transactions, and peer-to-peer transactions.[108] The DeFi sector lacks knowledge of its customers, due to the non-obligatory nature of KYC protocols within the

[102] Kirimhan, D. (2023). Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. Journal of Business Research, 157, 113558, p 2-3.
[103] Frajtova Michalikova *et al* (2021), *supra nota* 63, p 6-7.
[104] Wronka (2023), *supra nota* 27.
[105] Kirimhan (2023), *supra nota* 102, p 1-2.
[106] Wronka (2023), *supra nota* 27.
[107] Harvey *et al.* (2021), *supra nota* 19, p 17.
[108] FATF (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

industry. In contrast, centralised exchanges possess a database of their customers and oversee their transactions, thereby enabling the governing body to identify any suspicious activity.[109] The majority of DeFi initiatives lack the same KYC/AML standards as centralised organisations. Because peer-to-peer transactions are anonymous, it is difficult for law enforcement to investigate or seize something from a specific location or group. Additionally, the fact that DeFi projects can affect individuals worldwide makes it more difficult to police AML globally.[110]

Traditional financial intermediaries serve as a shield to safeguard sensitive data, but they also grant access to information when it is required for the economy or society to function. If DeFi does not have intermediaries monitoring system entry, KYC and AML laws must be regulated at the transactional level.[111] The application of a KYC function at the protocol level is an actual tool, which is where the Concordium blockchain[112] is headed right now. In this instance, the software would not allow transactions to be added to the distributed ledger until it was certain that all parties involved in the virtual asset transaction had undergone a trusted KYC procedure.[113]

Machine learning algorithms possess the capability to identify potentially illicit conduct and enhance AML and CFT alerts.[114] However, their adherence to European fundamental rights and the General Data Protection Regulation necessitates careful evaluation, given the wide range of offences and the opaque nature of certain machine learning models.[115] In addition, compliance with established financial regulatory norms such as KYC, AML, and CFT represents an alternative.[116] The proposition entails establishing a reliable network of anchors that can authenticate user addresses, thereby enabling them to avail commodities and amenities across various ventures without necessitating any modifications to the KYC protocol.[117]

---

[109] Karasek-Wojciechowicz, I. (2021). Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. Journal of Cybersecurity (Oxford), 7(1), p 2.
[110] Wronka (2023), *supra nota* 27.
[111] Makarov *et al* (2022), *supra nota* 48.
[112] *Concordium*. Concordium. https://concordium.com/.
[113] Karasek-Wojciechowicz (2021), *supra nota* 109, p 15.
[114] Bertrand, A., Maxwell, W., & Vamparys, X. (2021). Do AI-based anti-money laundering (AML) systems violate European fundamental rights? *International Data Privacy Law, 11*(3), 276-293.
[115] *Ibid*.
[116] Wronka (2023), *supra nota* 27.
[117] *Ibid*.

The potential for significant disruptions, including the relocation of economic activities, changes to the employment structure, and digital disparities, exists with the digitalisation of finance, despite its potential benefits.[118] In order to address the adverse impacts of such disruption, it is essential to formulate comprehensive policies that do not impede technological advancements or the evolution of current financial market circumstances.[119] At present, privately issued digital currencies do not seem to interfere with or contest the money creation function of central banks.[120] However, the strategy of adopting a "wait and see" position towards regulating crypto-assets is no longer rational or justifiable, as cryptocurrencies are not directly linked to central banks or the traditional monetary system, and regulatory measures which can be implemented and enforced are needed. [121]

Adoption of novel AML/CFT policy instruments to combat criminal activity must always be evaluated in light of fundamental human rights.[122] Any interference by a state in software that operates in cyberspace, may compromise the rights and liberties of the individuals who use these ecosystems.[123] These rights and freedoms include for instance the right to property for virtual asset owners, the freedom to pursue a trade or profession for platform owners and operators, data privacy rights, etc.[124] Furthermore, the flexibility of blockchain technology requires a regulatory strategy intended to mitigate potential risks associated with its implementation.[125] While policymakers are encouraged to create regulations, they must do so with care to avoid unintended consequences.[126] Notably, the actions of individuals in the Bitcoin network and other peer-to-peer cryptocurrency networks are protected by several fundamental rights, including the right to property, the right to pursue a trade or profession, the right to freedom of association, the right to freedom of expression and information, and the right to data protection and private life.[127]

---

[118] Pavlidis (2021), *supra nota* 20, p 465.
[119] *Ibid*.
[120] *Ibid*.
[121] *Ibid*, p 466.
[122] Karasek-Wojciechowicz (2021), *supra nota* 109, p 19.
[123] *Ibid.*
[124] *Ibid.*
[125] Kiviat (2015), *supra nota* 17, p 607.
[126] *Ibid.*
[127] Rueckert, C. (2019). Cryptocurrencies and fundamental rights. *Journal of Cybersecurity (Oxford), 5*(1).

To sum up, this chapter investigated developments that led to the emergence of DeFi services and provides an overview of risks and legal challenges associated with these services. DeFi is a collection of financial apps built on blockchain networks, with the goal of creating a financial system that is transparent, open source, and permissionless, and that operates without the intervention of a central authority. It is a result of Web 3.0. DeFi is composed of four fundamental technologies: artificial intelligence, cloud computing, data analytics, and blockchain technology. DeFi is mostly based on Ethereum, which is a decentralised blockchain network that is supervised by the Ethereum Foundation, a non-profit organisation. DeFi is a progressive phase that extends beyond Fintech.

DeFi presents opportunities for transparency and integrity, but also poses risks to the economy due to its pseudonymous nature, lack of formal leadership, and limited control over contracting processes. It also faces regulatory challenges due to its reliance on decentralisation. There are two types of risks associated with crypto assets: private-law risks that pertain to cryptocurrency consumers and public-law risks that affect society as a whole. Banks and regulators must collaborate to prevent money laundering in the financial industry.

Cryptocurrencies are attractive for illegal financial transactions such as money laundering due to their anonymity, ease of worldwide transfer, and low transaction fees. However, they pose technical challenges due to their insularity from extraneous information sources. Blockchain technology is associated with security concerns, such as infrastructure challenges, security breaches, and fraudulent activities. KYC and AML laws must be regulated at the transactional level, and machine learning algorithms must be evaluated for compliance. It is essential to formulate policies that do not impede technological advancements or impede the evolution of current financial market circumstances, and must be evaluated in light of fundamental human rights.

2. REGULATORY FRAMEWORK FOR DEFI EXCHANGE SERVICES IN THE EUROPEAN UNION

Chapter two of this thesis will provide a comprehensive analysis of the Markets in Crypto Assets (MiCA) in relation to DeFi. This chapter provides an in-depth examination of the regulatory framework proposed by the European Commission, specifically examining its approach to addressing the distinctive challenges presented by DeFi. This chapter will examine the key elements of the MiCA legislation and their potential impact on the DeFi sector.

2.1 Legislative background

The first reference to virtual assets within the scope of the EU framework is documented in the fifth amendment of the EU's AML Directive 2018/843. The European Parliament and the Council of the European Union officially adopted Directive 2018/843 on 30 May 2018, as the preamble states. Combatting money laundering is deemed a matter of "common interest" within the legal framework of the EU.[128] However, regulations pertaining to AML and other measures taken by governments to prevent criminal activities have the potential to impede upon individual rights.[129] AMLD5 constituted a significant advancement in regulation of cryptocurrency; however it still lacked a comprehensive structure for tackling concerns such as the guarantee of transaction transparency and identification of individuals, due to technological barriers.[130]

The European Commission introduced a set of legislative propositions in July 2021[131], with the objective of reinforcing the AML/CFT regulations. This final package comprises three regulatory measures, namely the "single rulebook" regulation pertaining to customer due diligence, transparency of beneficial ownership, and utilisation of anonymous instruments such

[128] De Vido, S. (2015). Anti-Money Laundering Measures Versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice. *German Law Journal, 16*(5), 1271-1292, p 1291.
[129] Rueckert (2019), *supra nota* 127.
[130] Datinsky (2020), *supra nota* 89.
[131] *Anti-money laundering and countering the financing of terrorism legislative package*. (2021). https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.

as crypto-assets.[132] Secondly, the next and 6th AML Directive encompasses regulations on a national level pertaining to oversight of Financial Intelligence Units, supervision, and the ability of competent authorities to obtain trustworthy information, including but not limited to registers of beneficial ownership and assets located in Free Zones.[133] Thirdly, a regulation exists that establishes the European Anti-Money Laundering Authority with the purpose of overseeing and conducting inquiries into AML/CFT adherence.[134]

Therefore, prior to the implementation of MiCA, the AML Directives constituted the sole legal framework mandating virtual currency service providers to undertake measures aimed at preventing money laundering and financing of terrorists or terrorism. Thus, it was the only regulatory framework that obliged DeFi service providers to comply with laws.

In June 2019, the Libra Association (now known as Diem Association) released a white paper introducing the creation of Libra, a digital currency that caused a significant disruption in the central banking world.[135] The proposed currency aimed to provide a low-cost medium of exchange primarily for the unbanked population, but the potential impact of the project's more than three billion Facebook users raised concerns about monetary sovereignty and the reliability of the payment system.[136] Despite the advantages that Libra offered over other cryptocurrencies such as Bitcoin,[137] the EU responded to the policy debate triggered by Libra's proposal with a proposal from MiCA, a regulation that aimed to address the regulatory gap and promote a harmonised approach to crypto-assets across the EU Single Market.[138]

In 2020, the European Union implemented a digital finance package consisting of legislative proposals and a digital finance strategy. The package seeks to regulate financial services based

---

[132] *New EU measures against money laundering and terrorist financing*. (2023, March 28). [Press release]. https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing.
[133] *Ibid*.
[134] *New EU measures against money laundering and terrorist financing*. (2023, March 28), *supra nota* 132.
[135] Pupolizio, I. (2022). From Libra to Diem. The Pursuit of a Global Private Currency. *Global Jurist, 22*(2), 281-306.
[136] *Ibid*.
[137] Senarathne, C. (2019). Possible Impact of Facebook's Libra on Volatility of Bitcoin: Evidence from Initial Coin Offer Funding Data. Organizacijų Vadyba, 81(1), 87-100.
[138] Zetzsche, D., Annunziata, F., Arner, D., & Buckley, R. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal, 16*(2), 203-225.

on blockchain technology, including those related to crypto-assets, with the aim to facilitate passporting for innovative startups throughout the EU.[139] The package is centred on the elimination of fragmentation within the Digital Single Market, modification of the regulatory framework to enable digital innovation, advancement of data-driven finance, and resolution of difficulties and hazards associated with digital transformation.[140] However, the EU's aim to establish better protection for market participants and consumers through disruptive innovation may be viewed as a barrier by those who prioritise innovation over regulation.[141] MiCA's objective is to address a significant regulatory void and establish a consistent methodology for managing crypto-assets throughout the EU's unified market.[142] The aforementioned aim encompasses prerequisites for the issuance, public offering, and exchange of said assets, alongside oversight, administration, and functioning of the service providers and issuers implicated.[143] Furthermore, the aforementioned regulation aims to safeguard individuals who possess crypto-assets and patrons of these service providers, while simultaneously tackling concerns such as insider trading exchange, market distortion, and illicitly divulging confidential information.[144]

MiCA's recitals (12a) state that fully decentralised finance initiatives, which lack a centralised authority accountable for providing services, are outside the scope of regulation in the context of DeFi. The aforementioned circumstance may give rise to noteworthy regulatory obstacles and fundamental challenges for the decentralised finance sector in the EU.

2.2 Regulated Crypto-Assets and Services

The MiCA framework has established a standard definition for crypto-assets and has categorised them into three distinct groups. In Article 3 (1(2)), the term "crypto-asset" refers to a type of digital asset or entitlement that can be electronically transmitted and stored using distributed ledger technology or comparable methods. This classification employs the methodology of

[139] *Digital finance package*. (2020). https://finance.ec.europa.eu/publications/digital-finance-package_en.
[140] *Digital finance package* (2020), *supra nota* 139.
[141] Zaccaroni, G. (2022). Decentralized Finance and EU Law: The Regulation on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology. European Papers, 2022 7(2), 601-613.
[142] *Digital finance package* (2020), *supra nota* 139.
[143] *Digital finance: agreement reached on European crypto-assets regulation (MiCA)* (2022), *supra nota* 12.
[144] *Ibid.*

encompassing all potential crypto assets. The principal ensures that the regulation encompasses all categories of crypto-assets that have not been explicitly defined.

The regulation categorises stablecoins into two discrete classifications. The initial category according to Article 3 (1(3)), denoted as "asset-referenced tokens," represents a type of crypto asset that preserves a stable value through its reference to another value or entitlement, such as an official currency. The aforementioned tokens are not classified as electronic currency and have the capacity of denoting various authorised currencies. The second category is commonly referred to as "electronic money tokens" or "e-money tokens" according to Article 3 (1(4)). These tokens are designed to retain a consistent value by relying solely on a single official currency as a reference point. As per the recitals (26) paragraph 1 of MiCA, stablecoins are intended to uphold a consistent value, rendering their stabilisation mechanism irrelevant. Examples of stablecoins in the form of e-money tokens include USDT and USDC, while the asset-referenced tokens are represented by the aforementioned Libra coin.

According to Article 4 (1) outlining the established principles for organising a crypto-asset offering, the issuer must be a legitimate entity, produce a white paper, inform the regulatory body of this white paper, make the white paper available publicly, and where relevant, create and distribute promotional materials. According to Article 2 (3), the regulatory framework of MiCA does not encompass financial instruments that are subject to governance of MiFID, such as security tokens.

All of the aforementioned types can be located on DEX. The DEX platform provides an extensive selection of cryptocurrencies, encompassing e-money tokens, asset-referenced tokens, crypto-assets, and financial instruments.

The definition of "crypto-asset service provider" provided in Article 3 (1) point 8, which pertains to a lawful entity or any other establishment whose principal occupation involves providing one or more professional crypto-asset services to third parties. Such entities are authorised to offer these services under Article 53. As per the provisions of Article 2 (1), entities that are legally or naturally constituted, along with other business enterprises that participate in the issuance, public

offering, and admission to the exchange of crypto-assets, or provide services related to crypto-assets within the EU, are considered as obligated persons.

The term "crypto-asset services" as defined in Article 3 (1) point 9 encompasses a range of services and activities as outlined in MiCA. Each distinct service category has its own set of prerequisites, and licensing is granted exclusively for a particular type of operation. Providers authorised to provide cryptocurrency exchange services according to Article 3 (1) point 9(b-d), with services for receiving and transmitting orders on behalf of third parties are precluded from receiving any type of incentive, reduction, or non-monetary advantage, benefit, inducement or remuneration for directing customer orders to a specific crypto-asset exchange platform or service provider.

The delivery of said services according to Article 15 (1) necessitates acquiring authorisation from the appropriate governing bodies or this may be dispensed by pre-approved market participants, including but not limited to banks, investment firms, and electronic money institutions.

It is imperative that authorised service providers according to Article 3 (1) point 22 maintain a registered office within one of the European Union's Member States in which they offer their services pertaining to crypto-assets. In order to comply with regulatory requirements, the organisation’s management must engage in activities in the EU that meet the standards specified by governing bodies according to recitals (50) para 3. Additionally, it is mandated according to recitals (50) para 4 that at least one director of the organisation must maintain residency within the European Union.

The MiCA framework encompasses services pertaining to crypto-assets, albeit exclusively those that exhibit partial decentralisation, while fully decentralised services fall outside of its scope according to recitals (12a). Thus, DeFi services that are offered or managed by individuals or entities are subject to regulatory oversight. Nevertheless, the MiCA framework does not encompass completely decentralised finance according to recital (12a) services that operate without any form of control or provisions from a central entity.

Even though hybrid DEXs may use DLT technology for trading and concluding securities transactions, they are primarily governed by MiCA as CASPs and not the DLT pilot regime as DLT market infrastructures. Consequently, analysing the DLT pilot programme may not be explicitly related to the regulatory requirements and responsibilities applicable to hybrid DEXs under MiCA. However, it is important to observe that hybrid DEXs may still be required by MiCA to comply with certain DLT-related requirements.

2.3 Obligations for hybrid DeFi services

The objective of this subsection is to examine the suitability of MiCA regulations for decentralised finance services that function in a partially decentralised fashion. The objective of this investigation is to explicate the process of identifying individuals who utilise decentralised financial services within the regulatory framework of the MiCA, and to establish a clear definition of a service provider. Based on our present school of thought, DeFi services categorised under MiCA regulation should exhibit hybrid features.

MiCA's recitals (12a) outline three primary criteria that classify decentralised services as falling within the scope of the regulation. The scope of the subject matter encompasses the actions and provisions of both natural and legal entities, as well as undertakings. This includes activities that are performed, provided, or controlled either directly or indirectly, and extends to those that are only hybrid decentralised.

As mentioned before, partial or hybrid DeFi can be described as a financial system that combines elements from traditional and decentralised finance, as it may have features such as centralised control, intermediaries and compliance obligations. FuFully or completely decentralised services are described as being a financial system entirely based on blockchain technology without the features of partial DeFi. The term "fully decentralised" pertains to services that function without any central authority or provider, whereas "no intermediary" denotes a self-executing, self-providing, self-performing, and self-governing service.

The primary requirement of MiCA's recitals (12a) for compliance is that the provider of services must be categorised as either a natural person or a legal entity, or other enterprises that have been appropriately enrolled or registered with relevant regulatory bodies. As per MiCA regulations, specific services pertaining to crypto assets are categorised as "Crypto Asset Service Provider" (CASP). According to MiCA, the provision of CASPs is restricted to legal entities that possess a registered office within a European Union member state and which have obtained authorisation. Investment firms and credit institutions have the option of obtaining exemptions.

In order to offer CASPs, corporate entities are required to seek authorisation from the relevant regulatory body in the European Union member state where they are officially registered. When providing CASPs in additional European Union member nations, it is imperative to inform the corresponding regulatory body. CASPs are obligated to adhere to a range of regulatory mandates, including minimum capital requirements, prudential safeguards, organisational prerequisites, secure storage requirements for clients' crypto assets and funds, grievance resolution, transparency, outsourcing, and other comparable requirements as stipulated in the MiCA. In addition, MiCA stipulates distinct criteria for every category of crypto asset service.

Therefore, it is crucial for a DeFi service provider to hold a legitimate licence issued by a European Union member state. It is crucial that regulators acknowledge DeFi and ensure that they satisfy the necessary legal and operational requirements to provide their services in accordance with the current structure. Participants in DeFi include traders, investors, brokers, exchanges, liquidity providers, and other types of service providers. However, the primary service provider for DeFi must be licensed.

The second criterion of MiCA's recitals (12a) pertains to the execution, provision, and oversight of services associated with crypto assets. Within the realm of DeFi, the term "execution" pertains to implementation of financial transactions through utilisation of smart contracts and other decentralised protocols. Conversely, the term "provide" denotes the action of furnishing liquidity to decentralised protocols or safeguarding smart contracts. The term "control" can pertain to possession of influence over DeFi. Within the DeFi exchange realm, various aspects are taken into consideration such as transaction performance, liquidity provision, asset management, risk

control, security, and compliance. The efficient execution of transactions and provision of liquidity and other necessary resources are crucial aspects of crypto-asset services. The management of crypto-asset services entails the mitigation of risks relating to market fluctuations and security vulnerabilities, in addition to adherence to regulatory mandates and established industry norms.

It is important to note that in both partially decentralised and centralised exchange services, the provision, performance, and control are dependent upon the service providers. It is crucial to note that in a state of complete decentralisation, the execution of these functions is dependent on smart contracts. It is noteworthy that the creators of DeFi services are responsible for crafting the code utilised in smart contracts, yet they may not necessarily adhere to the specifications outlined for said smart contract. Similarly to the concept of control, DeFi developers do not retain ownership of their clients' funds, as the funds' value is secured within a smart contract on the blockchain.

In terms of the FATF, the concept of "control" encompasses the capacity to possess, transfer, furnish, or utilise virtual assets.[145] It is crucial to comprehend that DeFi is constructed upon smart contracts and decentralised applications, which do not meet the criteria of crypto asset service providers due to the inapplicability of prescribed standards to software or technology. The criteria pertain to individuals who possess substantial control over a distributed application, including but not limited to developers, proprietors, or administrators.[146] Establishing a level of control can be achieved through various means such as monitoring the management of assets within the protocol, maintaining business relationships with service users, and exercising the ability to set or modify parameters that govern the provision of services.[147] In the realm of DeFi, any level of external influence would classify the environment as a partial DeFi model. This is due to the fundamental characteristic of full DeFi, which entails a complete absence of external control.

---

[145] FATF (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html, *para* 73.
[146] FATF (2022), *supra nota* 10, para 33.
[147] FATF (2021), *supra nota* 145, para 67.

The third criterion of MiCA's recitals (12a) is to have hybrid decentralisation. Partially decentralised services and activities pertain to crypto-asset services or activities that rather occupy a position around halfway between decentralisation and centralisation, which means these services have features such as central control or authority, and/or intermediaries and other centralised elements, but also decentralisation features like direct asset exchange between peers.This hybrid decentralisation is exemplified in certain DEXs that may still rely on a central entity to facilitate transactions or provide liquidity.

Therefore, hybrid DEXs possess all three criteria of MiCA's recitals (12a), if they have licensed entities, which exert an influence on the platform, and also have features of decentralisation that are automatised and independent. These features could be transactions on blockchain, while compliance with KYC and AML are monitored by a legal entity.

2.3.1 Hybrid DeFi services classification

To determine which due diligence measures apply under MiCA, it is necessary to know which services are included in the DeFi category and how they are classified under the regulation. This understanding will provide clarity on the scope of DeFi services that are subject to MiCA.

Decentralised exchange services are a type of DeFi service that fall under Article 2(1) of MiCA. DEXs involve exchanging one crypto-asset for another or operating as an exchange platform for crypto-assets. Exchange for crypto-assets refers to setting the exchange rate for converting cryptocurrencies into fiat currencies or other cryptocurrencies. An exchange platform is the service provider that operates a multilateral system by running the exchange platform that matches buyers and sellers of cryptocurrencies. Article 2(2) of the MiCA regulatory framework outlines four distinct categories of services that are subject to regulation by MiCA. These services include the issuance of crypto-assets, public offers of crypto-assets, admission of crypto-assets for exchange, and provision of services relating to crypto-assets.

There is a possibility that the decentralised exchange services have incorporated the services offered by MiCA Article 3(1) point 9 to a certain extent. MiCA creates a list of services in accordance with its stated provisions. MiCA defines the operation of a trading platform for crypto-assets in Article 3(1) point 11, as the management of one or more multilateral systems that bring together or assist in bringing together buying and selling interests of multiple third parties for crypto-assets – within the system and in accordance with its rules – in a manner that leads to a contract, either by exchanging one crypto-asset for another or a crypto-asset for funds.

In the realm of DEXs, these conditions govern hybrid decentralised exchanges if they lead to a contract established by the system or its rules. Since smart contracts are used to automatically execute trades between buyers and sellers based on predefined rules and algorithms, they meet the criteria. These smart contracts facilitate exchange of crypto-assets between parties without the need for a centralised exchange or an intermediary.

DeFi services do not apply to provisions involving acting on behalf of a third party provided in Article 3(1) point 9 (a, e, fa, g). Although smart contracts and other DeFi protocol features may provide security, their primary function is not to serve as third party representative assets. The primary objective on the blockchain network is to enable decentralised financial transactions and user interactions. Smart contracts cannot be considered a third party.

Additionally, the other services mentioned in MiCA by Article 3(1) point 9 (f, h, hb) are irrelevant to DeFi. As stated in Article 3(1) point 9 (15), placement of crypto-assets services implies marketing; however, DeFi protocols typically do not engage in marketing activities. Providing advice on crypto-assets as stated in Article 3(1) point 9 (17), also includes personalised recommendations, that DeFi has not traditionally established for these actions. DeFi platforms provide users with tools and analytics to optimise their cryptocurrency portfolios. With the expansion of DeFi projects, it is possible that these services will soon be offered in DeFi as well.

2.3.2 Hybrid DeFi authorisation

The following explores the extent of regulatory measures and the potential approaches and standards for executing due diligence within hybrid decentralised financial systems. The regulatory framework imposes standards for crypto-asset issuance and offering, as well as service provider authorisation. The due diligence of the AML directive applies to decentralised services that fall under the MiCA framework, since it will be under the auspices of EU regulation.

According to MiCA regulations, issuers of crypto-assets intend to offer their tokens to the public in the EU or who seek admission to trading platforms are obligated to adhere to three fundamental requirements of Article 4 (1). The first prerequisite according to Article 4 (1) point a, and 54 (1) specifies that issuers must be officially registered as legal entities within a European Union member state.

The aforementioned requirement has the potential to affect DeFi trading, specifically for issuers or platforms outside of the European Union. In order to adhere to MiCA regulations, a non-European platform or issuer seeking to offer tokens to the public in the EU or gain access to EU-based trading platforms must register as a legal entity in a member state of the European Union. The aforementioned stipulation may result in enhanced regulatory compliance costs for issuers and platforms, and may possibly establish barriers to entry for non-European participants within the field of DeFi. Nonetheless, it has the potential to enhance transparency and accountability for both issuers and platforms, while also enhancing investor confidence in the larger crypto-asset market.

The second prerequisite according to Article 4 (1) point b is to draft and publish a white paper containing marketing-related product information. MiCA requires white papers that describe the issuing company and development team of a crypto-asset. The document must also specify the rights and responsibilities of crypto-assets, the reasons for the offering, the intended use of proceeds, and all risks associated with the issuer, product, and project implementation. Lastly, white papers should contain technical information regarding the technology and mechanisms that permit holding tokens, their storage and transfer, the number of crypto-assets to be issued, their

price, and subscription terms. To avoid legal liability, issuers must confirm all the mandatory information required.

Implementation of this requirement has the potential to enhance transparency and lucidity for investors and traders in the DeFi space. The evaluation of DeFi platforms can be improved by mandating issuers to disclose pertinent information regarding their projects, products, and associated risks, thereby enabling investors and traders to make more informed decisions. Requiring the inclusion of technical details pertaining to token holding, storage, and transfer in white papers may potentially enhance investor and trader security while simultaneously mitigating risk. The disclosure of technical information by issuers has the potential to enhance the level of trust within the DeFi ecosystem.

In addition, according to Article 4 (1) point c it is a requirement for providers of crypto assets to present white papers to their respective competent authorities before their intended release. In the event that the issuer intends to proceed with the offering, according to Article 19 (2) the National Competent Authority (NCA) may refuse to grant authorisation to provide the services.

The aforementioned requirement may also impede decentralised finance trading and the process of listing new tokens on exchanges, as it may require additional time and resources. NCAs will undertake a thorough examination of the issuer's white papers, which could potentially result in a postponement of the listing process. Additionally, this stipulation has the potential to increase the administrative workload, as NCAs may solicit supplementary information or documentation from issuers. However, this requirement enhances transparency and regulatory oversight within the DeFi ecosystem.

Apart from the three primary duties mentioned above, issuers are also accountable for treating purchasers with acts of honesty, and acting fairly and professionally in accordance with Article 13 (1) point a, as well as implementing managerial mechanisms to prevent any potential conflicts of interest in the same Article, point c. Additionally, they implement security systems and protocols to safeguard ownership of investor crypto assets in Article 13 (1) point b and d. These

conditions have the potential to enhance investor assurance in the DeFi ecosystem, by affording increased safeguards to buyers of cryptocurrency assets.

On the other hand, certain enhancements may necessitate discontinuing certain DeFi initiatives. The implementation of legal incorporation, which guarantees an issuer responsibility, may pose a challenge for European Union trading platforms in accepting crypto-assets from unidentified entities. The writing and distribution of white papers, aimed at enhancing transparency, leads to an increase in administrative costs and expenses for the entities responsible for issuing them. The adoption of MiCA will necessitate crypto projects to abandon some of their autonomy and flexibility as a means to reduce the growth of illicit activities assisted by such projects.

According to Article 122, the Commission must submit an intermediate report 24 months after the regulation enters into effect and a final report 48 months after consulting with the EBA and ESMA about how the regulation is being used. These papers must contain an analysis of how decentralised finance has changed in the crypto-assets markets and how decentralised crypto-asset systems are regulated. If necessary, the papers may also include suggestions for new laws. In addition, Article 122 (b) states that 18 months after the regulation enters into effect, the Commission must submit a report to the European Parliament and Council on the latest changes to crypto-assets. The report must cover things that were not covered in the regulation. If necessary, it should also include a legislative proposal. The study should discuss the most recent changes in the crypto-assets market. It should also include an assessment of the progress of decentralised finance and correct ways to regulate crypto-asset systems that do not have issuers or service providers. The report must also ascertain and deduce if and how decentralised money can be regulated.

The involvement of the NCA and the EBA is required because it can serve as a solution for the problem of fragmentation of supervision in cross-border cases, as certain e-money token instruments will bear significant risks affecting multiple member states.[148] Producers of the MiCA are aware of the concept of decentralised finance, but currently lack a clear strategy for addressing it. The significance of reports lies in their ability to assist policymakers to remain

[148] Pavlidis (2021), *supra nota* 20, p 473.

aware of the most recent developments in crypto-asset markets and determine whether any modifications to the regulatory structure are necessary to address emerging risks or facilitate innovation in the financial services sector and industry. The MiCA sets out an approach with caution and evaluation, in light of the aforementioned circumstances.

To sum up, this chapter provides a response to the first research question of to what extent MiCA governs financial services related to decentralised exchange. Through the analysis, the paper can constitute that MiCA regulates hybrid decentralised exchange finance services to a significant extent. The hybrid services are those which have combined multiple aspects, such as centralised control, intermediaries or/and compliance obligations. In contrast, complete decentralisation does not exhibit the same features as a hybrid service. MiCA's recital (12a) outlines three primary criteria for classifying hybrid decentralised services within its scope. Firstly, DeFi exchange services should have existing licences in the EU. Secondly, any level of external influence, which can provide, perform or control the services would classify the environment as a hybrid DeFi service, thus falling into the scope. Thirdly, hybrid services are those, in which services still depend on centralised control for instance to provide liquidity or facilitate transactions, and at the same time have autonomous and independent parts and constituents, which are based entirely on smart contracts.

From the MiCA services in Article 3 (1) point 9, hybrid services are covered and included entirely by Article 3 (1) point 9 (b-d), which are trading and exchange, even if hybrid services lead to a contract established by the system or its rules independently and autonomously. Smart contracts are used to automatically execute trades between buyers and sellers based on predefined rules and algorithms, therefore these services meet the criteria of definition stated in Article 3 (1) point 9 (b-d). In order to become a DeFi hybrid exchange, authorisation requirements set out in Article 15 must be complied with, and cover establishing a legal entity in the EU, drafting a white paper and notifying the relevant national authority. MiCA sets out an approach to act with caution and to evaluate decentralised services. A more precise and detailed view will be available in reports, which will be available at least 18 months after MiCA has entered into force.

3. ESTONIAN LEGAL PERSPECTIVE OF DEFI EXCHANGE SERVICES

Chapter three of this thesis will conduct a comprehensive analysis of the current status of DeFi in Estonia. Estonia has gained recognition as a key player in the realm of digital technology, specifically in the fields of financial technology and blockchain. The present chapter aims to examine Estonia's strategic positioning within the dynamic DeFi market, along with the various measures implemented to promote innovation and expansion within this sector.

3.1 Overview of the Estonian legal framework

Estonia has gained recognition for its competence in digital innovation, after implementing multiple initiatives that utilise technology to enhance governance and public services. As early as 2017, Estonia expressed interest in introducing a blockchain-based digital token, known as the "estcoin", designed for use exclusively within the country's e-residency programme.[149] Estonia has achieved a prominent position in global rankings by exhibiting leadership in the number of active FinTech companies per one million inhabitants. Countries with flexible regulations and high levels of digitalisation tend to exhibit a positive correlation with the generation of FinTech per capita. Estonia, in particular, has emerged as a leader in this regard.[150]

The period between 2018 and 2019 witnessed a substantial rise in the number of virtual currency service providers seeking an operating licence in Estonia.[151] This can be attributed to the fact that, between 2017 and 2019, more than 1,300 companies were issued operating licences in Estonia.[152] It should be noted, that Estonia was among the first European countries to enforce the obligation for an operating licence to provide virtual currency services.[153]

[149] McLellan, L. (2018). Estcoin and sovereign cryptocurrencies: Not the future yet. Global Capital, 2018.
[150] Finnovating (2023). FinTech Global Vision 2023. https://finnovating.com/fintech-global-vision-report/, p 11.
[151] Estonian Financial Intelligence Unit (22.09.2020). *Virtuaalvääringu teenuse pakkujate uuring*. Rahapesu andmebüroo. https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
[152] *Ibid.*
[153] *Ibid.*

By 2021, 381 licences for provision of virtual currency services had been issued in Estonia, which is approximately 55% of all licences in the world.[154] Between 2008 and 2021, about 642 million euros passed through the Estonian financial system, of which 27% passed through virtual currency service providers with an Estonian licence.[155] Allegedly, 160 million euros passed through Estonia in the course of laundering proceeds of fraud, 88% of which passed through virtual currency service providers with an Estonian licence to operate.[156]

Despite the positive economic growth, the number of virtual currency services companies registered in Estonia was very large. Consequently, concerns have been raised about the effectiveness of current anti-money laundering measures. As a result, the issuance of licences has been suspended temporarily, pending enactment of new legislation that would mandate businesses to submit additional documents, including detailed business models and procedures.

In May 2022, Estonia underwent evaluations by the Council of Europe's anti-money laundering body MONEYVAL. It assesses states' adherence to "recommendations" established by the FATF, which are recognised as international standards. It is acknowledged that implementation of novel legislation does not invariably eradicate unlawful conduct.[157] This resulted in a report published in December 2022, that encourages Estonia to intensify its measures for combating money laundering and financing of terrorism.[158] The report highlights areas for improvement such as enhancing understanding of money laundering and risks of financing terrorism, effectiveness of investigations and prosecutions, confiscation of criminal proceeds, application of AML/CFT preventive measures by the private sector, and supervision and transparency of beneficial ownership.[159]

---

[154] Estonian Financial Intelligence Unit (2022), *supra nota* 16.
[155] *Ibid.*
[156] *Ibid.*
[157] De Vido (2015), *supra nota* 128, p 1291.
[158] MONEYVAL (2022). *Anti-money laundering and counter-terrorist financing measures. Estonia. Fifth Round Mutual Evaluation Report.* https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd96.
[159] *Ibid.*

3.2 Decentralisation in Estonia

DAOs generally fall into two categories: registered DAOs, which are structured in accordance with the laws of a particular country and registered in the relevant commercial register, and unregistered DAOs, which are established outside the legal framework defined by national law and do not have a commercial register.[160] However, a DAO without a legal entity (like a partnership) causes a number of legal issues, such as lack of global recognition, lack of personality and unlimited liability.[161] In 2022, INO MTÜ[162] was added to the Estonian business register, with the purpose of reducing legal risks emanating from DAO.[163]

However, concerning DeFi, in January 2022, the FIU published research that raised concerns regarding the forthcoming period, which is expected to see an increase in vulnerability of the decentralised finance sector to cyberattacks and a corresponding rise in the risk of money laundering.[164] The Estonian Financial Supervision Authority (FSA)[165] also warned about the DeFi trend, saying that it is necessary for DeFi participants to qualify their activities properly, since these should still fall under regulation of some kind. Several potential risks are associated with this, including the perceived achievement of complete decentralisation, risks associated with stablecoins, risks stemming from market volatility, and security vulnerabilities.[166]

In Estonia, the Money Laundering and Terrorist Financing Prevention Act (MLTFPA)[167] was imposed on virtual currency service providers, rendering an operating licence mandatory to provide virtual currency services.[168] The Financial Intelligence Unit (FIU) was entrusted with the responsibility of reviewing licence applications and verifying adherence of service providers' operations to MLTFPA mandates.[169]

---

[160] Financial Supervision Authority. *DAO*. https://www.fi.ee/en/finantsinspektsioon/innovatsioonikeskus/DAO.
[161] Lätt, P. (2022). Decentralised autonomous organisations/DAOs in estonia. *e-Residency.* https://www.e-resident.gov.ee/blog/posts/daos-in-estonia/.
[162] *Internet Native Organization*. https://internetnative.org/.
[163] Lätt (2022), *supra nota* 161.
[164] Estonian Financial Intelligence Unit (01.2022). Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis. *Rahapesu andmebüroo.* https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee.
[165] Financial Supervision Authority. *DeFi*. https://www.fi.ee/en/finantsinspektsioon/innovation-hub/defi.
[166] *Ibid.*
[167] RT I, 17.11.2017, 2.
[168] Estonian Financial Intelligence Unit (01.2022), *supra nota* 164.
[169] *Ibid*.

When it comes to trading virtual currencies, the MLTFPA 2 (1)) and its rules for financial institutions apply to virtual currency service providers. This makes virtual currency service providers "obligated persons" under the MLTFPA.[170] This means that, according to 70 subsection 1 point 4 of the MLTFPA, you need a licence to offer a virtual currency wallet service or a virtual currency trading service, unless one of the exceptions in 70 subsection 2 applies. 71 of the MLTFPA says that an application for an activity licence must be sent to the Financial Intelligence Unit, which is in charge of making sure that people who are required to by § 64 of the MLTFPA, follow the rules of this act and the laws that were made based on it.[171]

Currently, under MLTFPA § 3(9), crypto-assets are recognised as being three distinct types of services. The first type of service, known as the "virtual currency transfer service," permits electronic transactions that transfer virtual currency from the initiator to the recipient's wallet or account, regardless of whether they are using the same or different service providers. The second type, the "virtual currency exchange service," allows for exchange of virtual currency with fiat currency and vice versa, or the exchange of one virtual currency for another. Finally, the "virtual currency wallet service" generates keys or stores encrypted keys in order for customers to securely keep, store, and transfer their virtual currencies.

The relationship between the concept of a virtual currency wallet service and DeFi exchanges has been strongly established by utilising wallets for digital assets and cryptocurrencies for storage and management purposes, as defined in MLTFPA § 3(10) under the term "virtual currency wallet service". In the context of this specific service, the service providers hold a degree of control over the financial resources of their customers, which differs from decentralised financial services that do not possess such authority.

The forthcoming offering, as described in Section § 3 (10^1) of MLTFPA, pertains to a virtual currency exchange service that bears similarities to DeFi exchanges. Yet, within the traditional framework of virtual currency exchange, the exchange process is under the control of service

[170] Financial Supervision Authority. *The legal framework of initial coin offering in Estonia.* https://www.fi.ee/en/investment/aktuaalsed-teemad-investeerimises/virtuaalraha-ico/legal-framework-initial-coin-offering-estonia.
[171] *The legal framework of initial coin offering in Estonia, supra nota* 170.

providers, who possess the ability to convert customers' funds into any currency, be it fiat currency or crypto loans. Decentralised finance, in contrast, entails a mechanism of exchange between the customer and the blockchain, without the involvement of a centralised service provider. Within these models, it is possible for customers to engage in direct currency exchange with the blockchain.

The final service term, as stipulated in MLTFPA § 3 (10^2), pertains to the transfer of virtual currency. This service is intrinsically linked to the operational capabilities of DeFi hybrid exchanges, as the transfer of virtual currencies constitutes a fundamental aspect of these platforms. Within a DeFi exchange, individuals have the capability to transfer digital currencies from their personal wallet or account to wallets or accounts of other users. Smart contracts can facilitate transfer services by being stored on the blockchain. In comparison with traditional financial systems, electronic transactions are frequently assisted by intermediaries such as banks.

Furthermore, in the context of cryptocurrency trading, it is noteworthy that the Estonian Supreme Court's decision RKHKo 3-3-1-75-15[172] considered the act of trading Bitcoins as a commercial enterprise that involves the provision of various payment methods.[173] The statement implies that individuals engaged in the business of virtual currency trading may be considered to provide virtual currency services as per the provisions of the MLTFPA 2 (1) points 10 and 11.[174]The authorisation must be obtained in accordance with Section 70 (1) points 4 or 5 of the MLTFPA.[175]

The scope of the Act is restricted to the particular legal and natural entities as identified in MLTFPA § 2. The aforementioned limitation unsuccessfully meets the criteria of MLTFPA § 2, for complete decentralisation. Although the aforementioned services bear a strong resemblance to a DeFi exchange, it is important to note that a DeFi exchange platform in its entirety does not satisfy the requirements of a service provider.

[172] RKHKo 3-3-1-75-15, p 17.
[173] *The legal framework of initial coin offering in Estonia, supra nota* 170.
[174] *Ibid.*
[175] *Ibid.*

Hybrid DeFi exchange services fit the definitions in MLTFPA § 3 (9) very well, and may therefore be applied to this legislation, since DeFi hybrid exchange has a centralised control feature, which is typically a service provider. Due diligence criteria specify MLTFPA for hybrid exchange platforms, in MLTFPA § 19 and § 20.

3.3 Challenges for the legislative definition of DeFi services

The challenges for defining a service provider in full and complete decentralisation continue in other Estonian legislation. These regulations may be applicable to DeFi exchange services, including security finance laws, e-money institutions, and crowdfunding services. Firstly, a full DeFi exchange may be classified as a security platform. Within the realm of blockchain-based financial services, a service that meets the legal criteria for classification as a security may be subject to a range of regulatory requirements. The classification of a securities service may be applicable to exchange activities conducted on a fully decentralised finance platform, dependent upon the characteristics of the assets involved in the trading process. The assets transacted on DeFi platforms may be classified as securities in accordance with securities regulations, in particular if they exhibit features that are analogous to conventional securities. In general, tokens that are generated via initial coin offerings (ICOs)[176] or security token offerings (STOs)[177] may be subject to securities regulations.[178] In the event that these tokens are exchanged on a full DeFi platform, it is possible for the platform to be subjected to securities regulations.

The Securities Market Act (SMA)[179] is legislation for governing regulation of securities in Estonia. According to the Estonian FSA, tokens that give specific rights to investors in the issuing company or whose valuation is linked to the future profitability or success of a business are expected to be classified as securities under the definition provided in § 2 of the SMA.[180] The § 917 of the Estonian Law of Obligations Act defines a security as any instrument to which a patrimonial right is bound in a way that prevents the exercise of the right without the instrument.

---

[176] Delivorias, A. (2021). Understanding initial coin offerings: A new means of raising funds based on blockchain. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)696167, p 1.
[177] *A Deep Dive Into Security Token Offering (STO)*. (2023). Cryptoflies News. https://blog.cryptoflies.com/a-deep-dive-into-security-token-offering-sto/.
[178] *The legal framework of initial coin offering in Estonia, supra nota* 170.
[179] RT I 2001, 89, 532.
[180] *Ibid.*

It is probable that specific securities identified in SMA § 2 (1) may be transacted on fully decentralised exchange platforms. It is worth noting that the financial instruments specified in points 1-4 of SMA § 2 (1) may potentially be present on these platforms. Nonetheless, it is notable that decentralised exchange services may not satisfy the requirements set forth in the definitions of a regulated securities market, multilateral exchange facility, or organised exchange facility as stated in § 3 SMA (1), and thus may not be considered as a legitimate exchange venue.

As per Section § 3 (2-4) of SMA (2-4) regulations, a decentralised exchange platform cannot be classified as a "regulated securities market," "multilateral trading facility," or "organised trading facility." This is due to the fact that such platforms are not operated or managed by a central entity, regulated market, or investment firm. DeFi has the capacity to fulfil the prerequisites of enabling integration of diverse stakeholders' interests and creating a contractual agreement through a smart contract, thereby satisfying these criteria. However, the lack of a central operator that can be subject to regulatory oversight makes DeFi ineligible for qualification under these provisions.

It is important that specific elements of semi-decentralised finance exchanges, including trading protocols and order matching, may remain subject to regulatory compliance, particularly if they entail exchange of securities or other financial instruments that are regulated by extant laws. The reason for this occurrence can be attributed to the implementation of the proposed pilot regime for DLT, which serves to govern trading platforms that operate on decentralised ledgers.[181]

Therefore, DeFi has the ability to facilitate the acquisition and transfer of securities under non-discretionary conditions through bringing together the interests of various parties, resulting in a contractual agreement. However, its decentralised nature precludes it from being classified as a traditional exchange platform in accordance with Section § 3 (2-4) of Estonian SMA (2-4).

[181] COM(2020) 594 final, *supra nota* 14.

Secondly, a full DeFi exchange may be classified as an e-money institution. In Estonia, it is the Payment Institutions and E-money Institutions Act (PIEIA)[182], which regulates the use of e-money and provides specific guidelines for e-money issuers. Exchange on a completely decentralised platform may fulfil the legal criteria of an e-money institution, if an exchange offers payment services or facilitates the transfer of funds between users.

According to § 5 PIEIA, payment institutions refer to entities that are licensed and regulated by financial authorities and engage in the continuous provision of payment services, including execution of payment transactions. Decentralised finance services that operate on a fully decentralised basis possess the capability to fulfil the aforementioned criteria. This is due to the fact that such services generally entail users depositing virtual currencies into liquidity pools and independently making exchange determinations.

However, according to § 6 PIEIA, fully decentralised exchange services may not qualify because they do not satisfy all requirements specified in this section. Specifically, in PIEIA § 6 (1) e-money is stored on e-money devices, which is in contrast to DeFi, where services rely on a network of users to facilitate transactions rather than a single issuer of electronic currency.

Additionally, under PIEIA § 7 (1), completely decentralised financial service platforms do not qualify as e-money institutions, because they do not meet the requirement of being a public or private limited company. Notably, decentralised finance services typically do not issue e-money in their own names or engage in a continuous activity of issuing e-money according to PIEIA § 7 (2).

While DeFi exchange services may entail the use of stablecoins, they are not e-money institutions based on PIEIA § 6 (1) and 7 (1-2), thus they are not subject to the same regulatory requirements as e-money institutions.

[182] RT I 2010, 2, 3.

Thirdly, in 2021, Estonia introduced a proposal for national legislation called UMIVS[183] to set out operating requirements, supervision, and investor protection requirements for various types of companies operating in Estonia. These include crowdfunding services, companies offering crypto-assets and virtual currency services, and other companies that offer alternative investment opportunities that have not been subject to supervision yet.

Thus, at present, crowdfunding is regulated by Directive 2020/1503 and exchange on an entirely decentralised financial platform can be viewed as a form of crowdfunding service. Users can participate in exchange activities on a DeFi platform by depositing their virtual currencies into liquidity pools, which facilitate trades between various assets.[184] When users deposit virtual currencies into a liquidity pool, they are rewarded with tokens representing their proportional share of the pool, referred to as "liquidity shares".[185] Then, these tokens can be traded on the platform or used to participate in other platform-based activities.[186] As users are able to pool their virtual currencies to facilitate trades and receive returns on their investments, exchange on a fully decentralised finance platform can be considered a form of crowdfunding service.

Article 2 (1e) defines 'crowdfunding service provider' as a legal entity that offers crowdfunding services, while Article 2 (1l) defines 'crowdfunding project' as the business activity or activities for which a project proprietor seeks funding through a crowdfunding offer. Because crowdfunding services involve soliciting funds from a large number of investors for a particular project or business proposal, typically via an online platform, fully decentralised exchange services are not considered crowdfunding services. The crowdfunding service provider functions as an intermediary between the creator of the project and investors, facilitating the investment process and providing investors with certain forms of protection. Decentralised exchange services, on the other hand, enable users to trade assets without pooling their funds for a specific project or business concept, and there is no central entity responsible for facilitating the investment process or protecting investors.

[183] UMIVS draft explanation, 2021. https://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#FxmJFP8M.
[184] Jensen *et al* (2021), *supra nota* 39, p 50.
[185] *Ibid.*
[186] *Ibid.*

Furthermore, completely decentralised financial services do not qualify as crowdfunding services because they do not meet the criteria outlined in Article 2 (1a). However, decentralised finance services do not aggregate the capital of multiple investors but rather permit individual investors to engage in transactions directly with one another, without the need for intermediaries. Moreover, contrary to provisions of the Directive, decentralised finance services do not have a defined investment policy that is managed by a service provider. Rather, investors are permitted to make their own investment decisions based on the information available on the platform.

Therefore, fully decentralised exchange services do not satisfy the definition of crowdfunding services based on Article 2 (1a), and are not subject to the requirements outlined in the laws and regulations governing crowdfunding services.

This chapter answers the second research question, of what are the existing legal regulations governing decentralised exchange financial services in Estonia? Estonia has demonstrated worthy performance for attracting crypto services to its country. Hybrid DeFi fits the definitions according to MLTFPA § 3 (9), since DeFi hybrid exchanges may have a feature of centralised control, which in case of MLTFPA § 2 (1) is a service provider. Due diligence criteria for hybrid exchange platforms in MLTFPA sections § 19 and § 20.

On the other hand, complete or full DeFi is not addressed by these legislations. MLTFPA is limited to entities as identified in MLTFPA § 2 (1), and it does not meet the criteria for complete decentralisation. DeFi platforms have the ability to facilitate acquisition and transfer of securities under non-discretionary conditions, but they are not classified as traditional exchange according to § 3 (2-4) of SMA (2-4) on platforms due to their decentralised nature. In addition, fully decentralised exchange services do not satisfy the definition of crowdfunding services and are not subject to the requirements outlined in the laws and regulations governing crowdfunding services according to Article 2 (1a) of Directive 2020/1503. Finally, DEX services are not considered e-money institutions and are not subject to the same regulatory requirements as e-money institutions according to PIEIA § 5 and § 7 (1), despite involving users depositing virtual currencies into liquidity pools and making independent exchange decisions.

4. FULLY DECENTRALISED DEX SERVICES

The concluding section of the thesis will look into the subject matter of full financial exchange decentralisation and its prospective impacts. Based on the aforementioned analysis, it can be stated that the primary challenges encountered by regulators in shaping their views on DeFi start directly from its fundamental features. As it has been established, completely decentralised finance exchange services fall outside the scope of the regulatory framework. This is mainly because there is no central authority responsible for operation of these systems, and thus it is challenging to impose any legislative framework on them. Also, identifying participants involved in full DeFi presents a significant challenge.

In the realm of decentralised finance exchange services, a pertinent question or issue pertains to assessment of a platform's level of decentralisation. The matter at hand shows distinctions, as the services in question may vary in degree of decentralisation, spanning from complete decentralisation to partial decentralisation. Therefore, it is important to carefully examine a platform's governance, KYC and AML measures, liability, and protection of users.

4.1 Decentralisation of DEXs

The absence of traditional admission procedures such as registration and licensing, as well as the lack of effective supervision mechanisms such as accountability and responsibility, poses significant challenges in the context of decentralisation. This is a crucial concern for multiple parties involved in the regulation of the DeFi industry.

Decentralised systems are characterised by the absence of centralised ownership of data, control, and decision-making authority vested in a single entity. As a result, it can be a difficult task, and in some cases impossible, to identify the party that includes the crypto-asset service provider and is actively pursuing authorisation.[187] Furthermore, a DAO operates through a mechanism whereby anonymous token holders submit proposals, which are subsequently subject to a voting process based on the total number of tokens held by each participant. The majority of recommendations put forth typically pertain to potential investments, although they may also

[187] Pavlidis (2021), *supra nota* 20, p 470.

encompass malevolent schemes such as the unilateral allocation of the entirety of the DAO's funds to a single individual.[188] Services that have a centralised governance structure, on the other hand, are typically controlled by a single regulated entity or team.

Due to the dependence of DAO on specific decentralised governance mechanisms, the decision-making process is contingent on consensus among its members. In accordance with consensus among its constituents, a DAO has the ability to undergo modifications in its operational procedures, thereby adopting a fresh set of encoded regulations.[189] Determination of the voting populace responsible for implementation of modifications within the DEX ecosystem, including but not limited to Uniswap and Compound, remains uncertain. The findings of the study indicate that governance systems of the DeFi protocols Compound and Uniswap exhibit a high degree of centralisation, with a limited number of addresses exerting significant control over decision-making processes.[190]

The aforementioned fact means that a group of engaged users plays an important part in determining the future development of these platforms, even as the platforms themselves try to drive through full decentralisation. The process of becoming a DEX influencer and establishing contractual connections on Uniswap is an intriguing phenomenon to observe. Typically, contractual arrangements commence with the user's registration on the platform, which involves clicking on a button that displays the terms and conditions and providing personal information. The process of decentralisation involves an unusual approach to the formation of contractual relationships.

Notably, Uniswap's ecosystem has not been subjected to registration with the United States Securities and Exchange Commission[191] (SEC).[192] The UNI token, which is indigenous to the platform, does not possess the status of a "security," and the trading platform is not authorised as

[188] Nielsen, T. (2019). Cryptocorporations: a proposal for legitimizing decentralized autonomous organizations. Utah Law Review, 2019(5), 1105, p 1110.
[189] Faqir-Rhazoui, Y., Arroyo, J., & Hassan, S. (2021). A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. Journal of Internet Services and Applications, 12(1), p 4.
[190] Fritsch, R., Müller, M., & Wattenhofer, R. (2022). Analyzing Voting Power in Decentralized Governance: Who controls DAOs?, p 11.
[191] U.S. Securities and Exchange Commission (SEC). https://www.sec.gov/about/what-we-do.
[192] Kim (2021), *supra nota* 69, p 341.

an "exchange" or granted any exemption from the registration prerequisites.[193] On September 16, 2020, Uniswap made an announcement regarding the distribution of UNI tokens.[194] One of the supposed purposes of the token was to enable the management of the Uniswap ecosystem.[195] Individuals who possess UNI tokens have the ability to create and participate in voting for "governance proposals" that aim to enact modifications to the Uniswap protocol. This is due to the fact that each UNI token represents a share in the Uniswap community.[196] Therefore, prior to making any statements regarding the ownership of Uniswap, it is essential to note that the platform operates through utilising governance tokens. These tokens are not restricted to a specific group, but rather are accessible to any individual who wishes to participate.

The present version of Uniswap consists of the Uniswap V3 smart contract protocol and a web interface that is accessible online.[197] On Uniswap, which operates on the Ethereum blockchain, formation of contractual relationships between users is governed by the smart contract code of the platform. When a user interacts with Uniswap to exchange cryptocurrencies, they initiate a contractual relationship with the smart contract code that governs the platform's operation. This connection is created when a user transmits a transaction to the Uniswap smart contract on the blockchain. Moreover, the smart contract code determines the parameters of the contractual relationship between the user and Uniswap smart contract, such as the exchange rate for the transaction, fees charged, and duration of the transaction. Once the user submits a transaction to the Uniswap smart contract, the contract will implement the transaction based on the code's conditions. The user's cryptocurrency will be transferred into the contract, and then the exchange cryptocurrency will be transferred back to the user's wallet.

The following stages illustrate the principles for formation of contractual relationships in Uniswap. The user then selects the cryptocurrencies he wishes to trade and inputs the desired amount for the exchange. Then, the Uniswap smart contract is responsible for calculating the exchange rate and fees based on current market conditions and code-specified conditions. The user then verifies the transaction by transmitting it to the Uniswap smart contract, after which the

[193] *Ibid*.
[194] *Introducing UNI*. (2020). https://uniswap.org/blog/uni/.
[195] *Ibid*.
[196] *Ibid*.
[197] *Uniswap App*. https://app.uniswap.org.

Uniswap smart contract executes the trade in accordance with the code's conditions. Finally, the exchanged cryptocurrency is returned to the user's wallet and the transaction is completed.

As Uniswap is a decentralised platform, it lacks standard terms of service agreement. However, it provides users with a few guidelines to follow when using the platform. Users are initially accountable for their own security and privacy. This includes taking necessary precautions to safeguard their wallets, private keys, and other sensitive information. Users must abide by all applicable laws and regulations and refrain from engaging in unlawful activities on the platform. In addition, users should exercise caution when trading on the platform and conduct their own investigation prior to engaging in any transactions. Users are also encouraged to contribute to the platform's development and provide feedback on its functionality, as Uniswap is an open source project supported by the developer community.[198] Inherently meaning, Uniswap is a decentralised platform, so there is no central authority responsible for its operation. It would appear that users are expected to comprehend and embrace the risks associated with utilising a decentralised platform.

To sum up, due to the absence of traditional admission procedures and efficient supervision mechanisms, decentralisation of DEXs presents difficulties. Consensus among members governs the decision-making process, and consumers play a significant role in determining future development. Uniswap's ecosystem has not been registered with the SEC, and the UNI token is used to facilitate ecosystem management. To operate, the platform uses governance tokens, which are accessible to anyone who desires to participate. As Uniswap is a decentralised platform, users are responsible for their own security and privacy, must comply with applicable laws and regulations, and must contribute to its growth.

4.2 AML and KYC compliance

Lack of compliance with relevant regulations and laws, including AML and KYC requirements, is a notable issue for fully decentralised finance exchange services. However, several initiatives exist that enable DeFi services to comply with regulatory requirements. For instance, the World Economic Forum is spearheading a project aimed at developing a toolkit for policymakers in the

[198] *Uniswap Labs Terms of Service.* (2023). https://uniswap.org/terms-of-service.

field of DeFi, to aid governments globally to effectively address related challenges.[199] On the other hand, even though DeFi is predicated on the principle of decentralisation, it cannot operate in a controlled environment.[200] In addition, some claim that decentralised, self-managing finance is ultimately impractical and that entrepreneurs must supplement the technical infrastructure with social organisations that can effectively manage counterparty risk.[201]

In this regard, DeFi services have the potential to collaborate with regulatory bodies in order to ensure adherence to pertinent legal and regulatory frameworks. This could entail collaborating with regulatory bodies to establish protocols for adherence to or engaging in regulatory experimentation environments to evaluate novel compliance remedies. Nevertheless, the question arises as to which party should establish communication with regulatory authorities.

Additionally, regulators may lack the necessary skills to effectively resolve the challenges posed by this new type of technology. Due to the lack of a unified approach to DeFi regulation worldwide, it is currently difficult to determine the optimal approach. To discover the optimal regulatory approach to address these challenges, regulators must acquire the required competencies. The EU's digital finance package is an excellent starting point for gaining competencies.

In order for DeFi to function as intended, its guiding principles must be incorporated into the system.[202] Utilising oracles may prove advantageous. Nevertheless, it is necessary to establish a standardisation of oracle design and patterns to successfully address frequent security breaches.[203] Also, implementation of artificial intelligence and machine learning algorithms presents an opportunity to rectify errors that may arise from user actions, security breaches, and protocol shortcomings. However, utilisation of centralised data storage and management by artificial intelligence may pose a potential risk, as it could be vulnerable to data tampering,

---

[199] World Economic Forum. (2021). *Decentralized Finance: (DeFi) Policy-Maker Toolkit.* https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit/.
[200] Zetzsche *et al* (2020), *supra nota* 29.
[201] Harwick, C., & Caton, J. (2022). What's holding back blockchain finance? On the possibility of decentralized autonomous finance. *The Quarterly Review of Economics and Finance, 84*, 420-429.
[202] Zetzsche *et al* (2020), *supra nota* 29.
[203] Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance—A multivocal approach. *Applied Sciences, 11*(16), 7572.

manipulation, and violations of privacy.[204] This has the potential to function if certain criteria are met, such as the regular auditing of smart contract code by specialised specialists and the standardisation of DEX smart contracts.

In this regard, implementing instruments to monitor and analyse transactions is an important consideration. DeFi platforms can employ transaction monitoring and analysis tools to identify potentially illegal activities and ensure compliance with AML regulations. Tools for Blockchain analysis can monitor the transfer of funds and identify instances of possible money laundering. It is not known with whom and for what purpose this can be accomplished.

It is also possible to implement protocols for decentralised identity verification within DeFi services, which may facilitate the maintenance of compliance to KYC. In the context of decentralisation, the necessity of KYC protocols may be called into question, as it is the responsibility of both legal entities and individuals to verify the identity of their customers in order to evaluate any related risks. Based on what is mentioned above, establishing minimum requirements for launching DeFi protocols is crucial due to the nature of their adherence to established rules, which could potentially be regulated by laws and implemented without the need for additional oversight by governing authorities.

DeFi services have the potential to collaborate with regulatory bodies to ensure adherence to relevant legal and regulatory frameworks, but regulators may lack the necessary skills. Establishing minimum requirements for launching DeFi protocols is essential to ensure compliance with established rules, which could potentially be regulated by laws and implemented without additional oversight.

4.3 Liability and protection

The absence of a central authority responsible for operation of the platform implies that users bear liability for any losses or damages incurred. The issue of liability remains unresolved. According to the terms of Uniswap, customers are exclusively responsible for managing their

[204] Kirimhan (2023), *supra nota* 102*,* p 8.

own funds and carrying out their own transactions when utilising a DeFi exchange platform. Users can protect themselves by doing their own research and due diligence on the tokens they wish to trade, using appropriate security measures to protect their private keys and wallets, and being aware of the risks involved with using DeFi services.[205]

Another aspect of liability pertains to the responsible party for the smart contract code that governs its operation, as well as the methods for addressing any potential issues with said code. In the case of exchange services such as Uniswap, the smart contract code responsible for regulating the platform's functionality is commonly produced by a group of developers or a community of contributors. Nonetheless, the code lacks a central governing body, and users bear the burden of reviewing and validating the code prior to utilising the platform, given that it is open source. In the event that discrepancies are detected in the smart contract code, the community of users or contributors may suggest and execute modifications to the code via a decentralised governance mechanism. The customary procedure entails the presentation of a proposal, deliberation, a survey of opinions among members of the community, and the execution of the authorised modifications to the code.[206] In this scenario, it would be advantageous for certain DeFi services to be subjected to third-party code audits, in order to detect and resolve any possible vulnerabilities or bugs. Certain services, such as Ethereum[207], have instituted bug bounty initiatives, that incentivise individuals to detect and disclose any code-related concerns.

One of the challenges with controlling DeFi is that there are so many ways to hide who is using it, control it, and arrange it so that it can be difficult to ensure protection and authorities requirements. It is crucial to safeguard investors against potentially fraudulent activities and scams. As stipulated in the terms and conditions, conducting comprehensive research on the DeFi project is recommended. It is advisable for investors to undertake comprehensive research on the tokens or projects they intend to invest in on DeFi platforms such as Uniswap. The process may entail scrutinising the white paper, website, and social media profiles of the project to acquire a more comprehensive understanding of its objectives, personnel, and strategic plan.

---

[205] *Uniswap Labs Terms of Service*, *supra nota* 199.
[206] *Governance.* Uniswap Protocol. https://uniswap.org/governance.
[207] *Ethereum Bug Bounty Programme.* Ethereum.org. https://ethereum.org.

Moreover, Uniswap's provisions entail the verification of a smart contract code. It is advisable for investors to conduct thorough verification of the smart contract code of the tokens they intend to invest in in order to ascertain their security and the absence of vulnerabilities. The process of code verification can be accomplished by examining blockchain explorers or by availing the services of third-party auditing entities. It appears that utilising such services may not be suitable for lay consumers who lack knowledge of code functionality and the requisite code scrutiny.

Furthermore, the terms of Uniswap provide a set of general guidelines. Investors are advised to exercise caution when considering high-risk investments that offer substantial returns with minimal risk. Investors are recommended to utilise secure wallets to safeguard their tokens and private keys, as this measure can mitigate the risks of theft and hacking. Investors have the opportunity to engage in decentralised governance procedures on DeFi platforms such as Uniswap, with the aim of detecting and resolving potentially fraudulent activities and scams.[208] Although the steps outlined are excellent, they do not provide adequate protection for the consumer.

This chapter answers the third research question on what must be done in areas with no regulation, whether any additional regulations are required, and how to effectively implement due diligence regulations in DeFi technology. As in the analysis above, it became obvious that there are solutions that may be technical in nature. The extent of decentralisation in each case of DeFi services should be evaluated based on the presence of a central authority, an intermediary, or other third parties with significant control or who directly or indirectly perform or provide services. Even though there are supposedly fully decentralised markets, such as Uniswap or Compound, it is difficult to determine whether these markets are truly decentralised or merely claim to be. Notwithstanding, it makes sense to implement safety measures at the regulatory level, which may include establishing the minimum technical requirements for launching DeFi services, as the analysis of the risks associated with full DeFi has revealed that there are a number of legal obstacles involved.

[208] *Uniswap Labs Terms of Service*, *supra nota* 199.

DeFi platforms could implement transaction monitoring and analysis tools to identify potentially illegal activities and ensure compliance with AML regulations. This could involve monitoring the transfer of funds on the blockchain to detect instances of possible money laundering or other illicit activities. Furthermore, protocols for decentralised identity verification could be implemented within DeFi services to facilitate KYC compliance. This could involve establishing mechanisms to verify the identity of both legal entities and individuals to evaluate any associated risks while considering the decentralised nature of DeFi platforms.

In addition, establishing minimum requirements for launching DeFi protocols could be crucial to ensuring adherence to established rules and regulations. This could potentially be regulated in law and implemented without the need for additional oversight by governing authorities, considering the decentralised nature of DeFi platforms. Also, determining the responsible party for the smart contract code that governs operation of DeFi platforms could prove to be important. Users typically review and validate the open source code of DeFi platforms, but third-party code audits or bug bounty initiatives could be considered to detect and resolve any vulnerabilities or bugs in the code.

As for protection of customers, providing guidelines may be useful, however it has no legal boundaries or remit. To have a meaningful influence on the platform, consideration could be given to investors engaging in decentralised governance procedures to detect and resolve potentially fraudulent activities or scams on DeFi platforms.

As for regulations and wording directions of reports and services, regulations tend to centralise DeFi services, which is beneficial for consumers and protections but eliminates the advantages of decentralisation. According to MiCa's analysis, it properly includes exchanges with central elements, such as a central authority, intermediaries, or other significant third parties. This indicates that half of the Defi exchanges are well-regulated and safe for investors and other individuals. However, there are still grey areas between regulated and unregulated DeFi services where service providers may cover up illicit activities.

The DeFi is not ignored, and its potential risks are recognised. There are still risks, such as the potential for an uncontrolled outflow of capital from traditional and centralised finance into the grey zone, the absence of consumer and investor protection, and the absence of uniformity and norms. Thus, in light of the conclusions drawn in the chapters before this, we may conclude that hybrid services are subject to significant regulatory oversight, resulting in a multitude of legal advantages for consumers as well as corresponding obligations for service providers. However, present-day full DeFi exchanges continue to operate outside the purview of regulatory frameworks.

CONCLUSIONS

The birth of DeFi can be traced back to the publication of a whitepaper on decentralised applications in 2014, following the emergence of Bitcoin in 2009. DeFi is a blockchain-based service that facilitates direct cryptocurrency and other crypto-asset exchange between individuals, eliminating the need for intermediaries such as banks. In 2020, the European Commission unveiled a digital finance package, including the Regulation on Markets in Crypto-Assets (MiCA), which aims to safeguard the interests of investors and consumers, while encouraging innovation and competition within the crypto-asset market. MiCA covers services pertaining to crypto-assets, including partially decentralised services, while fully decentralised services are excluded.

Partial or hybrid DeFi is a financial system that combines elements from traditional and decentralised finance, while full DeFi is a financial system entirely based on blockchain without any features of partial DeFi. Regulators need to create innovative regulatory structures and technological solutions to ensure AML compliance for fully decentralised finance exchange services. Examining the Estonian regulatory structure may help, because Estonia has issued 381 licences for the provision of virtual currency services, which is 55% of all licences in the world.

This paper identified a research problem pertaining to the absence of a central authority or intermediary in fully decentralised finance services, which poses challenges for complying with legal and regulatory requirements. DeFi presents opportunities for transparency and integrity, but also poses risks to the economy due to its pseudonymous nature, lack of formal leadership, and limited control over contracting processes. It also faces regulatory challenges due to its reliance on decentralisation.

The objective of this paper was to analyse the MiCA proposal and existing legislation in Estonia regarding the relationship between decentralised finance systems and due diligence laws. The paper aims to provide policymakers and regulators with insights into regulatory obstacles and prospects encountered by the DeFi industry in Estonia and the EU through answering the questions posed. The paper presents three research inquiries that served as a framework for the

analysis: the extent to which MiCA governs financial services related to decentralised exchange; the existing legal regulations governing decentralised exchange financial services in Estonia; what needs to be done in areas with no regulations; whether any additional regulation is required, and how to effectively implement due diligence regulations in DeFi technology.

Answering the first question, through our analysis, this paper may constitute that MiCA regulates hybrid decentralised exchange finance services to a significant extent. Hybrid services are those that have combined characteristics such as centralised control, intermediaries, and/or compliance obligations with autonomous, independent mechanisms based on blockchains. In contrast, complete decentralised services do not have the features of a hybrid. Importantly, the MiCA framework has established a standard definition for crypto-assets and categorised them into three distinct groups. Crypto-assets refer to digital assets that can be electronically transmitted and stored using distributed ledger technology or comparable methods. Stablecoins are divided into two categories: asset-referenced tokens and electronic money tokens.

MiCA's definition of partially decentralised services consists of three primary criteria: extant EU licences, external influence, and hybrid services that are dependent on centralised control but have autonomous and independent components based on smart contracts. First, in order to qualify for the current EU licence, the service provider must fall under one of the following categories: natural person, legal entity, or other business that has been properly enrolled or registered with relevant regulatory bodies. For the provision of CASPs, corporate entities must obtain permission from the appropriate regulatory body in the European Union member state where they are formally registered. Second, any degree of outside influence or control would be classified as a partial DeFi service-based model in the context of DeFi. Considering that "control" includes the ability to possess, offer, furnish, or use virtual assets, the execution of these functions is dependent on smart contracts in a fully decentralised state. Due to the fact that the value of the funds is preserved within a smart contract on the blockchain, DeFi developers do not retain ownership of their clients' money. Thirdly, partially decentralised services and activities are those related to crypto-assets that fall somewhere between decentralisation and centralisation. So, it is crucial to pay attention to whether services have hybrid characteristics.

In addition, hybrid services, such as trading and exchange, are completely covered by MiCA's Article 3 (1) point 9 (b-d), regardless of whether the contract is established by a DEX system, that is an automatic smart contract. MiCA defines the operation of a trading platform for crypto-assets as the management of one or more multilateral systems that bring together or assist in bringing together the buying and selling interests of multiple third parties for crypto-assets. In the realm of DEXs, these conditions govern hybrid decentralised exchanges if they lead to a contract established by the system or its rules. Smart contracts are used to automatically execute trades between buyers and sellers based on predefined rules and algorithms, meeting the criteria for hybrid decentralised exchanges. DeFi services do not apply to provisions involving acting on behalf of a third party provided in Article 3(1) point 9 (a, e, fa, g). Additionally, the other services mentioned in MiCA by Article 3(1) point 9 (f, h, and hb) are irrelevant to DeFi.

To become a DeFi hybrid exchange, an entity must meet three fundamental requirements of MiCA's Article 4 (1) authorisation, which include establishing a legal entity in the EU, composing a white paper, and notifying the appropriate national authority. The AML directive applies to decentralised services that fall under the MiCA framework since they will be under the auspices of EU regulation.

In response to the second question, in Estonia, the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) was imposed on virtual currency service providers, rendering an operating licence mandatory to provide virtual currency services. The Financial Intelligence Unit (FIU) is in charge of reviewing licence applications and verifying the adherence of service providers' operations to MLTFPA mandates. MLTFPA § 3(9) recognises three distinct types of services for crypto-assets: virtual currency transfer service, virtual currency exchange service, and virtual currency wallet service.

The virtual currency transfer service is intrinsically linked to the operational capabilities of DeFi hybrid exchanges, as the transfer of virtual currencies constitutes a fundamental aspect of these platforms. Thus, the hybrid DeFi fits the definitions of MLTFPA § 3 (9), since DeFi hybrid exchanges may have a feature of centralised control, which is typically a service provider. MLTFPA does not, however, address fully decentralised exchanges, because MLTFPA § 3 (9)

does not satisfy the criteria for complete decentralisation. Therefore, full DeFi exchanges are not subject to the same regulatory requirements as centralised or hybrid exchanges. In addition, completely decentralised exchange services do not meet the criteria for traditional exchange, crowdfunding services, or e-money institutions.

MLTFPA is limited to entities as identified in MLTFPA § 2 (1), and it does not meet the criteria for complete decentralisation. DeFi platforms have the ability to facilitate the acquisition and transfer of securities under non-discretionary conditions, but they are not classified as traditional exchanges according to § 3 (2-4) of SMA (2-4) on platforms due to their decentralised nature. However, DeFi has the capacity to fulfil the prerequisites of enabling the integration of diverse stakeholders' interests and creating a contractual agreement through a smart contract.

In addition, fully decentralised exchange services do not satisfy the definition of crowdfunding services and are not subject to the requirements outlined in the laws and regulations governing crowdfunding services according to Article 2 (1a) of Directive 2020/1503. Decentralised finance services do not aggregate the capital of multiple investors but rather permit individual investors to engage in transactions directly with one another, without the need for intermediaries. Furthermore, DEX services are not considered e-money institutions and are not subject to the same regulatory requirements as e-money institutions according to PIEIA § 5 and § 7 (1), despite involving users depositing virtual currencies into liquidity pools and making independent exchange decisions. Therefore, under the current legal framework in Estonia, there are no corresponding due diligence criteria applicable to decentralised exchange services in their entirety.

In response to the third question, in the analysis above, it became obvious that there are solutions, that may have a technical character. The primary challenges faced by regulators in shaping their views on DeFi start directly with its fundamental features. Decentralised systems are characterised by the absence of centralised ownership of data, control, and decision-making authority vested in a single entity, making it difficult to identify the party that includes the crypto-asset service provider and is actively pursuing authorisation. Completely decentralised finance exchange services fall outside the scope of the regulatory framework, as there is no

central authority responsible for the operation of these systems. Additionally, identifying participants involved in full DeFi presents a significant challenge. The extent of decentralisation in each case of DeFi services should be evaluated based on the presence of a central authority, an intermediary, or other third parties with significant control.

The lack of compliance with relevant regulations and laws, including AML and KYC requirements, is a notable issue for fully decentralised finance exchange services. However, several initiatives exist to enable DeFi services to comply with regulatory requirements, such as the World Economic Forum spearheading a project aimed at developing a toolkit for policymakers in the field of DeFi. DeFi platforms should take proactive measures to ensure compliance with AML regulations and prevent illegal activities. Minimum requirements for launching DeFi protocols should be established to ensure adherence to established rules and regulations. Determining the responsible party for smart contract code could help detect and resolve any vulnerabilities or bugs in DeFi platforms. Effective implementation of due diligence regulations in DeFi technology is crucial to preventing fraudulent activities and protecting investors. To effectively implement due diligence regulations in DeFi technology, it is necessary to balance the benefits of decentralisation with the need for consumer protection and compliance with regulatory frameworks. This requires a collaborative effort between industry stakeholders, policymakers, and regulatory bodies. In areas with no regulation, establishing a framework of minimum requirements for DeFi platforms, implementing transaction monitoring tools, and promoting decentralised governance procedures can provide a foundation for protecting consumers and ensuring compliance with AML and KYC regulations.

The absence of a central authority responsible for the operation of the platform implies that users bear liability for any losses or damages incurred. According to the terms of Uniswap, customers are exclusively responsible for managing their own funds and carrying out their own transactions when utilising a DeFi exchange platform. Users can protect themselves by doing their own research and due diligence on the tokens they wish to trade, using appropriate security measures to protect their private keys and wallets, and being aware of the risks involved with using DeFi services.

In conclusion, the emergence of DeFi has disrupted traditional financial systems, presenting regulatory bodies and lawyers with novel opportunities and challenges. As previously stated in this thesis, regulatory bodies pay attention to the potential risks associated with DeFi, such as illicit activities. The recently introduced MiCA framework is a promising regulatory framework that seeks to ensure consumer protection, market integrity, and financial stability within the hybrid exchange DeFi space.

In addition to regulatory frameworks such as MiCA, it is essential to have effective legal mechanisms in place to guarantee the proper operation of DeFi markets. Recognising the potential risks associated with DeFi and implementing regulatory frameworks and legal mechanisms are essential steps for ensuring the sustainability and confidence of DeFi markets. To remain aware of the rapid development of the DeFi realm and to address emerging challenges, however, persistent investigation, cooperation, and adaptation are required.

KOKKUVÕTE

DETSENTRALISEERITUD FINANTSVAHETUSE TEENUSED EESTI JA EUROOPA LIIDU ÕIGUSE PERSPEKTIIVIST

Jaanika Ansip

Pidevalt arenevas krüptomaailmas on üheks valitsevaks arenguks detsentraliseeritud rahanduse (DeFi) esilekerkimine. DeFi on uus tehnoloogia, mis sarnaneb traditsioonilise finantseerimisega, kuid on üles ehitatud plokiahelale ega kasuta vahendajaid nagu pangad. DeFi vahetus hõlbustab krüptovaluutade ja muude krüptovarade otsevahetust üksikisikute vahel, kaotades vajaduse vahendajate jaoks. Protokoll kasutab finantstehingute loomiseks ja teostamiseks nutilepinguid, mis enamasti põhinevad Ethereumil, kuhu ostja ja müüja vahelised lepingutingimused on otseselt sisse kodeeritud. Ethereum on detsentraliseeritud plokiahela võrk, mille järelevalvet teostab mittetulundusühing Ethereum Foundation. Aastaks 2021 oli DeFi-protokollide üldine kasutajate arv pidevalt kasvanud ja registreeritud oli ligikaudu kolm miljonit unikaalset aadressi. Lisaks ületas 2023. aastaks DeFi protokollides lukustatud krüptovarade koguväärtus 50 miljardit USA dollarit. Rahapesuvastase töökonna (FATF) väitel on DeFi kasvu täpset mõju ebaseaduslikule rahastamisele keeruline hinnata, ent avatud lähtekoodiga teave näitab, et kuritegeliku väärkasutuse oht püsib.

Lõputöös püsitatud uurimisprobleemiks on järelevalveasutuse, keskasutuse või vahendaja puudumine täielikult detsentraliseeritud finantsteenuste puhul, mis muudab juriidiliste ja regulatiivsete nõuete täitmise keeruliseks. Euroopa Liidu krüptovaraturge käsitleva määruse (MiCA) eelnõu reguleerimisala hõlmab krüptovaradega seotud teenuseid, sealhugas osaliselt detsentraliseerrituid; täielikult detsentraliseeritud teenused MiCA põhjenduse punkti 12a kohaselt on välja jäetud ning need toimivad ilma igasuguse järelevalveasutuse kontrollita. Seega regulatiivsele järelevalvele alluvad üksikisikute või üksuste poolt pakutavatest DeFi teenustest ainult osaliselt detsentraliseeritud ehk hübriidlahendused.

Osalist või hübriid DeFit võib kirjeldada kui finantssüsteemi, mis ühendab traditsiooniliste ja autonoomsete mehhanismide elemente, kuna sellel võivad esineda sellised omadused nagu tsentraliseeritud kontroll, vahendajad ja/või vastavuskohustused. Teisest küljest on olemas täielik DeFi, mida võib kirjeldada kui finantssüsteemi, mis põhineb täielikult plokiahelal ilma osalise DeFi funktsioonideta. Täielikku DeFit iseloomustavad omadused on partnervõrgu (*peer-to-peer*) tehingud, tehingute läbipaistvus, avatud juurdepääs ning sõltumatu juhtimine. See tähendab, et kasutajad on kaasatud otsustusprotsessi, kuid otsused tehakse konsensusmehhanismi kaudu. Käesolev uurimistöö soovib anda ülevaate regulatiivsetest väljakutsetest ja võimalustest, mis seisavad DeFi teenuste ees Eestis ja ELis.

Lõputöös esitatakse analüüsi raamistikuks kolm uurimisküsimust:

- mil määral MiCA reguleerib krüptovara teenuseid, mis on seotud detsentraliseeritud finantsvahetusega;
- mil määral Eestis kehtivad õigusnormid reguleerivad detsentraliseeritud finantsvahetuse teenuseid;
- mida tuleb teha valdkondadega, kus puuduvad õigusnormid.

Analüüs näitas, et hübriid DeFi on olulisel määral reguleeritud, kuid regulatsioonid ei hõlma täielikku detsentraliseerimist. Eestis kehtiva õigusraamistiku kohaselt puuduvad täieliku DeFi suhtes kehtivad vastavad seadusandlikud kriteeriumid. Alas, kus õigusnormid puuduvad, võib DeFi platvormide seadistamiseks tehniliste miinimumstandardite kehtestamine aidata kaitsta tarbijaid ja tagada AML- ja KYC-reeglite järgimise.

Uurimistöö esimesele küsimusele MiCA regulatsioonide osas võib anda hinnangu, et hübriid DeFi on oluliselt reguleeritud, ent täielikult detsentraliseertiud DeFi mitte. MiCA hübriid detsentraliseeritud teenuste määratlus koosneb kolmest peamisest kriteeriumist: kehtiv ELi tegevusluba, mõju ehk kontroll ja hübriidteenused, mis sõltuvad tsentraliseeritud juhtimisest, kuid millel on autonoomsed ja sõltumatud nutilepingutel põhinevad komponendid. Hübriidteenused, nagu kauplemine ja vahetus, on täielikult hõlmatud MiCA artikli 3 lõike 1 punkti 9 alapunktidega b–d, olenemata sellest, kas leping on sõlmitud DEX-süsteemiga, st automaatse nutilepinguga. DEX on DeFi finantsteenuste automatiseeritud ja iseseisev rakendus või platvorm. DeFi hübriidvahetusplatvormiks saamiseks peab täitma MiCA artikli 4 (1)

loanõudeid, mis hõlmavad juriidilise isiku asutamist ELis, valge raamatu koostamist ja vastava riikliku asutuse teavitamist.

Teisele küsimusele vastates on oluline märkida, et Eestis kehtestati virtuaalvaluutateenuste osutajatele rahapesu ja terrorismi rahastamise tõkestamise seadus (RahaPTS), mis muudab virtuaalvaluutateenuste osutamiseks tegevusloa kohustuslikuks. Rahapesu andmebüroo vastutab tegevusloa taotluste läbivaatamise ja teenusepakkujate tegevuse RahaPTS kohustuste järgimise eest. RahaPTS § 3 (9) tunnustab kolme erinevat tüüpi krüptovarade teenuseid: virtuaalse valuuta ülekandeteenus, virtuaalse valuuta vahetusteenus ja virtuaalse valuuta rahakoti teenus.

Hübriid DeFi vastab RahaPTS § 3 lõike 9 määratlustele ja seetõttu võib olla kohaldatav käesolevale õigusaktile, kuna hübriid DeFi vahetusteenustel on tsentraliseeritud juhtimine. RahaPTS ei käsitle siiski täielikult detsentraliseeritud vahetusteenuseid. Lisaks, täielikult detsentraliseeritud vahetusteenused ei ole muude õigusaktidega kaetud. Täelik DeFi ei vasta traditsioonilistele vahetusteenustele väärtpaberituru seaduse (VPTS) ega ühisrahastusteenuste Direktiivi 2020/1503 alusel ning e-raha asutuste kriteeriumidele makseasutuste ja e-raha asutuste seaduse (MERAS) alusel.

Uurimistöö kolmandas küsimuses uuriti, mida tuleks teha piirkondades, kus puuduvad vastavad õigusnormid. Analüüsi käigus selgus, et lahendus võib olla tehniline. DeFi platvormid peaksid võtma vastu ennetavaid meetmeid, et tagada eeskirjade järgimine ja ennetada ebaseaduslikku tegevust tehnilisel tasandil. Kehtestatud reeglite ja eeskirjade järgimise tagamiseks tuleks kehtestada DeFi-protokollide käivitamise miinimumnõuded, mis aitaksid standardiseerida DeFi finantsvahetuse platvorme. DeFi tehnoloogia hoolsuskohustuste eeskirjade tõhus rakendamine on ülioluline pettuste ärahoidmiseks ja investorite kaitsmiseks. Hoolsuskohustuse eeskirjade tõhusaks rakendamiseks DeFi tehnoloogias on vaja tasakaalustada detsentraliseerimise eeliseid tarbijakaitse vajaduse ja regulatiivsete raamistike järgimisega. See nõuab sidusrühmade, poliitikakujundajate ja reguleerivate asutuste koostööd.

LIST OF REFERENCES

Books

1. Avgouleas, E. & Marjosola, H. (2022). *Digital Finance in Europe: Law, Regulation, and Governance*. Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110749472.
2. Harvey, C., Ramachandran, A., Santoro, J., Ehrsam, F., & Buterin, V. (2021). *DeFi and the Future of Finance*. Newark: John Wiley & Sons, Incorporated.
3. Motsi-Omoijiade, I.D. (2022). Cryptocurrency Regulation: A Reflexive Law Approach (1st ed.). Routledge. https://doi.org/10.4324/9781003254164.
4. Roukny, T. (2022). *Decentralized finance: information frictions and public policies: approaching the regulation and supervision of decentralized finance.* Luxembourg: Publications Office of the European Union. http://doi.org/10.2874/444494.

Scientific articles

1. Bertrand, A., Maxwell, W., & Vamparys, X. (2021). Do AI-based anti-money laundering (AML) systems violate European fundamental rights? International Data Privacy Law, 11(3), 276-293.
2. Caldarelli, G., & Ellul, J. (2021). The blockchain oracle problem in decentralized finance—A multivocal approach. Applied Sciences, 11(16), 7572.
3. Covarrubias, J., & Covarrubias, I. (2021). Different types of government and governance in the blockchain. Journal of Governance and Regulation, 10(1), 8-21.
4. Cumming, D., Johan, S., & Pant, A. (2019). Regulation of the Crypto-Economy: Managing Risks, Challenges, and Regulatory Uncertainty. Journal of Risk and Financial Management, 12(3), 126.
5. Datinsky, P. (2020). European Legal Regulation of Cryptocurrencies through the AML Scope. Public Governance, Administration and Finances Law Review, 5(1), 38-47.
6. De Vido, S. (2015). Anti-Money Laundering Measures Versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice. German Law Journal, 16(5), 1271-1292, p 1291.

7. Faqir-Rhazoui, Y., Arroyo, J., & Hassan, S. (2021). A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. Journal of Internet Services and Applications, 12(1).
8. Frajtova Michalikova, K., Poliakova, A. (2021). Decentralized finance. SHS Web of Conferences, 129, 3008.
9. Hardin, G. (1968). The Tragedy of the Commons. Science (American Association for the Advancement of Science), 162(3859), 1243-1248.
10. Harwick, C., & Caton, J. (2022). What's holding back blockchain finance? On the possibility of decentralized autonomous finance. The Quarterly Review of Economics and Finance, 84, 420-429.
11. Jensen, J., Von Wachter, V., & Ross, O. (2021). An Introduction to Decentralized Finance (DeFi). Complex Systems Informatics and Modeling Quarterly, (26), 46-54.
12. Kim, H., Kim, H., & Park, Y. (2022). Perpetual Contract NFT as Collateral for DeFi Composability. IEEE Access, 10, 126802-126814.
13. Kim, J. (2021). Regulation of decentralized systems: a study of Uniswap. Harvard Journal of Law & Technology, 35(1).
14. Kirimhan, D. (2023). Importance of anti-money laundering regulations among prosumers for a cybersecure decentralized finance. Journal of Business Research, 157, 113558.
15. Kiviat, T. (2015). Beyond bitcoin: issues in regulating blockchain transactions. Duke Law Journal, 65(3), 569-608.
16. Mohan, V. (2022). Automated market makers and decentralized exchanges: A DeFi primer. Financial Innovation (Heidelberg), 8(1), 1-48.
17. Nielsen, T. (2019). Cryptocorporations: a proposal for legitimizing decentralized autonomous organizations. Utah Law Review, 2019(5).
18. Nizovtsev, Y., Parfylo, O., Barabash, O., Kyrenko, S., & Smetanina, N. (2022). Mechanisms of money laundering obtained from cybercrime: The legal aspect. Journal of Money Laundering Control, 25(2), 297-305.
19. Ojog, S. (2021). The Emerging World of Decentralized Finance. Informatica Economica, 25(4/2021), 43-52.
20. Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. Journal of Cybersecurity (Oxford), 5(1), 1-11.
21. Pavlidis, G. (2021). Europe in the digital age: Regulating digital finance without suffocating innovation. Law, Innovation and Technology, 13(2), 464-477, 465.

22. Pupolizio, I. (2022). From Libra to Diem. The Pursuit of a Global Private Currency. Global Jurist, 22(2), 281-306.
23. Rueckert, C. (2019). Cryptocurrencies and fundamental rights. Journal of Cybersecurity (Oxford), 5(1).
24. Sai, B., Nikhil, R., Prasad, S., & Naik, N. (2023). A decentralised KYC based approach for microfinance using blockchain technology. Cyber Security and Applications, 1, 100009.
25. Salami, I. (2021). Challenges and approaches to regulating decentralized finance. AJIL Unbound, 115, 425-429.
26. Schueffel, P. (2021). DeFi: Decentralized Finance - An Introduction and Overview. Journal of Innovation Management, 9(3), I-XI.
27. Senarathne, C. (2019). Possible Impact of Facebook's Libra on Volatility of Bitcoin: Evidence from Initial Coin Offer Funding Data. Organizacijų Vadyba, 81(1), 87-100.
28. Stepanova, V., & Eriņš, I. (2021). Review of Decentralized Finance Applications and Their Total Value Locked. TEM Journal, 10(1), 327-333.
29. Suga, Y., Shimaoka, M., Sato, M., & Nakajima, H. (2020). Securing Cryptocurrency Exchange: Building up Standard from Huge Failures. Financial Cryptography and Data Security, 12063, 254-270.
30. Teomete Yalabik, F., & Yalabik, I. (2019). Anonymous Bitcoin v enforcement law. International Review of Law, Computers & Technology, 33(1), 34-52.
31. Trotz, E. (2022). Million dollar bash: a nuanced approach for calculating tax liability for participants in decentralized finance. Texas Tech Law Review, 54(3), 575-593.
32. Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: New challenges for compliance. Journal of Financial Crime, 30(1), 97-113.
33. Yeoh, P. (2020). Banks' vulnerabilities to money laundering activities. Journal of Money Laundering Control, 23(1), 122-135.
34. Zaccaroni, G. (2022). Decentralized Finance and EU Law: The Regulation on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology. European Papers, 2022 7(2), 601-613.
35. Zetzsche, D., Arner, D., & Buckley, R. (2020). Decentralized finance. Journal of Financial Regulation, 6(2), 172-203. https://doi.org/10.1093/jfr/fjaa010.

Other field-specific sources

1. A Deep Dive Into Security Token Offering (STO). (2023). Cryptoflies News. https://blog.cryptoflies.com/a-deep-dive-into-security-token-offering-sto/.
2. Anti-money laundering and countering the financing of terrorism legislative package. (2021). https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.
3. Concordium. https://concordium.com/.
4. Delivorias, A. (2021). Understanding initial coin offerings: A new means of raising funds based on blockchain. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)696167.
5. Digital finance package. (2020). https://finance.ec.europa.eu/publications/digital-finance-package_en.
6. Digital finance: agreement reached on European crypto-assets regulation (MiCA). (2022, June 30). [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/.
7. Estonian Financial Intelligence Unit (01.2022). Virtuaalvääringu teenuse pakkujatega seonduvad riskid Eestis. Rahapesu andmebüroo. https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvaaringu-tee.
8. Estonian Financial Intelligence Unit (2022). Rahapesu Andmebüroo väliskoostöö ülevaade 2021. https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#rahapesu-andmeburoo-
9. Estonian Financial Intelligence Unit (22.09.2020). Virtuaalvääringu teenuse pakkujate uuring. Rahapesu andmebüroo. https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b.
10. Ethereum Bug Bounty Program. Ethereum.org. https://ethereum.org.
11. Ethereum Foundation. Ethereum.org. https://ethereum.org/en/foundation/.
12. Ethereum price today, ETH to USD live, marketcap and chart. CoinMarketCap. https://coinmarketcap.com/currencies/ethereum/.
13. FATF (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris,

www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

14. FATF (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html.
15. FATF (2022). Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.
16. Financial Supervision Authority. DAO. https://www.fi.ee/en/finantsinspektsioon/innovatsioonikeskus/DAO.
17. Financial Supervision Authority. DeFi. https://www.fi.ee/en/finantsinspektsioon/innovation-hub/defi.
18. Financial Supervision Authority. The legal framework of initial coin offering in Estonia. https://www.fi.ee/en/investment/aktuaalsed-teemad-investeerimises/virtuaalraha-ico/legal-framework-initial-coin-offering-estonia.
19. Finnovating (2023). FinTech Global Vision 2023. https://finnovating.com/fintech-global-vision-report/.
20. Fritsch, R., Müller, M., & Wattenhofer, R. (2022). Analyzing Voting Power in Decentralized Governance: Who controls DAOs?.
21. Governance. Uniswap Protocol. https://uniswap.org/governance.
22. Internet Native Organization. https://internetnative.org/.
23. Introducing UNI. (2020). https://uniswap.org/blog/uni/.
24. Lätt, P. (2022). Decentralised autonomous organisations/DAOs in estonia. e-Residency. https://www.e-resident.gov.ee/blog/posts/daos-in-estonia/.
25. Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi) (National Bureau of Economic Research Working Papers No. 30006). https://doi.org/10.3386/w30006.
26. McLellan, L. (2018). Estcoin and sovereign cryptocurrencies: Not the future yet. Global Capital, 2018.

27. MONEYVAL (2022). Anti-money laundering and counter-terrorist financing measures. Estonia. Fifth Round Mutual Evaluation Report. https://rm.coe.int/moneyval-2022-11-mer-estonia/1680a9dd96.
28. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto Institute, Bitcoin.Org, 1–9. https://bitcoin.org/bitcoin.pdf.
29. New EU measures against money laundering and terrorist financing. (2023, March 28). [Press release]. https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing.
30. OECD (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications, OECD Paris.
31. Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., & Gervais, A. (2021). CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance. ArXiv.org.
32. The value is determined by using Coinmarketcap. Top DeFi Tokens by Market Capitalization. CoinMarketCap. https://coinmarketcap.com/view/defi/.
33. U.S. Securities and Exchange Commission (SEC). https://www.sec.gov/about/what-we-do.
34. Uniswap App. https://app.uniswap.org.
35. Uniswap Labs Terms of Service. (2023). https://uniswap.org/terms-of-service.
36. Who we are. Financial Action Task Force (FATF). https://www.fatf-gafi.org/en/the-fatf/who-we-are.html.
37. World Economic Forum. (2021). Decentralized Finance: (DeFi) Policy-Maker Toolkit. https://www.weforum.org/whitepapers/decentralized-finance-defi-policy-maker-toolkit/.
38. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.
39. Zetzsche, D., Annunziata, F., Arner, D., & Buckley, R. (2021). The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy. Capital Markets Law Journal, 16(2), 203-225.

EU and international legislation

1. Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, L 347/1.

2. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, L 156/43.
3. COM(2018) 109 final. Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the regions. FinTech Action plan: For a more competitive and innovative European financial sector.
4. COM(2021) 423 final. Proposal for a 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.
5. COM(2020) 591 final. Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU.
6. COM(2020) 593 final. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.
7. COM(2020) 594 final. Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology.

Estonian legislation

1. Money Laundering and Terrorist Financing Prevention Act. RT I, 17.11.2017, 2.
2. Payment Institutions and E-money Institutions Act. RT I 2010, 2, 3.
3. Securities Market Act. RT I 2001, 89, 532.
4. UMIVS draft explanation, 2021. https://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#FxmJFP8M.

Estonian court decision

RKHKo 3-3-1-75-15.

APPENDIX 1. NON-EXCLUSIVE LICENCE

A non-exclusive licence for reproduction and publication of a graduation thesis.[209]

I , Jaanika Ansip,

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

Decentralised finance exchange services through an Estonian and European Union legal perspective, supervised by Aleksi Kajander,

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

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

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

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

09.05.2023 (date)

[209] [1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period