IGOR INACIO

DECENTRALIZED FINANCE, NON-FUNGIBLE TOKENS AND MONEY LAUNDERING: IS THE EUROPEAN UNION LEGAL FRAMEWORK READY TO ADDRESS FINANCIAL CRIME RISKS ARISING FROM THE CRYPTO BUSINESS WHILE FOSTERING INNOVATION?

Dissertation to obtain a Master's Degree in Law, in the specialty of Business Law and Technology

Supervisor: Dr. Athina Sachoulidou, Professor of the NOVA School of Law

December, 2022

ACKNOWLEDGEMENTS

I would like to thank the following people, without whom I would not have been able to conclude this research and made it through my Master's degree:

I want to thank my wife Mia, for always supporting me in all my projects, encouraging me to always do my best to contribute to a better world, and for being my safe harbor protecting me from the storms of life. We make the best team!

I want to thank my supervisor, mentor, and friend Athina for encouraging me to follow my calling in fighting financial crime and for always being there when I needed guidance or encouragement. You are a role model!

I want to thank Professors Yakovina, Fabrizio, Agata, and Miguel for awakening in me the academic flame that had long been dormant, for the inspiring classes, and for believing in my potential.

Finally, I would like to thank the Trace Consortium and WhatNext.Law for the invaluable support and learning I have had while being part of their research teams.

ANTI-PLAGIARISM STATEMENT

I hereby declare for all intents and purposes that I am the sole author of this thesis and the use of contributions or texts of other authors are duly referenced throughout my work.

TABLE OF CONTENTS

TABLE OF ACRONYMS

AML – Anti-money laundering

AMLD5 – The 5th EU Anti-Money Laundering Directive

AMLD6 – The 6th EU Anti-Money Laundering Directive

ART – Asset-referenced token

ATM – Automated teller machine

CARF – OECD's Crypto-Asset Reporting Framework

CASP – Cryptoasset service provider

CDD – Customer Due Diligence

CeFi – Centralized finance

CRS – OECD's Common Reporting Standard

CTF – Counter-terrorism financing

DAC – EU Directive on Administrative Cooperation

DAO – Decentralized autonomous organization

DeFi – Decentralized finance

DEX – Decentralized exchange

DLT – Distributed ledger technology

EMT – E-money token

EU – European Union

FATF – Financial Action Task Force

FI – Financial institution

FIU – Financial intelligence unit

ICO – Initial coin offering

KYC – Know Your Customer

MiCA – Proposal for a Regulation on Markets in Cryptoassets

MiFID – EU Markets in Financial Instruments Directive

ML – Money laundering

NFT – Non-fungible token

OECD – Organization for Economic Co-operation and Development

P2P – Peer-to-peer

PEP – Politically exposed persons

R&D – Research and development

RBA – Risk-based approach

SBT – Soul-bound token

TF – Terrorist financing

UBO – Ultimate beneficial ownership

VA – Virtual asset

VASP – Virtual asset service provider

VCSP – Virtual currency service provider

ABSTRACT

EN: This thesis offers an analysis of Decentralized Finance underpinnings, particularly Non-Fungible Tokens and the challenges these innovations may pose over the European Union AML/CTF legal framework. On the one hand, the thesis will analyze the changes these innovations may bring to the art market and creative industry. On the other hand, it will focus on the financial crime risks arising from the increased ease to layer the crime proceeds on the blockchain.

PT: Esta tese oferece uma análise dos fundamentos da *Decentralized Finance*, particularmente das tokens não fungíveis e dos desafios que estas inovações representam para o arcabouço legal da União Europeia contra o branqueamento de capitais e financiamento do terrorismo. Por um lado, a tese irá analisar as mudanças que estas inovações podem trazer ao mercado da arte e à indústria criativa. Por outro lado, centrar-se-á nos riscos de crime financeiro que advêm da maior facilidade em ocultar os produtos do crime na *blockchain*.

Keywords: *Decentralized Finance - Cryptoassets - Non-Fungible Tokens - Blockchain - Anti-Money Laundering - Counter Terrorist Financing - Tax Evasion - Financial Crime - EU Laws - EU AML Directives*

1 Introduction

Particularly in 2021 and early 2022, non-fungible tokens (NFTs) became a global trend by taking the spotlight of the financial market and offering a disruptive vision to the art and collectibles market. Last year, the market cap of NFTs was estimated at USD 40BN[1], which demonstrated the investment potential attached to these tokens. During that year and until today, several projects involving NFTs have been created and their essentially speculative nature seems to be slowly being replaced by a more utility-oriented nature of these assets.[2]

The assets represented by NFTs may be exchanged in special marketplaces (e.g. OpenSea and Nifty Gateway), creating a process of tokenization from reality to digital. NFTs can be used to create verifiable digital ownership over several assets - crypto art, digital collectibles, online games, intellectual property rights, real estate, jewelry, vehicles, licenses, financial documents, among others - which may indicate its versatility as a cryptoasset and its disruptive potential on various markets.[3]

Innovative instruments like NFTs were only possible due to the advent of Decentralized Finance (DeFi). On the one hand, NFTs may create wealth by helping artists, collectors, and interested parties negotiate in a secure and decentralized environment. On the other hand, concerns related to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) may arise due to the current weak regulation on cryptoassets and the anonymity offered by distributed ledger technology (DLT)[4]. Market participants involved in trading NFTs may also face potentially high costs for non-compliance if the legislation is not clear enough about the legal status of NFTs and in establishing the legal requirements to operate in this novel market.

[1] Bloomberg. 2022. NFT Market Surpassed $40 Billion in 2021, New Estimate Shows. Accessed on 04.12.2022. Available at URL <https://www.bloomberg.com/news/articles/2022-01-06/nft-market-surpassed-40-billion-in-2021-new-estimate-shows?leadSource=uverify%20wall>.

[2] BUTERIN, Vitalik et. al. 2022. P. 02-03. *Decentralized Society: Finding Web3's Soul*. Accessed on 16.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763>.

[3] POPESCU, Andrei-Dragos. 2021. Non-Fungible Tokens (NFT) - Innovation beyond the craze. Proceedings of Engineering & Technology Journal - IBEM 2021. P. 26. Accessed on 04.12.2022. Available at URL <https://www.academia.edu/50920483/Non_Fungible_Tokens_NFT_Innovation_beyond_the_craze>.

[4] Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. P. 09. Accessed on 30.11.2022. Available at URL <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf>.

Being an emerging technology in rapid evolution, the regulation related to DeFi and cryptoassets has not yet been developed enough to address effectively the concerns arising from this technology, especially regarding money laundering (ML), terrorist financing (TF) and financial crimes practiced in the blockchain.

This thesis aspires to be part of the debate taking place between academia, public and private agencies to identify the best path to be taken in the legal analysis of cryptoassets (particularly NFTs) so that they are used for licit purposes and can generate wealth for the groups involved in their trade. The timing of this study is also a decisive factor, as the public debate on cryptoassets and AML/CTF is at its peak in the EU agencies, financial market and specialized media.

To accomplish this goal, the following chapters will expose: a historical background for cryptoassets with an emphasis on NFTs; the definitions and concepts pertaining DeFi and cryptoassets; the crypto regulatory gap and financial crime risks arising from cryptoassets; the current and upcoming crypto regulatory framework with an emphasis on the EU legislation and international legal provisions that may be applicable in the EU; and the research questions this work aims to answer.

2 Brief History of DeFi and NFTs

Even though there is no official or agreed-upon date when Decentralized Finance (DeFi) was born, a few important events were crucial to making it possible. The first event that worked as an enabler for DeFi was the creation of Bitcoin in 2009 by Satoshi Nakamoto[5], a pseudonym used by the person(s) that developed the referred cryptocurrency.

The creation of Bitcoin paved the way for the creation of Ethereum and its associated digital coin (Ether/ETH) by Vitalik Buterin[6] in 2015. Ethereum is a default blockchain in which the main DeFi protocols are built. Bitcoin's disruptiveness challenged the financial system and may have contributed permanently to the change of how investments are performed in the financial market. Nevertheless, it was built on a simple and limited language - Script - which could not provide Bitcoin with complex functionalities and services like lending, borrowing, funding and trading. Bitcoin could be sent anywhere in the world but only with Ethereum DeFi started presenting the robustness required from a financial system.

Following the creation of Ethereum, the Initial Coin Offering (ICO) became one of the first use cases of DeFi. Instead of raising money via traditional ways (e.g. venture capital firms), new DeFi projects could offer their tokens in exchange for ETH to capitalize on their projects built on Ethereum. On the one hand, ICOs allowed great projects to be launched (e.g. Maker, Aave and Ox) and become some of the main DeFi projects at the time. On the other hand, they contributed to the period known as "ICO Mania[7]", during which many projects were funded without providing any further documentation than a few whitepaper pages, which may have contributed to fraud schemes that undermined the credibility of the ICO.

---

[5] HAYES, Adam. 2022. *Who is Satoshi Nakamoto?* Accessed on 08.10.2022. Available at URL <https://www.investopedia.com/terms/s/satoshi-nakamoto.asp#:~:text=Satoshi%20Nakamoto%20is%20a%20pseudonym,not%20been%20heard%20from%20since.>.

[6] DELVENTHAL, Shoshanna. 2019. *Be Wary of Cryptocurrencies: Ethereum Founder*. Accessed on 08.10.2022. Available at URL <https://www.investopedia.com/news/cryptocurrencies-could-drop-nearzero-any-time-ethereum-founder/>.

[7] FINEMATICS - DECENTRALIZED FINANCE EDUCATION. *History of DeFi - From Inception to 2021 and Beyond*. Accessed on 08.10.2022. Available at URL: <https://finematics.com/history-of-defi-explained/>.

In November 2018, the initial version of Uniswap was made available on Ethereum. Uniswap, to this day, is one of the most important DeFi projects. Relying on a smart contract system[8], Uniswap allowed their users to exchange various cryptoassets with fundamental safety guarantees for all parties interacting on their platform.

On 12 March, 2020, due to fears related to the global pandemic of Covid-19, DeFi went through its first significant stress test in a period known as Black Thursday[9]. Back then, cryptoassets prices dropped between 50% to 60% in less than 24h and the Ethereum gas fees[10] raised to the highest until that time as a result of multiple users trying to increase collateral with loans and/or trading different assets. This devaluation, however, was not exclusive to DeFi. Black Thursday was a reflection of the financial instability of the initial period of the pandemic leveraged by the 2020 stock market crash[11] and the volatility of cryptoassets and their developing financial system. Lastly, despite its severity, this event resulted in the strengthening of DeFi which enabled a period of renewed growth known as DeFi Summer.

DeFi Summer is the term used to describe the period from March to September 2020 when many interesting projects were created on the Ethereum platform and the value of cryptoassets reached an all-time high. Among these projects, the following can be highlighted: Compound (lending and borrowing), Yearn Finance and Ampleforth (lending, trading and investments), and Sushiswap (exchange of cryptoassets enabled by smart contracts). In this period of time, the total value locked (TVL) in DeFi went from $800MN to $10BN, a more than tenfold increase in value.

After the period of significant growth, cryptoassets alternated between periods of devaluation and appreciation, a trend that continues to this day. The TVL in DeFi went

[8] UNISWAP DOCS. Smart Contracts. Accessed on 08.10.2022. Available at URL <https://docs.uniswap.org/protocol/V2/concepts/protocol-overview/smart-contracts>.

[9] FRANGELLA, Emilio. 2019. *Crypto Black Thursday: the Good, the Bad and the Ugly*. Accessed on 08.10.2022. Available at URL <https://medium.com/aave/crypto-black-thursday-the-good-the-bad-and-the-ugly-7f2acebf2b83>.

[10] FRANKENFIELD, Jake. 2022. *Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain*."A fee or cost required to conduct a transaction on the open-source Ethereum blockchain, denominated in small fractions of the cryptocurrency Ether (ETH)". Accessed on 15.10.2022. Available at URL <https://www.investopedia.com/terms/g/gas-ethereum.asp>.

[11] FRAZIER, Liz. FORBES. 2021. *The Coronavirus Crash of 2020 and the Investing Lesson it Taught Us*. Accessed on 08.10.2022. Available at URL <https://www.forbes.com/sites/lizfrazierpeck/2021/02/11/the-coronavirus-crash-of-2020-and-the-investing-lesson-it-taught-us/?sh=67dd269546cf>.

from $601MN by the start of 2020 to $239BN in April 2022[12]. Being a new and disruptive technology, it is predictable and expected that its value will fluctuate. There is still much speculation around the financial value of cryptoassets but the creative and disruptive value of DeFi has already demonstrated that it is a technology that is here to stay.

Since NFTs are stored in a distributed ledger or blockchain and may represent ownership of goods like artwork, collectibles, games and other digital or physical assets, they have become one of the most promising assets in DeFi. Combined with other DeFi products, NFTs may be used, among other possibilities, for investing, as in-game currencies, and for liquidity mining (a process in which cryptoassets are lent to a decentralized exchange in return for rewards).

In 2012, a few years before Ethereum's creation, Meni Rosenfeld, a mathematician and Bitcoin enthusiast, drafted a paper[13] that introduced the 'Colored Coins' concept for the Bitcoin blockchain. The referred paper described a series of methods to represent, manage and prove ownership of assets in the blockchain. Despite the technical limitations of the Bitcoin blockchain that prevented the Colored Coins from achieving its full potential, the project paved the way for the creation of the first NFT in 2014 by the digital artist Kevin Mccoy via the 'Quantum' project.[14]

In 2014, the Counterparty platform (Bitcoin 2.0) was built, a peer-to-peer (P2P) financial platform and a distributed, open-source internet protocol built on top of the Bitcoin blockchain that enabled the creation of digital assets like NFTs. Several projects, among which the 'Rare Pepes' NFTs[15], were created via Counterparty.

As mentioned above, the Bitcoin blockchain was not optimal for the creation of NFTs. In 2017, the creators and traders shifted to Ethereum encouraged by the

[12] AMBERDATA. *DeFi and the Transformation of Institutional Finance*. Accessed on 08.10.2022. Available at URL <https://blog.amberdata.io/defi-and-the-transformation-of-institutional-finance?utm_medium=email&_hsmi=210559080&_hsenc=p2ANqtz--4jBnJwnHdMtyADjUnlFmz3EWc60XJyaMGdl1NYqYtV3SX4KRwULMEajGaUK9DCcdv2vEuHTmoCtizJjEAq1tmaLmMOQ&utm_content=210559080&utm_source=hs_email>.

[13] ROSENFELD, Meni. 2012. *Overview of Colored Coins*. Accessed on 15.10.2022. Available at URL <https://allquantor.at/blockchainbib/pdf/rosenfeld2012overview.pdf>.

[14] ZENO, A. 2022. The beginning of NFTs - A Brief History of NFT Art. Accessed on 15.10.2022. Available at URL <https://www.zenofineart.com/blogs/news/the-beginning-of-nfts-a-brief-history-of-nft-art>.

[15] MARCOBELLO, Mason. 2022. *How Rare Pepes NFTs Reclaimed Pepe the Frog - And Why They Remain Relevant*. Accessed on 15.10.2022. Available at URL <https://decrypt.co/95528/how-rare-pepe-nfts-reclaimed-pepe-the-frog-and-why-they-remain-relevant>.

introduction of a set of token standards that would allow them to create, issue and deploy tokens in the blockchain. Soon after the shift to Ethereum, several projects like the CryptoPunks[16], CryptoKitties[17], Decentraland[18] and Axie Infinity[19] were created and could demonstrate that the purpose of NFTs was not only to replicate memes that were successful on the internet, but rather a type of cryptoasset that could be worth millions of dollars and serve many other purposes. For instance, Decentraland is a virtual reality (VR) decentralized platform built on the Ethereum blockchain that offers an open-world gaming platform in the metaverse, and Axie Infinity, the current leader in NFT gaming, introduced the play-to-earn (P2E) business model in which players are rewarded for adding value to the game's world or ecosystem.

To commercialize and integrate the emerging NFT market, several trading platforms have been created, including, for instance: OpenSea, which is currently the largest marketplace for NFTs representing digital art, music, domain names, collectibles and trading cards; Portion, which is an NFT platform that connects NFTs to other DeFi assets; and Niftex, a platform that allows users to buy pieces of NFTs or "shards", which are tokens representing a piece of the full NFT.

2021 was the year in which NFTs gained great popularity and became one of the most recurrent topics of discussion not only in the groups and media specialized in blockchain but also in academia, the business community, the financial market and the general public. According to nonfungible.com, an NFT data resource to discover, analyze and track digital assets, the NFTs trading business generated $17,6BN in that year, an increase of 21,000% when compared to 2020[20]. Moreover, the NFT business, particularly when it comes to crypto art, was not restricted to specialized platforms but had also conquered a position in traditional auction houses such as Sotheby's and Christie's. For

[16] LEE, Edward. 2021. *The Cryptic Case of the CryptoPunks Licenses: The Mystery Over the Licenses for CryptoPunks NFTs*. Accessed on 15.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3978963>.

[17] SERADA, A. et al. 2020. *CryptoKitties and the new ludic economy : how blockchain introduces value, ownership, and scarcity in digital gaming*. Accessed on 15.10.2022. Available at URL <https://osuva.uwasa.fi/bitstream/handle/10024/10686/Osuva_Serada_Sihvonen_Harviainen_2020a.pdf;jsessionid=71D6699B3B6844B05D4172DEA4633E70?sequence=2>.

[18] ORDANO, Esteban. 2017. Decentraland Whitepaper. Accessed on 15.10.2022. Available at URL <https://decentraland.org/whitepaper.pdf>.

[19] BARLOW, Justin. 2021. Axie Infinity: A Deep Dive. Accessed on 15.10.2022. Available at URL <https://research.thetie.io/axie-infinity/>.

[20] Nonfungible.com. 2021. *Yearly NFT Market Report.* Accessed on 15.10.2022. Available at URL <https://nonfungible.com/reports/2021/en/yearly-nft-market-report>.

instance, at that time Christie's set the record for the most expensive artwork offered online when it sold the NFT 'Everydays: The First 5000 Days'[21].

According to a study conducted by Footprint Analytics[22], one of the main blockchain analytics platforms, the first quarter (Q1) of 2022 maintained the growth trend of the NFT market, producing a total of $19BN in transactions. In the second quarter (Q2), the volume of transactions involving NFTs dropped to $11BN. This drop was caused mainly by a slowdown of investments in the metaverse and a massive sell-off of cryptoassets[23] following the turbulence in global financial markets and the political and security uncertainties related to the war in Ukraine[24].

Historically, investors in times of crisis tend to move their funds into lower-risk assets (e.g. gold and US dollars). Bearing this in mind, it was expected that the high-risk market of NFTs would follow the global financial market trend of devaluation. It is difficult to predict the trend for the end of 2022 onwards. Economists at Chainanalysis, a leading blockchain data analysis platform, argue that the recent crisis in the NFT market will contribute to moving the market away from NFTs and cryptoassets without additional utility[25]. This could lead to innovative use cases like gaming, royalties, proof of ownership of real-life assets or even a shift towards the real estate sector, ESG, healthcare, education and entertainment.

NFTs could also become a less financial and more utilitarian asset, a possibility advocated by Vitalik Buterin. The Ethereum founder argued in his May 2022 whitepaper that Web3 is currently focused on transferable and financialized assets rather than encoding social relations of trust. To address this issue, the author proposed the creation of

[21] Christie's. 2021. *A Record Breaking Year at Christie's: 2021 in numbers*. Accessed on 15.10.2022. Available at URL <https://www.christies.com/features/christies-auction-highlights-2021-12019-1.aspx?sc_lang=en>.

[22] Footprint Analytics. *2022 Q2 NFT Industry Report*. Accessed on 15.10.2022. Available at URL <https://www.footprint.network/@KikiSmith/NFT-Dashboard-KikiSmith?date_filter=2022-01-01~2022-06-30>.

[23] WANG, Tracy. Coindesk. 2022. *Crypto Sell-Off Wipes $700B From Industry Market Cap So Far in 2022*. Accessed on 15.10.2022. Available at URL <https://www.coindesk.com/markets/2022/01/24/crypto-sell-off-wipes-700b-from-industry-market-cap-so-far-in-2022/>.

[24] OECD. 2022. *Paying the Price of War*. Accessed on 15.10.2022. Available at URL <https://www.oecd.org/economic-outlook/september-2022/>.

[25] WILLIAMS, Lara. Investment Monitor. 2022. *The NFT Market Has Collapsed (But That May Not Be a Bad Thing)*. Accessed on 16.10.2022. Available at URL <https://www.investmentmonitor.ai/crypto/nft-market-collapse-cryptocurrency-value>.

Soul Bound Tokens[26] (SBTs), a type of NFT that retains the proof of ownership functionality but is focused on addressing interpersonal or contractual relationships, such as undercollateralized lending or simple contracts like an apartment lease.

The idea of non-transferable tokens (NTTs) is further developed by Certi.NFT, a startup that leverages blockchain technology to generate certification in the form of NFTs, enabling degrees and accreditations to be fully unique, tamper-proof and verifiable. Another example of the usefulness of NTTs could be to prove that a certain individual participated in a special event, e.g. a World Cup final or a concert by a globally known band, and the token could serve as a trophy or collectible that would portray a special moment in that person's life.

The NFT market crash mentioned above, despite imposing losses for investors who seek financial reward for their involvement in the market, may contribute to NFTs generating not only financial return but effectively contributing to building a Decentralized Society[27] (DeSoc). Currently, it is not possible to predict the future of NFTs, but if the trends advocated by the main players in the business are confirmed, we could see a less speculative market involved in building a sustainable ecosystem for NFTs and, above all, in providing usefulness and security for business and interpersonal relationships on the blockchain.

[26] BUTERIN, Vitalik et. al. 2022. P. 02-03. *Decentralized Society: Finding Web3's Soul*. Accessed on 16.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763>.

[27] Id. P. 01.

3 Definitions and Concepts

3.1 Decentralized Finance and Distributed Ledger Technology

Popescu states that Decentralized Finance (DeFi), also known as 'open finance', "is a set of blockchain/distributed ledger-based financial services and applications intended to augment or replace the existing financial system, which is comparatively referred to as Centralized Finance (CeFi)[28]". Most of the DeFi initiatives have been built on the Ethereum network, while others on permissionless blockchains[29] such as Bitcoin.

DeFi is a disruptive movement that proposes an open and transparent alternative to the current financial system and the services offered therein (e.g. trading, savings, loans and insurance). One of the few requirements to access DeFi services is to have access to an internet connection and a smartphone or computer. By reducing the entry prerequisites into the financial system, DeFi may shift traditional financial services to an open-source, decentralized environment. Instead of banks and financial institutions (FIs), the main players in DeFi are Decentralized Autonomous Organizations[30] (DAOs) and their members that exercise control over the organization through voting rights granted to the holders of governance tokens[31].

In a progressive view of DeFi, Buterin went even further by proposing that DAOs could transcend an essentially capitalist vision in which profit is the main goal and evolve into a Decentralized Autonomous Community (DAC) built on the blockchain. In this community, all members would have an equal share in the decision-making and could, in theory, decide the course of a given project.

---

[28] POPESCU, Andrei-Dragos. 2020. P. 316. *Decentralized Finance (DeFi) - The Lego of Finance*. P. 316. Accessed on 21.10.2022. Available at URL <https://www.academia.edu/44523671/DECENTRALIZED_FINANCE_DEFI_THE_LEGO_OF_FINANCE>.

[29] ZETZSCHE D. et al. 2017. Pp. 11-12. "Permissioned systems are essentially private networks where data authorization depends upon the agreement of multiple pre-defined servers. (…) In contrast, permissionless blockchains such as Bitcoin operate on public domain software and allow anyone who downloads and runs the software to participate". Accessed on 21.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214>.

[30] BUTERIN, Vitalik. 2014. P. 23. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed on 21.10.2022. Available at URL <https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf>.

[31] HOWELL, James. 101 Blockchains. 2022. *What Are Governance Tokens and Why do They Matter?* Accessed on 21.10.2022. Available at URL <https://101blockchains.com/governance-tokens/>.

One of DeFi's main pillars resides in the reliability of smart contracts to confer security and transparency to the transactions made on the blockchain. Generally, a smart contract is a programmable contract capable of self-execution and enforcement when certain requisites are met[32]. It consists of an agreement between the interested parties that hold each party responsible for the contract. Since they are built on the blockchain, smart contracts inherit its immutability, transparency and increased security features.

Since data stored in a DLT such as the blockchain is equally spread across all storage points (nodes) that are connected and store all data simultaneously, a cyber-attack on a given DLT would need to manipulate all nodes/servers necessary to achieve consensus, a process in which the members of the DLT reach agreement about the data written on the ledger. Thus, when compared to a centralized ledger that relies on a hub-and-spoke model in which data originates in the hub and/or is sent to the hub for distribution, data stored in the DLT is harder to manipulate[33].

Additionally, one of the main principles of DLT lies in the immutability principle (namely, once you execute a transaction, it cannot be erased or tampered with) and this could provide an audit trail to identify the parts involved in questionable affairs[34]. Transaction details in the blockchain may not be immediately identifiable and the complexity of this emerging technology may confer apparent anonymity to users that could exploit the platform in an unlawful way. However, since most of the blockchains are open-source, to investigate blockchain transactions, one would only need the proper tools and resources to uncover potential illicit activities (e.g. Chainalysis).

When compared to traditional financial services, DeFi may bring significant benefits through smart contracts[35] and DLTs[36]. As it grows and matures, deploying

[32] SADIKU, Matthew et. al. 2018. Journal of Scientific and Engineering Research. *Smart Contracts: A Primer*. Accessed on 21.10.2022. Available at URL <https://www.researchgate.net/publication/326752872_Smart_Contracts_A_Primer#:~:text=A%20smart%20contract%20is%20a,ever%20occurred%20in%20the%20network.>.

[33] ZETZSCHE D. et. al. 2017. *The Distributed Risks of Distributed Ledgers: Legal Risks of Blockchain*. P. 11. Accessed on 21.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214>.

[34] LYONS T. et. al. 2019. *Regulatory Framework of Blockchains and Smart Contracts*. P. 14. Accessed on 21.10.2022. Available at URL <https://www.researchgate.net/publication/344338974_LEGAL_AND_REGULATORY_FRAMEWORK_OF_BLOCKCHAINS_AND_SMART_CONTRACTS>.

[35] FRANKENFIELD, Jake. Investopedia. 2022. *What Are Smart Contracts on the Blockchain and How They Work*. "A smart contract is a self-executing contract with the terms of the agreement between buyer and

financial applications or products will become less complex and cheaper. That, in turn, may lead to reduced operational costs and lower entry barriers. By removing financial intermediaries, reducing costs, and improving security and transparency, the DeFi movement may permanently change the global financial system.

3.2 Cryptoassets

The Proposal for a Regulation on Markets in Cryptoassets (MiCA) states that a cryptoasset is a digital representation of value or rights that may be transferred and stored electronically via distributed ledger technology or similar technology[37]. Broadly, cryptoasset is a blanket term created to define assets issued in the blockchain/DLT.

Concerning the definition of cryptoassets, MiCA affirms that any definition in this regard should correspond to the definition of virtual assets (VAs) provided for in the recommendations of the Financial Action Task Force (FATF). Those recommendations[38], lastly updated in March 2022, state that a virtual asset is "a digital representation of value that can be digitally traded or transferred and may be used for payment or investment purposes".

As it is an emerging technology, there is yet no concrete delimitation about the types of assets that can qualify as cryptoassets. The Canadian Securities Administrators (CSA), an organization whose objective is to improve, coordinate, and harmonize

seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism". Accessed on 21.10.2022. Available at URL <https://www.investopedia.com/terms/s/smart-contracts.asp>.

[36] ZETZSCHE. 2017. Pp. 10-11. "DLT or Distributed Ledger Technology, generally speaking, is a digital system for recording the transactions of its assets which database exists across several locations or among multiple participants. Unlike centralized ledgers, where the data is stored in the ledger itself and a trusted administrator of the ledger maintains it, in DLTs the data storage points (nodes) are all connected to each other and store all data simultaneously". Accessed on 21.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214>.

[37] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final. Article 3(2).

[38] FATF (2012-2022). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Accessed on 23.10.2022. Available at URL <www.fatf-gafi.org/recommendations.html>.

regulation of the Canadian capital markets, proposed an interesting division[39] for the various types of cryptoassets, namely cryptocurrencies, crypto-related funds and tokens.

Cryptocurrency is a type of digital/virtual currency held as a record written in the blockchain. The Directive (EU) 2018/43 amended the 5th Anti-Money Laundering Directive (AMLD5) in May 2018 to add a definition for virtual currencies. According to article 3(18) of the AMLD5, virtual currencies are digital representations of value that are not issued or guaranteed by a central bank or public authority, are not necessarily attached to a legally established currency, and do not have the legal status of currency or money. Moreover, virtual currencies should be accepted by natural or legal persons as exchangeable assets which may be transferred, stored and traded electronically[40]. Given this definition, cryptocurrencies are necessarily virtual currencies but not all virtual currencies may be considered cryptocurrencies.

The crypto-related funds may be divided into three subtypes of cryptoassets, namely cryptocurrency funds, cryptocurrency exchange-traded funds (ETF) and blockchain funds. The cryptocurrency funds consist of cryptocurrency investment funds that allow the indirect purchasing, owning and trading of crypto[41]. A cryptocurrency ETF works similarly to a traditional ETF,[42] but instead of keeping track of an index, sector or commodity, it tracks cryptocurrencies. A blockchain fund is similar to a regular investment fund that invests in a particular sector of the economy or industry, except that its goal is to invest specifically in the crypto industry or companies that operate with blockchain technology.

[39] Canadian Securities Administration. *Types of Crypto Assets*. Accessed on 23.10.2022. Available at URL <https://www.securities-administrators.ca/investor-tools/crypto-assets/types-of-crypto-assets/>.

[40] 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. Article 3(18). Accessed on 23.10.2022. Available at URL <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843>.

[41] ROSENBERG, Eric. Investopedia. 2022. How to Invest in Crypto without Buying Crypto. Accessed on 23.10.2022. Available at URL <https://www.investopedia.com/indirect-crypto-investment-6386330>.

[42] CHEN, James. Investopedia. 2022. *What Is an Exchange-Traded Fund (ETF)?* "An exchange-traded fund (ETF) is a type of pooled investment security that operates much like a mutual fund. Typically, ETFs will track a particular index, sector, commodity, or other assets, but unlike mutual funds, ETFs can be purchased or sold on a stock exchange the same way that a regular stock can. An ETF can be structured to track anything from the price of an individual commodity to a large and diverse collection of securities. ETFs can even be structured to track specific investment strategies". Accessed on 23.10.2022. Available at URL <https://www.investopedia.com/terms/e/etf.asp>.

Several types of tokens are issued on the blockchain, among which one may highlight utility tokens, security tokens and non-fungible tokens (NFTs). According to MiCA, a utility token is a cryptoasset intended to provide digital access to a good or service available in the blockchain and is normally only accepted by the issuer of that given token.

Security tokens represent or provide rights to a class of financial assets that are considered to be securities, such as bonds, shares, options or warrants[43]. Additionally, a security token usually represents a right to financial return and claim on the token issuer and entitles its holder to rights similar to those guaranteed by "classical" securities, which are fungible and negotiable financial instruments that hold monetary value and are normally used to raise capital in public and private markets.

Concerning the types of cryptoassets, Zetzsche[44] proposes they are divided into three categories: utility tokens, security/financial/investment tokens and currency/payment tokens. These three categories are currently followed a handful of European financial institutions such as: the Swiss Financial Market Supervisory Authority (FINMA) in the new Swiss DLT Law of 2020[45]; the 2019 Maltese regulation on cryptoassets; and the 2020 Liechtenstein Token and Trusted Technology Service Provider Act (TVTG).

3.3 Non-Fungible Tokens (NFTs)

To define NFTs, one should first define the concept of fungibility. An asset is considered fungible if it can be replaced by an identical one in terms of quality and quantity. The most common example of a fungible asset is money. A non-fungible asset cannot be substituted for an identical item given the intrinsic individuality of the good itself (e.g. art works)[46].

---

[43] CHANCE, Clifford. 2020. *Security Token Offerings - A European Perspective on Regulation*. P. 4. Accessed on 23.10.2022. Available at URL <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/security-token-offerings-a-european-perspective-on-regulation.pdf>.

[44] ZETZSCHE, DIRK A. et al.2020. University of Luxembourg Law Working Paper Series No. 2020-018. The Markets in Crypto-Assets Regulation(MICA) and the EU Digital Finance Strategy. Accessed on 18.11.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725395>.

[45] Swiss Financial Market Supervisory Authority. 2019. Federal Council wants to further improve framework conditions for DLT/blockchain. Accessed on 18.11.2022. Available at URL <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-77252.html>.

[46] EU Blockchain Observatory and Forum. *NFT – Legal Token Classification*. P. 2. Accessed on 21.10.2022. Available at URL <https://www.eublockchainforum.eu/sites/default/files/research-paper/EUBOF%20-%20NFT%20-%20Token%20Classification%20Latam.pdf>.

NFTs can be defined as a representation of a unique (usually but not necessarily digital) asset that cannot be changed or traded for another NFT of the same type. It is also a digital certificate of authenticity that cannot be replicated. NFTs are stored in a distributed ledger or a blockchain[47] and are used to prove ownership of unique assets. Due to the structure of blockchain technology, this proof of ownership is always available, immutable, and guarantees that the given asset has a unique owner[48].

Unlike fungible assets usually built according to Ethereum Request for Comments No. 20 (ERC20) guidelines, NFTs are created following ERC721, a standard set of rules for creating tokens, so that they can work properly and interact correctly with other assets in the blockchain. ERC721 allows developers to tokenize the ownership of any type of data, confers to each token a unique and identifiable identity and guarantees the token's indivisibility[49].

The most common and visible example of the disruptive power of NFTs lies in the digital art market. As mentioned above, NFTs may revolutionize the art market and change the way profits from this activity are divided among the different market participants. Chevet[50] states that NFTs and blockchain technology may contribute to a power shift in the art market by giving creators greater freedom and profitability over their creations.

Currently, digital art creators can create content more easily and distribute it directly or self-publish it, contributing to the reduction of entry barriers in the art market. Additionally, they can have access to a higher income by, for example, embedding the NFT into a smart contract that ensures the creator will receive a given percentage for each subsequent sale of their work.

---

[47] ZETZSCHE. 2017. P. 11. "'Blockchain' refers to how data are stored on the ledger. Rather than being stored individually, data are stored in a block bundled with other data. The block serves as the container of multiple data points, and all blocks are stored in a specific order (the 'chain')".

[48] POPESCU, Andrei-Dragos. 2021. *Non-Fungible Tokens (NFT) - Innovation beyond the craze*. P.26. Accessed on 21.10.2022. Available at URL <https://www.academia.edu/50920483/Non_Fungible_Tokens_NFT_Innovation_beyond_the_craze>.

[49] IREDALE, Gwyneth. 101 Blockchains. 2021. ERC20 Vs. ERC721 - Key Differences. Accessed on 21.10.2022. Available at URL <https://101blockchains.com/erc20-vs-erc721/>.

[50] CHEVET, Sylve. 2018. *Blockchain Technology and NonFungible Tokens: Reshaping value chains in creative industries*. Pp. 50-52. Accessed on 22.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212662>.

NFTs may be exchanged in special marketplaces (e.g. OpenSea and Nifty Gateway), creating a process of tokenization from reality to digital. They may be used to create verifiable digital ownership over several assets: crypto art, digital collectibles, online games, intellectual property rights, real estate, jewelry, vehicles, licenses, financial documents, among others.

The phenomenon of NFTs, by removing intermediaries in the art market, may also contribute to reducing the role of producers and publishers[51]. With blockchain technology, art financing and rights management may be reshaped to a scenario in which the creators internalize some of the processes previously handled by producers and publishers. For instance, a creator could sell their work directly to the buyers or a distributor with more favorable contractual terms when compared to the current market.

Innovative instruments like NFTs were only possible due to the advent of DeFi. On the one hand, NFTs may create wealth by helping artists, collectors, and interested parties negotiate in a secure and decentralized environment. On the other hand, concerns related to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) may arise due to weak or inexistent regulation and the apparent anonymity in the blockchain. Market participants involved in trading NFTs may also face potentially high non-compliance costs if the legislation is not clear enough about the legal status of NFTs and in establishing the legal requirements to operate in this novel market.

[51] Id. P. 54. Accessed on 22.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212662>.

4 The Crypto Regulatory Gap and Financial Crime Risks Arising from the Cryptoasset Business

As previously explained, the blockchain technology and especially cryptoassets have changed the way investments in the financial market are made, offered efficient technological solutions to provide greater security and transparency to financial transactions, and changed paradigms in the digital art and collectibles market. However, being an emerging technology in rapid evolution, the regulation related to DeFi and cryptoassets has not yet been developed enough to address effectively the concerns arising from this technology, especially regarding money laundering, terrorism financing and financial crimes practiced in the blockchain.

It is understandable that in the early stages of DeFi there was not a broad regulation for this technology, not only because the portion of society involved in this market was not significant, but also because the imposition of regulation in the early stages of research and development (R&D) could lead to an excessive bureaucratic burden on the developers. This, in turn, could contribute to stifling innovation and discouraging developers, especially small ones, from entering the DeFi business.

Blind argues that, when regulation is introduced, the compliance costs may reduce the available resources for R&D in a manner similar to taxation[52]. Nevertheless, the lower capital flow that may reduce innovation and technological progress is likely in the short run and may not affect all market players. In the long run, a smart, clear and efficient regulatory framework that entails flexible solutions may reduce the regulatory burden and create incentives for R&D. Consequently, the impact of regulation on innovation depends on the balance between the compliance costs and the incentive effect proposed by the regulation in place.

Concerning ML/TF risks related to cryptoassets, a preliminary risk lies in the fact that they are borderless assets, i.e. assets that can be easily moved from one country to another. Because of this feature, they may represent a higher ML/TF risk than traditional financial assets. As a highly regulated market, the financial services offered by banks and payment platforms are subject to strict control aiming to combat financial crime. The same

[52] BLIND, Knut. 2012. *The Impact of Regulation on Innovation*. P. 10. Accessed on 28.10.2022. Available at URL <https://media.nesta.org.uk/documents/the_impact_of_regulation_on_innovation.pdf>.

cannot be said about cryptoassets - with the respective regulation still being in its early stages.

A second significant ML/TF risk-aggravating factor arising from the crypto business is the fact that decentralized exchanges (DEXs) like Uniswap, Sushiswap and Venus allow users with unhosted wallets[53] to exchange cryptoassets without a centralized party that would be obligated to conduct Know Your Customer (KYC), Customer Due Diligence (CDD) and AML/CTF checks, which could offer clear opportunities to layer the proceeds of crime on the blockchain.

A hosted wallet is a digital account that is hosted by a third-party financial institution (e.g. a bank or an e-money institution) that allows the account holder to store, send and receive cryptoassets. In contrast, an unhosted wallet is a crypto wallet that is not hosted by a third-party financial system and therefore does not necessarily comply with regulations concerning financial crime applicable to FIs. Taking into account that unhosted wallets facilitate anonymity and asset concealment in the blockchain, added to the fact that it is very difficult to establish who their beneficial owner is, they represent a high ML/TF risk that could put into perspective the benefits offered by blockchain technology.

A third ML/TF risk-aggravating factor related to cryptoassets lies in the availability of Crypto ATMs (also known as Bitcoin ATMs), namely machines that are connected to a given DEX and allow their users to buy and sell cryptoassets using cash. According to Coin ATM Radar[54], there are currently 38,775 Crypto ATMs across 79 countries. Among those, approximately 1,600 ATMs are spread throughout the European Union (EU). Moreover, providers like Coinhub allow their users to purchase up to $25,000.00 per day in cryptoassets[55].

[53] U.S. Department of the Treasury. 2020. *Requirements for certain transactions involving certain convertible virtual currency or digital assets*. Accessed on 28.10.2022. Available at URL <https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf>.

[54] Coin ATM Radar. Bitcoin ATM Map. Accessed on 28.10.2022. Available at URL <https://coinatmradar.com/>.

[55] Coinhub ATM. Accessed on 28.10.2022. Available at URL <https://coinhubatm.com/>.

There are two types of Crypto ATMs: one-way and two-way[56]. The former allows the purchase of cryptoassets and the latter also enables the selling of those assets. Regardless of the type of ATM, the ML/TF risks are considerably high. For example, individuals involved in the commission of a crime (e.g. drug trafficking, illegal weapon trading or trafficking in human beings) may employ one of those ATMs to deposit cash obtained from their criminal activities. The referred amounts can be easily converted into Bitcoins which can be transferred to an unhosted wallet outside the EU. By doing so, the criminals could then layer the crime proceeds by transferring these assets to various other wallets and investing in cryptoassets, which, ultimately, could result in the laundering of the illicitly obtained proceeds.

The possibility of such a situation happening is not a distant hypothesis. According to Europol[57], the use of cryptoassets for criminal activity and money laundering has grown over the past few years in volume and sophistication. In addition to obscuring illicit money flows, criminals are employing crypto as a means of payment and as investment fraud currency[58]. Cryptocurrencies have also been used as part of exchanges within for-profit schemes related to child sex abuse material[59] (CSAM) and to execute payments to an ISIL propaganda website via Bitcoin donations[60], hence financing that terrorist organization.

A fourth increased ML/TF risk related to the cryptoasset business is the possibility of settling peer-to-peer (P2P) transactions using the blockchain. According to the definition suggested by the FATF, P2P transactions are virtual assets (VAs) transfers conducted without the use or involvement of a virtual asset service provider (VASP) or

[56] MACKENZIE, Alice. 2022. *Bitcoin ATMs - An Easy Guide to Bitcoin Teller Machines*. Accessed on 28.10.2022. Available at URL <https://bitcoinmagazine.com/guides/easy-guide-to-bitcoin-atms#:~:text=A%20Bitcoin%20ATM%20is%20a,private%20ways%20to%20do%20so.>.

[57] Europol. 2021. P. 4. *Cryptocurrencies - Tracing the Evolution of Criminal Finances*. Accessed on 30.10.2022. Available at URL <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf>.

[58] EUROJUST. 2022. *Takedown of Online Investment Fraud Responsible for Losses of Several Million Euros*. Accessed on 30.10.2022. Available at URL <https://www.eurojust.europa.eu/news/takedown-online-investment-fraud-responsible-losses-several-million-euros>.

[59] Europol. 2021. P. 11.

[60] FATF. 2018. *Financing of Recruitment for Terrorist Purposes*. P. 20. Accessed on 30.10.2022. Available at URL <https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-Recruitment-for-Terrorism.pdf>.

other obliged entity[61]. Concerning the risks related to P2P transactions, the FATF Guidance for a Risk-Based Approach for VAs and VASPs[62] states that illicit actors may exploit the lack of an obliged intermediary to layer their crime proceeds precisely because there is no entity obliged to conduct KYC, CDD and AML/CTF checks. Furthermore, the encrypted and unrecorded transactions in a P2P network may create additional obstacles to financial crime investigations particularly when it comes to layering the proceeds of crime[63].

The concept of a P2P economy bears a very similar definition when compared to DeFi. Wright argues that the former refers to decentralized individual, cooperative and coordinated action carried out via distributed mechanisms that do not depend on proprietary strategies, i.e. strategies created by centralized entities. Taking advantage of the fact that P2P transactions do not require intermediaries that may be subject to KYC, CDD and AML/CTF checks, P2P marketplaces like Bisq and PrimeXBT provide a platform for buyers and sellers to trade cryptoassets anonymously.

Additionally, the ML/TF risk is aggravated by the fact that the regulatory framework applicable to the crypto sector will only be operational as of 2024 in the EU. Besides this, as will be shown in the following chapter, the current regulatory framework presents several regulatory gaps that need to be addressed.

As a type of cryptoasset, NFTs are also subject to the above-mentioned risks. However, specifically regarding these assets, there is an increased risk of tax evasion since NFTs are mostly exchanged as crypto-collectibles and digital art. That characteristic, added to their significant price fluctuation, makes it difficult to appraise their valuation, a key factor to calculate the overall capital and capital gains for tax purposes. Furthermore, Houser argues that government agencies do not seem to fully understand the concept of

[61] FATF. 2022. *International Standards on Combating Money-laundering and the Financing of Terrorism & Proliferation*. Paragraph 54. Accessed on 04.11.2022. Available at: <www.fatf-gafi.org/recommendations.html>.

[62] FATF. 2021.*Updated Guidance for a Risk-based Approach to Virtual Assets and Virtual Asset Service Providers*. Accessed on 04.11.2022. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>.

[63] ALHOSANI, Walled. 2016. *Anti-Money Laundering : A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Unit*. Pp. 3-4.

NFTs and may not be able to differentiate them from fungible cryptoassets[64], which may add to the frustration and confusion facing the industry.

Currently, national tax authorities and the EU may not hold sufficient information about the NFT trading business, thus possibly resulting in losses related to non-taxation. Additionally, the disparity between the EU Member States' tax laws may be contributing to tax evasion within the Union. On the one side, "crypto-friendly" countries like Portugal, Germany, and Slovenia have favorable laws that may benefit certain types of investors (e.g. by taxing crypto only in specific scenarios). On the other side, countries with stricter tax laws like Spain, Norway, and Italy have opted, for instance, to tax the capital gains arising from the crypto business.

Sitompul argues that the lack of consensus among countries[65] about when and how to tax cryptoassets is not an EU/EEA issue. Considering each country may propose a particular cryptoasset definition for tax purposes, which is not necessarily aligned with other countries' definitions, a given country may classify and tax these assets independently.

Different tax regimes for cryptoassets within the EU may give rise to a "race to the bottom" in which crypto investors are constantly moving their assets to "friendlier" EU Member States. Moylan states that the lack of a reporting framework[66] that allows tax authorities to monitor the ownership and use of cryptoassets may lead to crypto businesses moving outside of the EU or to crypto holders sending their assets to unhosted wallets that are not required to conduct KYC and CDD, resulting in an increased risk of tax evasion.

Considering the technological novelty brought by DeFi, the disruptive nature of the blockchain, the regulatory gap regarding cryptoassets and the financial crime risks related to crypto, an important question that needs to be explored is whether the EU regulatory framework is ready to address and foster innovation while avoiding an increase in financial crime. As particularly regards NFTs, four sub-questions need to be answered to

[64] HOUSER, Kimberly et al. 2022. Utah Law Review. *Navigating the Non-Fungible Token*. Accessed on 05.11.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4055535>.

[65] SITOMPUL, Anggia Debora. 2022. Journal of Pancasila and Law Review. *Imposition of Tax Law on Cryptocurrencies and NFT in Indonesia*. Accessed on 05.11.2022. Available at URL <https://jurnal.fh.unila.ac.id/index.php/plr/article/view/2555/1838>.

[66] MOYLAN, Christopher Ignatius. 2022. *OECD's Proposed Crypto-Asset Reporting Framework - A Critique*. Accessed on 05.11.2022. Available at URL <https://www.diva-portal.org/smash/get/diva2:1664824/FULLTEXT01.pdf>.

determine whether the EU laws applicable to crypto will be able to address ML/TF risks and financial crime arising from the NFT business effectively:

- What is the legal status of the NFTs?
- Should NFTs be treated as artwork, collectibles, investments or cryptocurrencies for AML/CTF purposes?
- Considering that NFTs are borderless assets, what are the financial crime risks and how to combat them?
- What may be improved so that EU law is better prepared for the changes brought by DeFi, particularly the NFT trading business?

In the following chapters, these questions will be explored by means of a legal analysis of the EU AML/CTF regulation and the financial crime legal framework applicable to cryptoassets with an emphasis on NFTs.

5 Cryptoassets Regulatory Framework

Cryptoassets have recently acquired the status of (informal) financial assets and for many investors have been considered a tangible possibility to generate profits, finance economic activities and contribute to the development of blockchain technology. As pointed out in the previous chapters, these assets have been increasingly present in the financial market, business community, academia and the general public.

Since it is an emerging and disruptive technology that can facilitate the concealment of assets taking advantage of the anonymity in the blockchain, besides offering clear facilities for, *inter alia*, money laundering (ML), terrorist financing (TF) and tax evasion[67], DeFi and cryptoassets have been receiving special attention from the EU and its regulatory agencies.

Taking that into account, on July 20, 2021, the European Commission presented an ambitious new package of legislative proposals[68] to combat ML and TF in the EU, with a special focus on monitoring financial transactions of cryptoassets. The Commission's goal is to improve the detection of suspicious transactions and activities in the financial system, considering new and emerging technologies such as cryptoassets.

This package includes proposals for: a Regulation establishing a new AML/CTF authority[69]; a Regulation on AML/CTF[70] containing applicable rules in the areas of CDD and beneficial ownership; a sixth Directive on AML/CTF[71] (AMLD6) containing general provisions that shall be transposed into national law, (e.g. rules on national supervisors

[67] Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. P. 09. Accessed on 30.11.2022. Available at URL <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf>.

[68] European Commission. 2021. *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules*. Accessed on 06.11.2022. Available at URL <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690>.

[69] Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. COM/2021/421 final.

[70] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. COM/2021/420 final.

[71] 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. COM/2021/423 final.

and Financial Intelligence Units (FIUs)); and a revision of the Regulation on Transfers of Funds[72] to enable the tracing of cryptoassets.

In addition to these regulatory instruments, several others have been proposed or are being updated to address the risks arising from the cryptoasset business and the potential to facilitate the commission of financial crimes on the blockchain. On the one hand, from an EU perspective, one may highlight the Proposal for a Regulation on Markets in Cryptoassets[73] (MiCA) and the Proposal for a Directive on Administrative Cooperation[74] (DAC8) to combat tax fraud and evasion via cryptoassets. On the other hand, from a global perspective, the following soft law instruments may be highlighted: the FATF Recommendations[75] and the updated Guidance for a Risk-Based Approach for VAs and VASPs[76]; and the OECD's Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard (CARF).[77]

5.1 AMLD5

The Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[78] (AMLD5) is considered a landmark in the fight against financial crime in the EU. Being strongly influenced by the FATF standards, it contributed to the standardization of the AML/CTF checks and

[72] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast). COM/2021/422 final.

[73] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final.

[74] European Commission. 2021. Tax fraud & evasion – strengthening rules on administrative cooperation and expanding the exchange of information. Accessed on 30.11.2022. Available at URL <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en>.

[75] FATF (2012-2022). International Standards on Combating Money Laundering and the Financing of

Terrorism & Proliferation, FATF, Paris, France. Accessed on 30.11.2022. Available at URL <www.fatf-gafi.org/recommendations.html>.

[76] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. Accessed on 30.11.2022. Available at URL <www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html>.

[77] OECD (2022). Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, OECD, Paris. Accessed on 30.11.2022. Available at URL <https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm.>.

[78] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

balances in the EU context, particularly in those EU Member States that previously presented deficiencies in their AML/CTF regulatory framework. It did so by, *inter alia*, ensuring that enhanced due diligence (EDD) and countermeasures are coordinated and harmonized in the EU[79].

The Directive was a pioneer when it brought virtual currencies, virtual currency service providers (VCSP) and custodian wallet providers under its scope[80]. Silva argued that the inclusion of the referred entities into the list of obliged entities might configure a rule-based approach instead of a risk-based approach (RBA) as proposed by the FATF Recommendations, which could shrink the margin given to Member States to extend the scope of the Directive according to their own RBA[81]. To address this issue and clarify which rules may apply to the crypto sector, in October 2021, the FATF proposed an RBA to VAs and VASPs that will be discussed in the following analysis (see chapter V, section 5).

As previously seen (see chapter 3, section 2), the AMLD5 considered virtual currency a "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically".[82] Considering this wording of the definition of virtual currencies, it may apply to fungible tokens, particularly to cryptocurrencies.

Regarding virtual currency platforms that provide exchange services between virtual and fiat currencies (e.g. DEX), as well as custodian wallet providers (e.g. Coinbase and Kraken), they should be considered obliged entities for AML/CTF purposes[83]. However, when it comes to NFTs, the Directive's applicability remains unclear and doubts may arise as to whether NFTs should be considered virtual currencies. Considering that

[79] SILVA, Patrícia Godinho. 2019. New Journal of European Criminal Law. *Recent developments in EU legislation on anti-money laundering and terrorist financing*. Accessed on 06.11.2022. Available at URL <https://journals.sagepub.com/doi/pdf/10.1177/2032284419840442>.

[80] Directive (EU) 2015/849. Article 3(1)(g)(h).

[81] SILVA, Patrícia Godinho. 2019. P. 62.

[82] Directive (EU) 2015/849. Article 3(18).

[83] Id. Article 2(1)(g)(h).

the main characteristic of the NFTs is their non-fungibility and currencies are inherently fungible, one could argue that NFTs might escape the grasp of the AMLD5.

Next, the AMLD5 reduced the thresholds for identification when purchasing anonymous payment methods (e.g. prepaid cards like Paysafe and SimpledCard). The Directive reduced these thresholds from EUR 250 to EUR 150 and widened the requirements for customer verification.[84] It has also clarified the FIUs' prerogative to request information from obliged entities and have direct access to information held by them while ensuring the Member States' legislation is aligned with international standards.[85]

Moreover, the AMLD5 urged the Member States to establish centralized automated mechanisms, such as central registries or central electronic data retrieval systems, which could enable the FIUs to timely identify natural or legal persons holding or controlling bank or payment accounts in the EU[86].

Besides this, the AMLD5 improved scrutiny over ultimate beneficial ownership (UBO) information by ensuring public access to certain beneficial ownership registers on the company and business-related trusts and other legal arrangements similar to trusts[87]. The Member States were also required to establish a central beneficial ownership register[88] to store UBO information and, when required, share it with the parties with a legitimate interest.

Concerning the UBO register, on 22 November 2022, a decision from the Court of Justice of the European Union[89] (CJEU) ruled that the provision of Directive 2018/843[90] whereby Member States must ensure that the UBO information of companies incorporated within their territory should be accessible in all cases to any member of the public is invalid. The CJEU ruled that the general public's access to UBO information constitutes

[84] Id. Article 12(1).

[85] Id. Article 32(9).

[86] Id. Article 32a(1).

[87] Id. Article 31(1).

[88] Id. Article 31(3a).

[89] Joined cases C-37/20 Luxembourg Business Registers and C-601/20 Sovim.

[90] 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. Article 30(5).

an infringement to the fundamental rights concerning private life and data protection. Furthermore, this infringement could not be justified by the purposes of combating ML and TF. Harari stated that CJEU's decision is a step backwards in the fight against financial crime in the EU because, for most companies, the legal and beneficial owners are the same individuals. The decision only benefits those individuals that have the means and incentive to acquire shell companies and pay for law and accounting firms to hide their identities. Moreover, it may have created a double standard that will shield the rich and powerful from accountability and public transparency.[91]

The AMLD5 suggested including the regulatory framework for virtual currencies in a report that should have been published at the beginning of 2022. This report, which had not yet been released at the time of this research, should have included measures to set up and maintain a central database registering virtual currency service provider users' identities and wallet addresses making them accessible to the FIUs, as well as self-declaration forms for the use of virtual currency users.[92]

Lastly, the Directive obliged the Member States to create a list indicating which national public offices and functions may qualify as politically exposed persons (PEPs), providing further clarity over PEPs[93] and the rules to which they are subject.[94] The AMLD5 also put an end to the anonymity of bank and savings accounts, passbooks, as well as safe deposit boxes and paved the way for the creation of central access mechanisms to holder information on the referred assets[95].

Regarding the prohibition of anonymous bank accounts, passbooks and safety deposit boxes imposed on traditional financial institutions, one might argue that this rule may apply to VCSPs, particularly when it comes to cryptocurrencies. Taking into consideration that VCSPs are obliged entities under the AMLD5, cryptocurrencies are covered by the definition of virtual currencies, and crypto exchanges might be considered

[91] Tax Justice Network. November 2022. EU court returns EU to dark ages of dirty money. Accessed on 01.12.2022. Available at URL <https://taxjustice.net/press/eu-court-returns-eu-to-dark-ages-of-dirty-money/>.

[92] Directive (EU) 2015/849. Article 65(1)(g).

[93] Id. Article 20a(1)(2).

[94] KOSTER, Harold. 2020. Journal of Money Laundering Control. *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework*. Accessed on 06.11.2022. Available at URL <https://www.emerald.com/insight/content/doi/10.1108/JMLC-09-2019-0073/full/html>.

[95] Directive (EU) 2015/849. Article 10(1).

as VCSPs, an extensive interpretation of Article 10(1) could consider VCSPs as a financial institution under AMLD5. In this case, the Directive's applicability could prevail and, therefore, the prohibition of maintaining anonymous accounts (e.g. unhosted wallets) could be enforced by the EU Member States.

Supporting this understanding, the MiCA Proposal[96] suggests that the current definition of financial instruments, which shapes the scope of the Markets in Financial Instruments Directive (MiFID II), expressly includes financial instruments based on DLT. Should this understanding become prevalent, crypto exchanges could be considered financial institutions and, therefore, be subject to the AML/CTF compliance rules applicable to the traditional financial institutions.

5.2 AMLD6

The Directive (EU) 2018/1673 on combating money laundering by criminal law[97] (AMLD6) aims to harmonize the definition of money laundering[98] and the scope and sanctioning of ML infringement rules in national law, which may result in optimizing the cooperation between the EU Member States.[99]

Rose[100] states that the AMLD6 also aims to make sure the EU regulation is compliant with international obligations, particularly the obligations arising from the Council of Europe Convention from 2005 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financing of Terrorism (Warsaw Convention) and the updated FATF Recommendations.

With a position aligned with the Warsaw Conference and the FATF recommendations, one of the main novelties brought by the Directive was the inclusion of liability for legal persons. Before the AMLD6, there was no liability regulated for legal persons except for financial entities, EU Member States and national competent authorities. With the new rule imposed by the Directive, criminal liability could be

[96] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA). COM/2020/593 final. Explanatory Memorandum.

[97] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.

[98] Id. Article 3.

[99] Id. Recitals 1 and 2.

[100] ROSE, Kalle Johannes. 2021. *Lack of clarity in recent Criminal Law Directive gives ground for significant expansion of EU money laundering regulation*. Pp. 02-04. Accessed on 13.11.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3799569>.

extended to legal entities when: an ML offence is committed to their benefit by an individual in a leading position within these entities; or in cases in which the lack of supervision or control by such individual allowed the commission of the ML offence. The inclusion of liability towards legal persons[101] in the EU may open up a new branch of preventing financial crime by extending the liabilities previously imposed only on the financial sector.[102]

Against this backdrop, even if the regulations currently proposed or enforced on cryptoassets do not expressly consider CASPs to be financial institutions, the (lack of) liability issue would be covered by this legal provision provided for the AMLD6. Thus, virtual/crypto asset service providers (e.g. crypto exchanges) could be subject to the liability provided for in the Directive.

The AMLD6 also provided for a unified list of twenty-two predicate offences. The term 'predicate offence' refers to the underlying criminal offence that gave rise to the criminal proceeds which are the subject of a money laundering charge.[103] In other words, since money laundering consists in "cleaning" the proceeds of crime so that they can be used with the appearance of lawfulness, the predicate crime is the crime that generates the illicit proceeds.

Among the predicate offences provided for in the AMLD6, the following can be highlighted: environmental crimes; trafficking of drugs, weapons and human beings; fraud; terrorism; corruption; murder and grievous bodily injury; insider trading and market manipulation; tax crimes; and cybercrimes[104]. Concerning market abuse rules involving crypto service providers, MiCA will provide for these rules, which will be further discussed (see chapter V, section 4).

Finally, the Directive also provided for sanctions applicable to the above-mentioned legal persons.[105] The AMLD6 states that possible sanctions may include: the prohibition to receive public benefits or aid for four years; a temporary or permanent ban

[101] Directive (EU) 2018/1673. Article 7.

[102] ROSE. 2021. P. 02-04.

[103] ROSSEL, Lucia et. al. 2021. *The Implications of Making Tax Crimes a Predicate Crime for Money Laundering in the EU*. P. 240. Accessed on 13.11.2022. Available at URL <https://academic.oup.com/book/39754/chapter/339818508>.

[104] Directive (EU) 2018/1673. Article 2(1).

[105] Id. Article 8.

to conducting business; a temporary or permanent exclusion from access to public funding; a judicial supervision on the legal person; judicial winding-up order; and a temporary or permanent closure of the business units through which the offences were committed. These measures do not necessarily bear a criminal nature and could ultimately result in greater control over the cryptoasset business and a tightening of compliance rules to combat financial crimes

5.3 Revision of the 2015 Regulation on Transfers of Funds

To date, the transfers of cryptoassets fall outside the scope of the EU's legislation on financial services, exposing cryptoasset holders and service providers to ML/TF risks and potentially damaging the integrity, stability and reputation of the financial sector. Considering cryptoasset transfers are subject to similar financial crime risks as wire funds transfers, the European Commission (EC) understands that the former assets should abide by the same laws that apply to the latter concerning the transfer of funds.[106] This is why, in July 2021, the EC presented a Proposal for a Regulation on information accompanying transfers of funds and certain crypto-assets[107] that will amend the 2015 Regulation on Transfers of Funds.[108] The proposal aims to make it possible to trace the transfers of cryptoassets and address the financial crime risks arising from the cryptoasset business.

For clarity purposes regarding the various terms created to define cryptoassets, the Proposal states that its definition of cryptoassets and cryptoassets service providers (CASPs) correspond to the definitions proposed by MiCA. Moreover, the definition of CASPs corresponds to that of virtual asset service providers (VASPs) included in the FATF Recommendations. This convergence of definitions is important to clarify which assets and businesses the Regulation will apply to and to avoid legal loopholes that could make way for non-compliance by CASPs.

The Proposal reflects the FATF Recommendation No. 15 on new technologies to cover VAs and VASPs, particularly new information obligations for the originator and beneficiary CASPs at both ends of a crypto transfer. This information exchange is known

[106] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets. COM(2021) 422 final. Recital 28.

[107] COM(2021) 422 final.

[108] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

as the travel rule,[109] namely the obligation to obtain, hold and submit information about the originator and beneficiary of financial transfers to identify and report suspicious transactions, take freezing actions and prohibit transactions with designated persons and entities.[110]

When adopted, the revised Regulation will apply to CASPs whenever their transactions involve a traditional wire transfer or a cryptoasset transfer between a CASP and any other obliged entity (e.g. another CASP, a bank or a payment platform).[111] Furthermore, transactions involving cryptoassets - as previously stated, borderless assets - will have to meet the same requirements as cross-border wire transfers, following the FATF Recommendation No. 16 and its interpretive note.[112]

Additionally, according to the Proposal,[113] the CASP of the originator - a person who holds an account with a given CASP and allows a transfer of cryptoassets from the referred account - shall ensure that cryptoasset transfers are accompanied by personal information about the originator such as name, account number, address, official personal document number, customer identification number or date and place of birth. The CASP of the originator should also ensure the transfers are accompanied by the name and account number of the beneficiary of the transaction. Moreover, the CASPs should verify the information accuracy provided by the originator from a "reliable and independent source"[114] before making funds available to the beneficiary.[115]

To guarantee that the above-referred measures are actually taken, CASPs should have in place effective transaction monitoring during and after the transactions are settled to make sure the risks related to financial crime in the blockchain are mitigated.[116] This

[109] SCHMIDT, Alicia. 2022. *Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model*. International Journal of Law and Information Technology, Volume 29, Issue 4, Pages 332-363. Accessed on 17.11.2022. Available at URL <https://academic.oup.com/ijlit/article-abstract/29/4/332/6516792?redirectedFrom=fulltext>.

[110] FATF Recommendation No. 16.

[111] COM(2021) 422 final. Article 2(1).

[112] FATF. 2012-2022. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Interpretive Note to Recommendation 16.

[113] COM(2021) 422 final. Article 14(1)(2).

[114] Id. Article 14(5).

[115] Id. Article 16(2).

[116] Id. Article 16(1).

transaction monitoring shall be implemented according to a risk-based approach provided for in Articles 16, 18(3) and 37 of the AMLD5. In case a CASP repeatedly fails to provide the required information about the beneficiary and the originator, the beneficiary's CASP is expected to: issue warnings and deadlines; return the cryptoassets to the originator's account; hold the transferred cryptoassets from being available to the beneficiary pending review from the AML/CTF compliance officer.[117]

Considering the above, when the Proposal requires compliance with the travel rule, it is tacitly forbidding the use of unhosted/anonymous wallets. Assuming that these wallets do not retain personal information about their beneficiaries, CASPs would be unable to transmit and receive this mandatory data, and therefore would be effectively prevented from conducting transactions originating from or directed to these anonymous wallets.

The Proposal is an important step towards combating financial crime in the cryptoasset business. However, Karasek-Wojciechowicz[118] argues that it failed to address risks arising from P2P transactions when it stated that it will not apply to person-to-person transfers of cryptoassets.[119] In article 3(14), the Proposal defined a person-to-person transfer of cryptoassets as a transaction between natural persons acting, as consumers, for purposes other than trade, business or profession, without the use of a CASP or other obliged entity. In an attempt to address this legal gap, the FATF proposed a risk-based approach[120] (RBA) to cryptoassets, which will be discussed below (See chapter V, section 5).

5.4 Proposal for a Regulation on Markets in Crypto-assets (MiCA)

In September 2020, the European Commission released the Proposal for a Regulation on Markets in Crypto-assets (MiCA),[121] which aims to address the potential risks to the stability of the financial system and monetary policy arising from the

[117] Id. Article 17(2).

[118] KARASEK-WOJCIECHOWICZ, Iwona. *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces*. Journal of Cybersecurity, 2021, 1–28. Accessed on 17.11.2022. Available at URL <https://academic.oup.com/cybersecurity/article/7/1/tyab004/6166133>.

[119] COM(2021) 422 final. Article 2(4).

[120] FATF's updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers.

[121] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final.

cryptoassets business. As part of a new EU Digital Finance Package[122], MiCA provides for a regulatory framework for cryptoassets - currently not covered by the existing EU financial legislation - and establishes uniform rules for CASPs and crypto issuers.

The Proposal also aims to regulate the public offer of cryptoassets, determine which cryptoassets may be traded on a trading platform, create a single licensing of CASPs in the EU, and implement market abuse rules for cryptoasset-based businesses across all Member States by 2024.[123] One of MiCA's main priorities is to ensure financial stability, prevent the financial system's disruption and preserve the continuity of the current financial order.[124]

MiCA is part of a new EU Digital Finance Strategy[125] (DFS) which aims to: eliminate regulatory fragmentation in the Digital Single Market; improve the EU regulatory framework to pave the way for digital innovation; promote data-driven finance; address the risks arising from digital innovation; and enhance the digital operational resilience (i.e. cybersecurity) of the financial system.

MiCA was also a strong response to the 2019 Facebook (Meta) Libra project[126]. Back then, the big tech company proposed the creation of a global digital currency potentially accessible to billions of people across the world. This currency would be a stablecoin backed by a handful of sovereign currencies such as the dollar, euro and yen. This plan gave rise to significant concerns due to the possibility of disruption of the global financial system. This was due to Libra's capacity of reaching billions of people through a social network platform and the potential impact on financial stability, monetary policy, competition, and AML/CTF associated therewith. The Libra project was later abandoned at the beginning of 2022 amid regulatory pressure but it served as a warning for the global financial system to finally give cryptoassets due regulatory attention.

---

[122] European Commission. 2020. Financial Stability, Financial Services and Capital Markets Union. Communication on Digital Finance Package. Accessed on 18.11.2022. Available at URL <https://finance.ec.europa.eu/publications/digital-finance-package_en>.

[123] COM/2020/593 final. Preamble, item 5 - Other Elements.

[124] FERREIRA, Agata. *The Curious Case of Stablecoins—Balancing Risks and Rewards?* Journal of International Economic Law, Volume 24, Issue 4, December 2021, Pages 755–778. Accessed on 17.11.2022. Available at URL <https://academic.oup.com/jiel/article/24/4/755/6446841>.

[125] European Commission. 2020. Communication on a Digital Finance Strategy for the EU. COM (2020) 591 final.

[126] FERREIRA, Agata. P. 756.

MiCA was drafted around two concepts: 1) providing rules applicable to cryptoassets that can be regarded as or are similar to payment instruments and e-money (including stablecoins); and 2) outlining rules applicable to all cryptoassets that currently fall within the scope of the existing EU financial markets legislations, including, for instance, cryptoassets not intended to offer any kind of financial return or investment.[127]

Concerning the taxonomy of cryptoassets, in Titles III and IV, MiCA provides for two categories of cryptoassets created to regulate stablecoins, namely asset-referenced tokens (ARTs) and e-money tokens (EMTs).[128] ARTs are a type of crypto-asset that purports to maintain a stable value by referencing currencies that are legal tender, commodities, cryptoassets, or a basket of such assets, while EMTs mean a type of cryptoasset that is primarily used as a means of exchange and aims to maintain a stable value by referring to the value of a fiat currency that is legal tender. According to Maia, EMTs shall be deemed as electronic money in terms of Article 2(2) of Directive 2009/110/EC[129], with the specificity of e-money tokens being issued, transferred and stored using DLT technology.[130] Next, MiCA provides for an additional category of cryptoassets known as the "other" tokens. More specifically, in Title II, MiCA stipulates the "offers of crypto-assets, other than asset-referenced tokens or e-money tokens", creating a "catch-all" category of cryptoassets that encompasses, for instance, NFTs.[131] Bearing this into mind, the scope of MiCA's Title II is essentially limited to NFTs, utility tokens and other non-financial cryptoassets.

In article 2(2), MiCA establishes which types of cryptoassets will not fall under its scope; this is the case with cryptoassets qualifying as financial instruments, e-money, deposits, structured deposits or securitized assets. Thus, MiCA will only apply to

[127] ZETZSCHE, DIRK A. et al. 2020. University of Luxembourg Law Working Paper Series No. 2020-018. *The Markets in Crypto-Assets Regulation(MICA) and the EU Digital Finance Strategy.* Accessed on 18.11.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725395>. P. 11.

[128] COM/2020/593 final. Article 3(1)(3) and (4).

[129] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

[130] MAIA, Guilherme et al. 2021. MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). Forthcoming article in "Blockchain and the law: dynamics and dogmatism, current and future". Accessed on 18.11.2022. Available at SSRN: https://ssrn.com/abstract=3875355 or http://dx.doi.org/10.2139/ssrn.3875355.

[131] COM/2020/593 final. Article 4.

cryptoassets that are not subject to other EU financial laws such as Directive 2014/65/EU.[132]

To give an example, in case a token is classified as an ART or EMT and contemplated by another EU financial law, MiCA will not be applicable since the token will be deemed as a financial instrument - i.e. it will be considered similar to a share, debenture or derivative. In case a token is not similar to a financial instrument or is similar to a financial instrument but it is not negotiable (i.e. it does not have a clear financial/investment nature), MiCA will consider this token as a utility token and apply thereto.

When MiCA refers generally to utility tokens as tokens that are not regulated by the existing EU financial laws, it gives rise to doubts as to its applicability to these tokens. One may argue that it will be difficult to determine when tokens fall within the definition of financial instruments covered by the MiFID and therefore are not subject to MiCA. This may lead to legal uncertainty considering the possibility of an *ex post* approach of supervision due to the risks of re-characterization and re-qualification of utility tokens.[133]

Regarding ARTs and EMTs, their qualification as cryptoassets should be supported by a legal opinion that establishes that the given assets do not fall within the scope of MiCA under article 16(2)(d) - that is, that they do not qualify as financial instruments, e-money, deposits or structured deposits. By leaving this prerogative to the private sector, MiCA might promote a "race to the bottom" among the EU jurisdictions as CASPs and token issuing actors may migrate their business to countries in which practicing lawyers will be willing to draft accommodating legal opinions. This could ultimately lead to legal uncertainty, conflicts of interest and regulatory arbitrage. A better approach to this qualification would be if it were left to the national supervisors, who will have the duty to oversee the CASPs.

According to MiCA's Title II, a legal opinion is not required for utility tokens, as they may be issued without prior review or authorization from national supervisors, only requiring mandatory disclosure.[134] It states that for CASPs to be able to offer utility

[132] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[133] ZETZSCHE, DIRK A. et al. 2020. P. 23.

[134] COM/2020/593 final. Article 4(1).

tokens, they have to comply with the following requirements: be a legal entity; draft a cryptoasset white paper under articles 5, 7 and 8; and comply with the obligations provided for in article 13 (conduct of good faith toward crypto holders and transparency with Supervisors).

It is also worth noting that MiCA exempts the issuers of unique and not fungible cryptoassets from the requirement to publish a white paper for public offerings[135]. This exemption will apply to the NFTs. While this may mean less bureaucracy that could encourage innovation, this exemption may facilitate the concealment of illicit activities.

According to Ferreira, MiCA's regulatory framework will apply to ARTs and EMTs and any stablecoins that fall outside the scope of those two definitions will not be permitted to operate within the EU.[136] These narrow parameters for operation do not consider the diversity of the stablecoins' design and could ultimately hinder innovation by denying regulatory approval to the coins that do not fit the referred definitions.

According to Recital 8 MiCA, any legislation adopted to regulate cryptoassets should be "specific, future-proof and be able to keep pace with innovation and technological developments". Additionally, such legislation should contribute to combating money laundering and the financing of terrorism. Cryptoassets and DLT should be defined as broadly as possible to capture all types of cryptoassets which currently fall outside of the scope of the EU financial laws. Considering the above, MiCA is an important step for regulating all types of cryptoassets but is not equally successful as to specifying the difference between the ARTs and EMTs that will be considered financial assets under EU law and those that will not. In this sense, Busch argues that, if MiCA is not revised, the desired regulatory level in the cryptoasset business may not be reached.[137]

In Recitals 34 and 38, MiCA urges that CASPs and their shareholders have in place adequate measures to combat money laundering and terrorism financing, sound internal control, risk assessments mechanisms, appropriate mechanisms to keep records of all transactions, orders and services, as well as a system to detect market abuse potentially committed by clients. In this context, it also requires that the persons involved in the

[135]Id. Article 4(2)(c).

[136] FERREIRA, Agata. P. 764.

[137] BUSCH, Danny. 2021. The Future of EU Financial Law. Capital Markets Law Journal, Volume 17, Issue 1, January 2022, Pages 52–94. Accessed on 19.11.2022. Available at URL <https://academic.oup.com/cmlj/article/17/1/52/6459070>.

management of CASPs do not hold a criminal record in the field of financial crime.[138] The proposed measures, together with the legal instruments previously discussed (particularly AMLD5, AMLD6 and the Revision of the Regulation on Transfers of Funds), represent an important milestone in the fight against financial crime in the EU.

5.5 FATF Recommendations and Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

As previously discussed (see Chapter III, section 2), the FATF Recommendations, lastly updated in March 2022, state that "a virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes[139]". Based on this definition, one can argue that cryptoassets and particularly NFTs are subject to the Recommendations.

While defining which cryptoassets should be subject to the Recommendations, the FATF stated that flexibility is particularly relevant in the context of virtual assets, since they involve a wide range of products and services that are evolving rapidly.[140] The Recommendations also point out that some items (i.e. tokens) that may not appear to constitute virtual assets may enable the transfer or exchange of value or facilitate money laundering and terrorist financing.

According to FATF Recommendation 15, to mitigate the ML/TF risks arising from the cryptoasset business, countries should ensure that VASPs/CASPs are: regulated for AML/CTF purposes; licensed or registered and subject to effective transaction monitoring systems; and compliant with the Recommendations. To do so, the countries should identify and assess the financial crime risks that may arise from emerging technologies and novel business practices. Concerning financial institutions, this risk assessment should be carried out before launching new products, business practices or start using novel technologies, and, in case an ML/TF risk is detected, the VASPs/CASPs should take appropriate measures to manage and mitigate those risks.

[138] COM/2020/593 final. Articles 16(3)(a), 30(4), 54(2)(f) and 61(3).

[139] FATF. 2012-2022. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.

[140] FATF. 2021. Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. P. 30. Accessed on 19.11.2022. Available at URL <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html>.

Another proposal is to be found in the interpretive note to Recommendation 15, which states that countries should consider VAs as "property", "proceeds", "funds", "funds or other assets", or "other corresponding value". However, being a soft law instrument, it does not bind any of the member countries. The interpretive note also suggests that countries should establish effective, proportionate and dissuasive sanctions (criminal, civil or administrative) to apply over VASPs/CASPs that fail to comply with AML/CTF requirements[141]. This Recommendation is in line with the administrative sanctions included in the MiCA[142].

In October 2021, the FATF published an updated Guidance for a Risk-Based Approach for Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs). The Guidance is part of FATF's ongoing monitoring of the VAs and VASPs sector and further explains how the FATF Recommendations should apply to them.

A risk-based approach[143] (RBA) means that countries, competent authorities, financial institutions and VASPs need to identify, assess and understand the ML/TF risks to which they are exposed. These entities also need to take appropriate mitigation measures according to the level of risk: usually, lower risk requires less strict measures and higher risk demands stricter actions.

On the one hand, the Guidance acknowledges that new technologies, products and related services have the potential to foster financial innovation, efficiency and improve financial inclusion. On the other hand, they may create new opportunities for criminals to launder the proceeds of their illicit activities. To address these issues, the Guidance focuses on six key areas: clarification of the definitions of VA and VASP; how the FATF standards apply to stablecoins; risks and tools available to countries to address ML/TF risks to peer-to-peer (P2P) transactions; guidelines on the licensing and registration of VASPs; additional guidance for the public and private sectors about the implementation of

[141] FATF Recommendation 35.

[142] COM/2020/593 final. Article 92.

[143] FATF. *Risk-based approach for the bank sector*. Accessed on 19.11.2022. Available at: <https://www.fatf-gafi.org/documents/documents/risk-based-approach-banking-sector.html>.

the travel rule; and principles of information-sharing and cooperation amongst VASP Supervisors.[144]

Concerning stablecoins, the FATF reaffirmed the statements on its G20 report,[145] namely that a stablecoin is covered by the FATF Standards as either a VA or a financial asset depending on its exact nature and the regulatory regime in a country. In addition to that, the Guidance clarified that a range of entities involved in stablecoin trading could be deemed as VASPs or financial institutions under the FATF Standards.[146] Finally, the Guidance presents a hypothetical case study[147] of a stablecoin arrangement and the applicability of the FATF Standards for that case.

The FATF Guidance is one of the few soft law instruments highlighting the ML/TF risks related to P2P transactions. It states that illicit actors may exploit the lack of an intermediary obliged to conduct KYC, CDD and AML/CTF checks to layer the proceeds of crime.[148] To address the financial crime risks arising from P2P transactions, the Guidance suggests a handful of tools and measures that countries may employ: conduct outreach to VASPs and P2P sector regarding consulting on AML/CTF requirements for P2P transactions; train supervisory, FIU and law enforcement personnel to raise awareness of risks involving P2P transactions; encourage the development of methodologies and tools (e.g. blockchain analytics) to collect and analyze P2P metrics and provide risk-mitigation solutions, identify suspicious behavior and determine if crypto wallets are hosted or unhosted.[149]

Furthermore, the Guidance suggests that countries implement additional measures on the national level, such as: creating controls that facilitate the visibility of P2P activity, particularly the activity between obliged and non-obliged entities (e.g. record-keeping of these transactions); establishing ongoing enhanced supervision of VASPs and entities

[144] FATF. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. P. 05. Accessed on 02.12.2022. Available at URL <www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html>.

[145] FATF. *Report to G20 on So-called Stablecoins*. Accessed on 19.11.2022. Available at: <https://www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-so-called-stablecoins-june-2020.html>.

[146] FATF. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. P. 09.

[147] Id. Pp. 34-35.

[148] Id. Paragraph 38.

[149] Id. Paragraph 105.

whose business has a special focus on unhosted wallets transactions; obliging VASPs to allow transactions only to and from VASPs and other obliged entities, as well as imposing additional AML/CTF requirements on them; and drafting comprehensive guidance applying an RBA to the customers of VASPs that engage in or facilitate P2P transactions.[150]

The Guidance also clarifies that the FATF Standards apply to VASPs/CASPs and other obliged entities that provide virtual assets. In Part Four, the Guidance included references to: correspondent banking and other similar relationships; technological solutions that may enable VASPs to comply with the travel rule; counterparty VASP identification and CDD; transfers to and from unhosted wallets; and key red-flag indicators for VAs.

Regarding transfers to and from unhosted wallets, the Guidance suggests that, under such circumstances, a VASP/CASP should obtain the originator and beneficiary information from their customer and these transactions should be subject to enhanced due diligence and targeted financial sanctions compliance.[151] Moreover, a VASP/CASP may choose to impose additional limitations, controls or prohibitions on transactions with unhosted wallets according to their risk-based control framework. This position is less restrictive than the rules that will be enforced in the EU by the Revision of the Regulation on Transfers of Funds. As already explained above, the latter imposes tacitly a ban on transactions originating from or sent to unhosted wallets.

The Guidance also provided for the principles of information sharing and cooperation amongst VASP/CASP supervisors.[152] These principles are non-binding and applicable to all countries whether they permit or prohibit these service providers: identification of supervisors and VASPs, information exchange and cooperation.

To conclude, the Guidance is an important step toward the fair regulation of VAs and VASPs/CASPs. By proposing a broader definition of VAs and VASPs/CASPs, urging countries to accommodate technological advancements and innovative business models, and establishing a risk-based approach to emerging technologies, the FATF continues to play an important role in the global AML/CTF regulatory framework.

[150] Id. Paragraph 106.

[151] Id. Paragraphs 295-297.

[152] Id. Paragraph 357.

5.6 New Regulation on AML/CTF

The Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[153] contains directly applicable rules, particularly in the areas of customer due diligence and beneficial ownership, as well as an EU-wide limit of EUR 10,000.00 for payments in cash.

Being aligned with the Revision of the Regulation on Transfer of Funds, the Draft Regulation stipulates that the provision and custody of anonymous crypto wallets will be prohibited in the EU.[154] Article 58 states that credit institutions, financial institutions and CASPs shall be prohibited from keeping anonymous accounts, passbooks, safe-deposit-boxes and cryptoasset wallets, as well as any account that could potentially allow for the anonymization of the account holder.

Next, according to this Proposal, CASPs, like credit and financial institutions, shall be deemed obliged entities in the upcoming Regulation.[155] Moreover, it states that credit/financial institutions and CASPs will be obligated to conduct CDD when initiating or executing a transfer of funds, or a transfer of cryptoassets whose value exceeds EUR 1,000.00.[156]

When conducting CDD, the obliged entities should: identify the customer and verify their identity; identify the beneficial owner and verify their identity so that the obliged entity knows who the UBO is and understands the customer's ownership and control structure; assess and obtain information on the purpose and intended nature of the business relationship; and conduct ongoing monitoring of the business relationship.[157]

Finally, concerning the limits to large cash payments, the Proposal states that persons trading in goods or providing services may only accept cash payments up to a limit of EUR 10,000.00, whether the transaction is carried out in single or several operations which appear to be linked.[158]

---

[153] Proposal for a Regulation of the European Parliament and of he Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (COM/2021/420 final).

[154] Id. Recital 93.

[155] Id. Article 3(3)(g).

[156] Id. Article 15(2).

[157] Id. Article 16(1).

[158] Id. Article 59(1).

Against this backdrop, the Draft Regulation can be considered an important step toward the proper regulation of cryptoassets in the EU. By proposing a ban on unhosted wallets and establishing that CDD must be carried out on cryptoasset transactions above EUR 1,000.00, one can argue that, if adopted, the AML Regulation will contribute to greater control over these assets within the EU and a potential reduction of financial crime related to the cryptoasset business.

5.7 Regulatory framework for combating tax evasion

The EU does not play a direct role when it comes to tax law, as this is the competence of the Member States.[159] However, the EU oversees tax rules in key areas to ensure and promote the free flow of goods and services within the Union, make sure one country does not have an unfair tax advantage over the other, and guarantee that taxes do not discriminate against consumers, workers or businesses.[160]

Currently, national tax authorities and the EU do not have sufficient information about the cryptoasset business, a fact that may result in losses related to non-taxation. Additionally, the disparity between the Member States' tax laws may contribute to tax evasion within the Union. As previously stated, different tax regimes for cryptoassets within the EU may give rise to a race to the bottom in which crypto investors are constantly moving their assets to “friendlier” EU Member States. Moreover, the lack of a reporting framework that allows tax authorities to monitor the ownership and transfers of cryptoassets may lead to an increased risk of tax evasion in the EU and consequential revenue losses.

Article 115 of the Treaty on the Functioning of the European Union (TFEU) stipulates that the main rationale underlying EU taxation lies in the well-functioning of the Internal Market, which shall not be hindered due to uncoordinated national legislation. Promoting EU-wide standardization of reporting rules would make it easier for taxpayers to comply with reporting obligations and help tackle tax evasion. Additionally, this would ensure that taxpayers, particularly those who make profit out of crypto, pay their fair share.

[159] HELMINEN, Marjanna. 2021. EU Tax Law - Direct Taxation. P. 04. Accessed on 02.12.2022. Available at URL <https://www.ibfd.org/sites/default/files/2021-09/20_007_EU_Tax_Law_Direct_Taxation_2021_final_web.pdf>.

[160] European Commission. 2018. Towards fair, efficient and growth-friendly taxes. Accessed on 02.12.2022. Available at URL <https://european-union.europa.eu/priorities-and-actions/actions-topic/taxation_en>.

To address these discrepancies and prevent such risks, the EU needs fair, efficient, and sustainable taxation schemes. Bearing this in mind, the European Commission is working on the DAC-8,[161] which will amend the Directive on Administrative Cooperation (DAC),[162] to expand the information exchange framework in the field of taxation to include cryptoassets and e-money.

The DAC obliges financial intermediaries to report financial activities to the tax authorities[163] and provides for an information exchange duty among the EU Member States.[164] Nevertheless, this obligation does not apply to cryptoassets as the intermediaries of the crypto sector (i.e. CASPs) do not fall into the subjective scope of the Directive, which only covers traditional financial institutions.

Such an obligation to report financial activities of the crypto sector accompanied by the mandatory information exchange between the Member States would enable tax authorities to obtain the necessary information to conduct a risk-based approach to cryptoassets, as well as facilitate the exercising of tax control over them.

MiCA also provides for a framework for tax purposes when it states that the competent authorities responsible for carrying out the functions and duties provided for in the Proposal should cooperate with the European Banking Authority (EBA) and European Securities and Markets Authority (ESMA) for tax purposes.[165] Nevertheless, the Proposal does not specify how that cooperation shall be carried out.

On a global level, the Organisation for Economic Co-operation and Development (OECD) recognizes that cryptoassets may pose an increased risk to global tax transparency.[166] This is particularly the case because of their borderless nature and the possibility of trading and storing them in anonymous wallets. To address the tax evasion

[161] European Commission. 2021. *Tax fraud & evasion – strengthening rules on administrative cooperation and expanding the exchange of information*. Accessed on 19.11.2022. Available at URL <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en>.

[162] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.

[163] Id. Annex I, Section I.

[164] Id. Articles 5, 8, 8a, 8aa, 8ab and 9.

[165] COM/2020/593 final. Articles 85 and 110.

[166] OECD. 2022. *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. P. 09. Accessed on 24.11.2022. Available at URL <https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm.>.

risks arising from cryptoassets, in August 2022, the OECD proposed a Crypto-Asset Reporting Framework (CARF),[167] which contains amendments to the Organization's Common Reporting Standard[168] (CRS).

The CRS, approved in 2014, requires that jurisdictions obtain information from their financial institutions and automatically exchange that information with other jurisdictions on an annual basis.[169] It sets out the financial account information to be exchanged, the financial institutions that are required to report, the types of accounts and taxpayers that are covered by the CRS, as well as the common due diligence procedures to be followed by the financial institutions.[170]

While the CRS has been an important step towards international collaboration to combat tax evasion, because it was proposed in 2014 and applies to traditional financial assets and institutions, it does not cover cryptoassets. In response to the cryptoasset tax concerns, the CARF was developed and its implementation package consists of: rules that shall be transposed into domestic laws aiming to collect information from CASPs; a framework for bilateral or multilateral authority agreements and arrangements for the automatic exchange of information; and IT solutions to support this exchange of information.[171]

More specifically, the CARF has been designed around four building blocks: the covered scope of cryptoassets; the entities and individuals that shall be subject to data collection and reporting requirements; the transactions subject to reporting and the information arising from these transactions; the due diligence procedures to identify crypto holders and the relevant tax jurisdictions for reporting and information exchange purposes.[172]

When defining its scope, the CARF proposed a broad definition for cryptoassets stating that they are "a digital representation of value that relies on a cryptographically

[167] Ibid.

[168] OECD. 2014. *Standard for Automatic Exchange of Financial Account Information in Tax Matters*. Accessed on 24.11.2022. Available at URL <http://dx.doi.org/10.1787/9789264216525-en>.

[169] Id. Annex 3 - Common Reporting Standard user Guide.

[170] Id. Introduction, Paragraph 8.

[171] Id. Executive Summary. Pp. 06-07.

[172] OECD. 2022. P. 11.

secured distributed ledger or a similar technology to validate and secure transactions".[173] By encompassing 'similar technologies', it ensures that emerging technologies that operate similarly to cryptoassets are included in the cryptoassets definition. This position seems to be following Recital 8 MiCA, according to which any legislation adopted to regulate cryptoassets should be "specific, future-proof and be able to keep pace with innovation and technological developments".

The CARF expressly excluded three types of cryptoassets from its scope because it considered them to pose a limited tax compliance risk. This is the case with: cryptoassets that cannot be used for payment or investment purposes (e.g. utility tokens such as in-game currencies); Central Bank Digital Currencies, which represent a claim in fiat currency on an issuing Central Bank or monetary authority; and Specified Electronic Money Products that represent s single fiat currency and may be redeemed under that currency according to strict requirements (closed-loop cryptoassets).[174] All cryptoassets that are not expressly excluded by the Framework are considered "Relevant Cryptoassets".[175] This means that they will also fall within the scope of the FATF Recommendations, ensuring the due diligence requirements can build on existing AML/CTF, CDD and KYC obligations worldwide.

At the same time, the exclusion of cryptoassets that cannot be used for payment or investment purposes and are not a digital representation of value - as per the Framework's definition for cryptoassets - may allow for the continued innovation of cryptoassets and DLTs that do not have investment or tax relevance. Potential examples of cryptoassets that fit these exclusion criteria are an inventory management system that aims to track product delivery, a record of ownership such as a real estate ledger, soul-bound tokens and non-transferrable NTFs.[176]

[173] Id. P. 19.

[174] Id.P. 48. Regarding closed-loop cryptoassets, "Provided these Crypto-Assets are characterised by operating in a limited fixed network or environment beyond which the CryptoAssets cannot be transferred or exchanged in a secondary market outside of the closed-loop system, and cannot be sold or exchanged at a market rate inside or outside of the closed-loop, such Crypto-Assets would generally not be able to be used for payment or investment purposes".

[175] Id. P. 11.

[176] CUTLER, Jonathan. 2022. CRS for Crypto: Demystifying the OECD's Proposed Crypto-Asset Reporting Framework. Journal of Taxation of Financial Products (Vol. 19, Issue 2). P. 10. Accessed on 25.11.2022. Available at URL <link.gale.com/apps/doc/A715600236/AONE?u=ull_ttda&sid=bookmark-AONE&xid=22e71f82>.

Regarding CASPs, the Framework has adopted a definition in line with that proposed by the FATF Recommendations and MiCA stating that they mean any individual or entity that, as a business, provides cryptoasset exchange services or makes available a cryptoasset trading platform.[177] This definition covers not only crypto exchanges such as DEX but also other intermediaries like crypto brokers and providers of crypto ATMs.

The Framework's Commentary Notes gives some examples of persons that qualify as CASPs, namely: dealers that allow for the buying and selling of relevant cryptoassets; cryptoasset ATM operators; exchanges that act as intermediaries connecting a buyer and a seller of cryptoassets and charge a commission for their services; cryptoasset brokers; and intermediaries that resell and distribute cryptoassets. Cutler[178] argues that the CASP definition and examples provided by the CARF will also include DeFi platforms that may escape the grasp of MiCA, particularly P2P cryptoasset exchange platforms.

Next, the Framework establishes that a handful of CASP types shall not be considered as Reporting CASPs, namely: a cryptoasset investment fund since investors cannot transaction on their behalf; a person that is solely engaged in validating DLT transactions (i.e. crypto miners); persons that solely issue relevant cryptoassets and do not offer crypto exchange services; persons making available a platform solely allowing users to make posts offering cryptoassets and do not engage in the actual exchange (e.g. crypto-related forums); persons creating or selling software that facilitate exchange transactions on behalf of customers, provided they do not use the software to provide a service effectuating crypto exchanges on behalf of their customers.[179]

On the one hand, the above-mentioned reporting exclusions might pose a business incentive to software creators and cryptoasset issuers not directly involved in trading cryptoassets, which could ultimately contribute to further developing the crypto ecosystem. On the other hand, one could argue that exempting from reporting obligations crypto investment funds and crypto miners (particularly large mining pools) may serve as a legal loophole to be exploited by persons who would profit from exchanging cryptoassets without necessarily contributing to the development of the ecosystem.

[177] OECD. 2022. Paragraph 16.

[178] CUTLER, Jonathan. 2022. P. 11.

[179] OECD. 2022. Pp. 50-51.

To conclude, the regulatory framework outlined above may contribute significantly to the prevention of tax evasion in the cryptoasset arena. The cooperation with the EBA and ESMA proposed by MiCA, as well as DAC-8 and CARF will advance the EU and global tax legislation and may address the current (lack of) tax legislation regarding cryptoassets.

6 Research Questions

After a historical analysis of the evolution of DeFi, a study of the definitions surrounding cryptoassets, an exposition of the increased risks of committing financial crimes in the DLT, and a brief analysis of the regulatory framework related to DeFi, blockchain, and cryptoassets, the previously raised research questions (See Chapter IV) can be answered and suggestions for the improvement of current and future legislation involving cryptoassets will be made.

Before addressing these questions, however, it is important to note that decentralized and centralized finance may not be drastically opposed as they seem. DeFi supports most of the products and services that already exist in CeFi such as asset exchange, loans, leveraged trading, decentralized governance voting and stablecoins - in the sense that they are assets pegged to the valuation of a traditionally stable financial asset.[180]

The most prevalent distinguishing features between DeFi and CeFi are: who controls the assets; how transparent and accountable the system is; and what privacy guarantees exist for the end user. As previously stated, DeFi is a disruptive movement that is challenging the current financial system due to its inherent features of immutability, increased transparency and security.[181]

From an AML/CTF compliance perspective, the traceability of DeFi assets is, in theory, more accessible than in CeFi due to the open-sourced nature of the blockchain.[182] Law enforcement agencies (LEAs) and FIUs sometimes face difficulties obtaining information from financial institutions - one of the most recent examples being the alleged suppression of information regarding the monitoring of suspicious transactions by Deutsche Bank[183]. Since most of the blockchains are open-source, to investigate blockchain transactions, provided KYC procedures were followed, one would only need the proper tools and resources to uncover potential illicit activities (e.g. Chainalysis).

[180] QIN, Kaihua et al. 2021. CeFi vs. DeFi - Comparing Centralized to Decentralized Finance. P. 13. Accessed on 26.11.2022. Available at URL <https://arxiv.org/abs/2106.08157>.

[181] Ibid.

[182] Id. P. 04.

[183] Deutsche Welle. 2022. *Deutsche Bank under pressure after money laundering raids*. Accessed on 26.11.2022. Available at URL <https://www.dw.com/en/deutsche-bank-under-pressure-after-money-laundering-raids/a-61644712>.

As discussed in the previous chapters, there is a major EU legislative effort to regulate cryptoassets and mitigate the financial crime risks that arise from transactions made on the blockchain. However, the main regulatory focus seems to be on the cryptoassets that are most prominent or those that present a higher possibility of disrupting the financial system - such as cryptocurrencies and stablecoins.

When it comes to NFTs, there are still some legal loopholes that need to be filled so that there is not only a control regarding the risks of financial crime (particularly tax evasion) but that there is also a level playing field for the stakeholders involved in the NFT business - be they creators, developers, individual traders or CASPs.

Against this backdrop, an important question that needs to be explored is whether the EU regulatory framework is ready to address and foster innovation while avoiding an increase in financial crime. As particularly regards NFTs, four sub-questions shall be answered to determine whether the EU laws applicable to crypto will be able to address ML/TF risks and financial crime arising from the NFT business effectively:

6.1 What is the legal status of the NFTs?

According to MiCA's Title II, NFTs may fall under a "catch-all" category of cryptoassets[184], namely "crypto-assets, other than asset-referenced tokens or e-money tokens" or simply 'other tokens'. NFTs may also be classified as 'virtual assets' under the FATF Recommendations when they state that "a virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes".[185]

As NFTs aim to create verifiable digital ownership over several assets - e.g. crypto art, digital collectibles, online games, intellectual property rights, real estate, jewelry, vehicles, licenses and financial documents - it is important to note which asset a particular NFT is representing when classifying it. For instance, the definition proposed by MiCA will only apply to those NFTs that do not represent financial instruments under other EU financial laws such as Directive 2014/65/EU.[186] In this sense, if MiFID II is enacted and

[184] COM/2020/593 final. Recital 15 and Article 4.

[185] FATF. 2012-2022. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.

[186] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

proposes a clarification of the current definition of financial instruments to include cryptoassets in its scope, NFTs that represent financial instruments could be considered financial assets.

Since NFTs are perhaps the most versatile cryptoasset and might represent various assets (virtual or not), one may argue that they should be classified according to the nature of the goods that they represent. For instance, if they represent a given financial asset, they should be classified as such, and if they represent digital art or crypto collectibles, they should bear the same status as traditional art or collectibles.

A possible solution to this classification could be to put it in charge of the national supervisory authorities described in MiCA.[187] As already discussed (see chapter V, section 4), one might argue that leaving the cryptoasset classification to legal opinions[188] drafted by the private sector could lead to a "race to the bottom" among the EU jurisdictions as CASPs and token issuers may migrate their businesses to countries in which practicing lawyers will be willing to draft accommodating legal opinions.

In this sense, following the analysis by the UK Jurisdiction Taskforce in its Legal Statement on Cryptoassets and Smart Contracts,[189] Low argues that NFTs fall under the category of intangible property called "things in action" and therefore are considered property.[190] This approach was endorsed in several cases in England[191], New Zealand[192] and Singapore[193]. These decisions, when considered NFTs as property, may allow the property rights to be assigned to NFTs and therefore represent an important step towards providing legal certainty to the holders of these assets and CASPs that deal in NFTs.

[187] COM/2020/593 final. Article 81.

[188] IBid. Article 16(2)(d).

[189] UK Jurisdiction Taskforce. 2019. Legal statement on cryptoassets and smart contracts. Pp. 09-12. Accessed on 27.11.2022. Available at URL <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf>.

[190] LOW, Kelvin et al., 2021, as cited in COOPER, Gilead. Digital Assets: Chapter 8 of the Law of Personal Property (3rd edition). Trusts & Trustees, Volume 28, Issue 5, June 2022, Pages 447–450. Accessed on 27.11.2022. Available at URL <https://academic.oup.com/tandt/article/28/5/447/6576852>.

[191] AA v Persons Unknown [2020] 4 WLR 35; Fetch.AI Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm).

[192] Ruscoe v Cryptopia Ltd [2020] NZHC 728; Jonathan Dixon v R - [2015] NZSC 147.

[193] [2022] SGHC 264. Originating Claim No 41 of 2022 (Summons No 1800 of 2022).

Finally, considering the virtual currencies' definition proposed by AMLD5[194], NFTs cannot be considered cryptocurrencies under the Directive. Taking into account that the main characteristic of the NFTs is their non-fungibility and that currencies are inherently fungible, one could argue that NFTs will not be deemed as cryptocurrencies and thus will escape the grasp of the AMLD5. Nevertheless, as previously explained (see chapter V, section 4), they will be subject to MiCA and, in case they represent financial assets, they will also be subject to the EU financial laws.

6.2 Should NFTs be treated as artwork, collectibles, investments or cryptocurrencies for AML/CTF purposes?

As seen above, NFTs could be classified according to the nature of the goods that they represent. In case NFTs represent a financial asset, they could be classified as such, and if they represent digital art or crypto collectibles, they could hold the same legal status as traditional art or collectibles. Moreover, given the unique and non-fungible features of the NFTs, they should not be considered cryptocurrencies - even if they represent assets with financial/investment purposes.

6.3 Considering that NFTs are borderless assets, what are the financial crime risks and how to combat them?

As previously stated (see Chapter IV), when it comes to NFTs, one of the main financial crime risks lies in the fact that they are borderless assets, i.e. assets that can be easily moved from one country to another. Because of this feature and the lack of a regulatory framework that can properly control transactions involving NFTs, they may represent a high financial crime risk[195]. As a highly regulated market, the financial services offered by banks and payment platforms are subject to strict control aiming to combat financial crime. The same cannot be said about NFTs since the respective regulation is still in its early stages.

To solve the cryptoasset regulatory gap within the EU, as seen earlier (see chapter V, section IV), the European Commission recently approved the Digital Finance

[194] Directive (EU) 2018/43. Article 3(18).

[195] Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. P. 09. Accessed on 30.11.2022. Available at URL <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf>.

Package[196], a set of laws to be transposed by the Member States to unify the EU's approach to cryptoassets. The package is part of a new EU Digital Finance Strategy[197] which aims, among others, to eliminate regulatory fragmentation in the Digital Single Market, improve the EU regulatory framework to pave the way for digital innovation and address the risks arising from digital innovation.

Among the laws proposed by the legislation package, special mention should be made of MiCA, which aims to regulate the public offering of cryptoassets, determine which cryptoassets may be traded on a trading platform, create a single licensing of CASPs in the EU, and implement market abuse rules for cryptoasset-based businesses across all Member States by 2024.[198] As seen earlier, this set of rules may unify the legal approach to cryptoassets in the EU and provide legal certainty to stakeholders involved in the cryptoasset business - including those stakeholders specializing in NFTs.

A second significant financial crime risk-aggravating factor arising from the crypto business is the fact that some DEXs allow users with unhosted wallets to exchange cryptoassets without a centralized party that would be obligated to conduct KYC, CDD and AML/CTF checks, offering clear opportunities to layer the proceeds of crime on the blockchain.[199]

Regarding this matter, the Proposal for a Regulation on information accompanying transfers of funds and certain crypto-assets[200] that will review the 2015 Regulation on Transfers of Funds[201] makes it possible to trace the transfers of cryptoassets. These transfers will be treated with the same requirements as cross-border wire transfers, following the FATF Recommendation No. 16 and its interpretive note.[202] The Proposal

[196] European Commission. 2020. Financial Stability, Financial Services and Capital Markets Union. Communication on Digital Finance Package. Accessed on 27.11.2022. Available at URL <https://finance.ec.europa.eu/publications/digital-finance-package_en>.

[197] European Commission. 2020. Communication on a Digital Finance Strategy for the EU. COM (2020) 591 final.

[198] COM/2020/593 final. Preamble, item 5 - Other Elements.

[199] U.S. Department of the Treasury. 2020. Requirements for certain transactions involving certain convertible virtual currency or digital assets. Accessed on 28.10.2022. Available at URL <https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf>.

[200] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets. COM(2021) 422 final.

[201] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

[202] Id. Interpretive Note to Recommendation 16.

reflects the FATF Recommendation No. 15 on new technologies to cover cryptoassets and CASPs, particularly new information obligations for the originator and beneficiary CASPs at both ends of a crypto transfer (i.e. the travel rule).[203]

Considering the above, when the Proposal requires compliance with the travel rule, it is tacitly forbidding the use of unhosted/anonymous wallets. Assuming that these wallets do not retain personal information about their beneficiaries, CASPs would be unable to transmit and receive this mandatory data, and therefore would be effectively prevented from conducting transactions originating from or directed to these anonymous wallets.

In a more direct approach, the Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing establishes that the provision and custody of anonymous crypto wallets will be prohibited in the EU.[204] The Draft Regulation also states that CASPs, like credit and financial institutions, shall be deemed obliged entities in the upcoming Regulation.[205] Bearing this in mind, if the Draft Regulation is transposed to national laws, the high financial crime risk arising from unhosted wallets may be mitigated.

A third risk-aggravating factor related to cryptoassets lies in the availability of Crypto ATMs that are connected to a given DEX and allow their users to buy and sell cryptoassets using cash.[206] Taking into account the fact that AMLD5 states that virtual currency platforms such as DEXs should be considered obliged entities for AML/CTF purposes, CASPs that exchange exclusively virtual currencies could be considered obliged entities under the Directive and therefore would need to comply with reporting and transaction monitoring obligations. However, when it comes to NFTs, the Directive could not apply based on the fact that NFTs are not to be considered virtual currencies.

The Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing establishes that CASPs, like

[203] SCHMIDT, Alicia. 2022. Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model. International Journal of Law and Information Technology, Volume 29, Issue 4, Pages 332-363. Accessed on 17.11.2022. Available at URL <https://academic.oup.com/ijlit/article-abstract/29/4/332/6516792?redirectedFrom=fulltext>.

[204] Proposal for a Regulation of the European Parliament and of he Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (COM/2021/420 final). Recital 93.

[205] Id. Article 3(3)(g).

[206] Coinhub ATM. Accessed on 28.10.2022. Available at URL <https://coinhubatm.com/>.

credit and financial institutions, shall be deemed obliged entities in the upcoming Regulation.[207] Moreover, it states that credit/financial institutions and CASPs will be obligated to conduct CDD when initiating or executing a transfer of funds, or a transfer of cryptoassets whose value exceeds EUR 1,000.00.[208]

By considering crypto ATM providers as CASPs and therefore obliged entities, as well as requiring CDD to be performed on all transactions above EUR 1,000.00 (individual transactions or transactions that together exceed this amount and are connected), the Draft Regulation, if approved, could contribute to significantly reducing the risk arising from the availability of crypto ATMs throughout the EU.

To further reduce the risks of financial crime, the EU could develop an impact study to consider the possibility of banning cash deposits in these ATMs, therefore allowing crypto ATM users to only withdraw cash from these machines.[209] Considering all CASPs will have to perform KYC on their users and, to withdraw cash from a crypto wallet, those users need to be properly registered and identified by the CASP and carry unique and personal identifiers such as password and/or biometrics, one might argue that withdrawing cash from crypto ATMs represents a lesser risk factor than depositing it.

A fourth increased financial crime risk related to NFT trading is the possibility of settling P2P transactions using the blockchain without the use or involvement of a CASP or other obliged entity.[210] Illicit actors may exploit the lack of an obliged intermediary to layer their crime proceeds precisely because there is no entity obliged to conduct KYC, CDD and AML/CTF checks. Furthermore, the encrypted and unrecorded transactions in a P2P network may create additional obstacles to financial crime investigations particularly when it comes to layering the proceeds of crime.[211]

The existence of P2P transactions is perhaps one of the most significant gaps in EU legislation in the fight against financial crime on the blockchain. As previously discussed

[207] Id. Article 3(3)(g).

[208] Id. Article 15(2).

[209] FATF. 2021. Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers. Paragraph 43.

[210] FATF. 2022. International Standards on Combating Money-laundering and the Financing of Terrorism & Proliferation. Paragraph 54.

[211] : Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. P. 09.

(see chapter V, section 5), the FATF Guidance for an RBA for VAs and VASPs is one of the few soft law instruments highlighting the ML/TF risks related to P2P transactions. It establishes a handful of tools and measures that countries may employ to mitigate the risks arising from P2P transactions[212] and suggests that they implement additional measures[213] on the national level, such as creating controls that facilitate the visibility of P2P activity and establishing ongoing enhanced supervision of VASPs and entities whose business has a special focus on unhosted wallets transactions, as well as imposing additional AML/CTF requirements on them.

Finally, NFTs may pose a high risk of tax evasion since they are mostly exchanged as crypto-collectibles and digital art. This characteristic, added to their significant price fluctuation, makes it difficult to appraise their valuation, a key factor to calculate the overall capital and capital gains for tax purposes.[214] Government agencies also do not seem to fully understand the concept of NFTs and may not be able to differentiate them from fungible cryptoassets, which may add to the frustration and confusion facing the industry.[215]

The disparity between the Member States' tax laws also may be contributing to tax evasion within the Union. Moreover, the lack of a reporting framework that allows tax authorities to monitor the ownership and transfers of cryptoassets may lead to an increased risk of tax evasion in the EU and consequential revenue losses.

To address these discrepancies and prevent such risks, the EU is working on the DAC-8[216] which will amend the current Directive on Administrative Cooperation (DAC)[217] to expand the information exchange framework in the field of taxation to include cryptoassets and e-money. Furthermore, on a global level, the OECD proposed a Crypto-

[212] Id. Paragraph 105.

[213] Id. Paragraph 106.

[214] GELLMAN, Philippe. 2021. Blockchain: The New Art House, ITNOW, Volume 63, Issue 3, Autumn 2021, Pages 18–19. Accessed on 03.12.2022. Available at URL <https://doi.org/10.1093/itnow/bwab070>.

[215] HOUSER, Kimberly et al. 2022. Utah Law Review. Navigating the Non-Fungible Token. Accessed on 05.11.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4055535>.

[216] European Commission. 2021. *Tax fraud & evasion – strengthening rules on administrative cooperation and expanding the exchange of information*. Accessed on 19.11.2022. Available at URL <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en>.

[217] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.

Asset Reporting Framework (CARF)[218], which contains amendments to the Organization's Common Reporting Standard[219] (CRS).

The CARF implementation package consists in rules that shall be transposed into domestic laws aiming to collect information from CASPs and provide a framework for bilateral or multilateral authority agreements and arrangements for the automatic exchange of information regarding cryptoassets.[220] The Framework provides for a CASP definition and gives examples of CASPs that suggest P2P cryptoasset exchange platforms, which may escape the grasp of MiCA, will be subject to the rules provided for in the CARF.[221]

In other words, P2P platforms specializing in NFTs may not be expressly covered by MiCA and the laws that regulate the transfer of funds, but when it comes to the requirement to report cryptoasset transactions for combating tax evasion, in case the OECD's member countries enforce the CARF, these platforms will need to comply with the Framework and therefore report transactions involving NFTs (even if they are settled through P2P transactions).

Conclusively, the regulatory framework to combat tax evasion employing cryptoassets is an important step towards preventing this crime from being committed by crypto holders or facilitated by CASPs. Provided the DAC-8 is drafted and approved, and the CARF is followed by the OECD's member countries, the risk of tax evasion using NFTs will potentially be mitigated.

6.4 What may be improved so that EU law is better prepared for the changes brought by DeFi, particularly the NFT trading business?

Regarding the financial crime risks related to the NFT business, one may argue the regulatory room for improvement may involve: the fact that AMLD5 only applies to

[218] OECD. 2022. Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard. P. 09. Accessed on 24.11.2022. Available at URL

<https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm.>.

[219] OECD. 2014. *Standard for Automatic Exchange of Financial Account Information in Tax Matters*. Accessed on 24.11.2022. Available at URL <http://dx.doi.org/10.1787/9789264216525-en>.

[220] Id. Executive Summary. Pp. 06-07.

[221] CUTLER, Jonathan. 2022. CRS for Crypto: Demystifying the OECD's Proposed Crypto-Asset Reporting Framework. Journal of Taxation of Financial Products (Vol. 19, Issue 2). P. 11. Accessed on 25.11.2022. Available at URL <link.gale.com/apps/doc/A715600236/AONE?u=ull_ttda&sid=bookmark-AONE&xid=22e71f82>.

virtual currencies and considers virtual currency service providers (VCSPs) as obliged entities; AMLD5 did not provide for the prohibition for maintaining anonymous accounts/wallets in VCSPs; the lack of hard laws to prevent financial crime through P2P transactions; the absence of a specific classification for NFTs in MiCA and the fact that MiCA left the cryptoasset classification task to the private sector via a legal opinion.

As previously seen (see chapter V, section 1), VCSPs that provide exchange services between virtual and fiat currencies, as well as custodian wallet providers, should be considered obliged entities for AML/CTF purposes under AMLD5.[222] Moreover, considering the virtual currencies' definition proposed by the Directive,[223] NFTs cannot be considered as so and may not be under its scope. A possible solution to this legal gap could be achieved if AMLD5 were amended to bring to its scope not only cryptocurrencies, but all types of cryptoassets as provided for in MiCA.[224]

Although AMLD5 has brought virtual currencies and VCSPs under its scope, it did not provide for the prohibition of maintaining anonymous accounts/wallets in VCSPs. As previously discussed, even though AMLD5 put an end to the anonymity of bank accounts, passbooks and safe deposit boxes, it did not extend this prohibition to VCSPs.[225] One may argue that an alternative to close this legal loophole could be to amend the Directive to expressly extend this obligation to VCSPs.

As seen above (see chapter V, section 5), the FATF Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers[226] is one of the few soft law instruments highlighting the ML/TF risks related to P2P transactions. Although the RBA is an important step towards mitigating the risks arising from P2P transactions, because it is a soft law instrument, it does not bind any of the member countries. From an EU perspective, one may argue that a possible solution to this legal gap could arise if P2P transactions were provided for in amendments to the Regulation on Transfer of Funds[227]

[222] Directive (EU) 2015/849. Article 2(1)(g)(h).

[223] Id. Article 3(18).

[224] COM/2020/593 final. Article 3(2).

[225] Directive (EU) 2015/849. Article 10(1).

[226] FATF. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.

[227] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets. COM(2021) 422 final.

or to the new Regulation on AML/CTF[228]. Alternatively, a specific Proposal could be drafted to provide for the risks arising from those transactions.

Finally, another improvement factor lies in the absence of a specific classification for NFTs in MiCA. As previously discussed (see chapter V, section 4), MiCA inserted NFTs in a "catch-all" category of cryptoassets known as the "other" tokens.[229] The legal provisions applicable to this category of cryptoassets will only apply to those NFTs that do not represent financial instruments under other EU financial laws such as Directive 2014/65/EU.[230] A possible solution for this classification deficiency could be to put the national supervisory authorities described in MiCA[231] responsible for differentiating which types of NFTs will fall under the scope of the Proposal and which will be subject to other EU financial laws.

[228] Proposal for a Regulation of the European Parliament and of he Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (COM/2021/420 final).

[229] COM/2020/593 final. Article 4.

[230] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[231] COM/2020/593 final. Article 81.

7 Conclusion

DeFi is a phenomenon that will inevitably be incorporated into global financial relations. In a world that is preparing for Economy 4.0, a broad discussion about innovation is needed so that society can benefit from it and efficiently address the risks arising from emerging technologies. Cryptoassets and particularly NFTs are important elements of DeFi that may empower the art market and the creative industry.[232] Furthermore, they generate wealth by helping artists, collectors and interested parties negotiate in a secure and decentralized environment.[233] However, as previously exposed, they may ease the layering of the crime proceeds on the blockchain, raising financial crime concerns due to the weak regulation and the anonymity offered by DLT.[234]

As seen in chapter II, the 2022 NFT market crash, despite imposing losses for investors who seek financial reward for their involvement in the market, may contribute to NFTs generating not only financial return but effectively contributing to building a Decentralized Society[235] (DeSoc). Currently, it is not possible to predict the future of NFTs, but if the trends advocated by the main players in the business are confirmed, we could see a less speculative market involved in building a sustainable ecosystem for NFTs and, above all, in providing usefulness and security for business and interpersonal relationships on the blockchain.

The impact of regulation on innovation depends on the balance between the compliance costs and the incentive effect proposed by the regulation in place. As previously discussed (see chapter IV), when regulation is introduced, the compliance costs may reduce the available resources for R&D in a manner similar to taxation[236]. In the long run, however, an efficient regulatory framework that entails flexible solutions may reduce

[232] CHEVET, Sylve. 2018. *Blockchain Technology and NonFungible Tokens: Reshaping value chains in creative industries*. Pp. 50-52. Accessed on 22.10.2022. Available at URL <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212662>.

[233] Forbes. August 2021. NFT Sales Top $1.2 Billion In July As Demand For Blockchain Games Soars. Accessed on 04.12.2022. Available at URL <https://www.forbes.com/sites/ninabambysheva/2021/08/04/nft-sales-top-12-billion-in-july-as-demand-for-blockchain-games-soars/>.

[234] Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. P. 09. Accessed on 30.11.2022. Available at URL <https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf>.

[235] Id. P. 01.

[236] BLIND, Knut. 2012. *The Impact of Regulation on Innovation*. P. 10. Accessed on 28.10.2022. Available at URL <https://media.nesta.org.uk/documents/the_impact_of_regulation_on_innovation.pdf>.

the regulatory burden, create incentives for R&D and may decrease the risk of financial losses due to non-compliance with the new EU laws on cryptoassets.

Taking into account the financial crime risks related to cryptoassets, as previously seen (see chapter V, introduction), the European Commission recently presented an ambitious new package of legislative proposals[237] to combat ML and TF in the EU, with a special focus on monitoring financial transactions of cryptoassets. The Commission's goal is to improve the detection of suspicious transactions and activities in the financial system, considering new and emerging technologies such as cryptoassets.

This package includes proposals for: a Regulation establishing a new AML/CTF authority[238]; a Regulation on AML/CTF[239] containing applicable rules in the areas of CDD and beneficial ownership; the sixth Directive on AML/CTF[240] (AMLD6) containing general provisions that shall be transposed into national law, (e.g. rules on national supervisors and Financial Intelligence Units (FIUs)); and a revision of the Regulation on Transfers of Funds[241] to enable the tracing of cryptoassets.

In addition to these regulatory instruments, several others have been proposed or are being updated to address the risks arising from the cryptoasset business and the potential to facilitate the commission of financial crimes on the blockchain. On the one hand, from an EU perspective, one may highlight the Proposal for a Regulation on Markets in Cryptoassets[242] (MiCA) and the Proposal for a Directive on Administrative Cooperation[243] (DAC8) to combat tax fraud and evasion via cryptoassets. On the other

[237] European Commission. 2021. *Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules*. Accessed on 06.11.2022. Available at URL <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690>.

[238] Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. COM/2021/421 final.

[239] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. COM/2021/420 final.

[240] 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. COM/2021/423 final.

[241] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast). COM/2021/422 final.

[242] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final.

[243] European Commission. 2021. Tax fraud & evasion – strengthening rules on administrative cooperation and expanding the exchange of information. Accessed on 30.11.2022. Available at URL

hand, from a global perspective, the following soft law instruments may be highlighted: the FATF Recommendations[244] and the updated Guidance for a Risk-Based Approach for VAs and VASPs[245]; and the OECD's Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard (CARF).[246]

As already explained (see chapters V and VI), with some minor exceptions and points for improvement, the EU regulatory framework is prepared to encourage innovation from emerging technologies while providing satisfactory legislation to combat financial crimes committed on the blockchain. The desired approval of the EU legislation regarding cryptoassets, together with respect for the guiding principles established in the soft law provisions proposed by the OECD and FATF will potentially provide a satisfactory level of legal certainty for crypto stakeholders, as well as contribute to slowing the advance of financial crimes employing cryptoassets.

To conclude, whether through: the ban on maintaining crypto anonymous wallets and the incorporation of CASPs into the list of obliged entities that may be imposed by the New Regulation on AML/CTF;[247] the CASPs' mandatory compliance with the travel rule as proposed by Revision of the 2015 Regulation on Transfers of Funds;[248] the cryptoasset classification and regulatory framework proposed by MiCA[249]; the FATF Guidance on how to address the risks arising from P2P transactions;[250] and the measures for mandatory reporting of transactions involving cryptoassets and combating tax evasion that may be

<https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en>.

[244] FATF (2012-2022). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France. Accessed on 30.11.2022. Available at URL <www.fatf-gafi.org/recommendations.html>.

[245] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. Accessed on 30.11.2022. Available at URL <www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html>.

[246] OECD (2022). Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, OECD, Paris. Accessed on 30.11.2022. Available at URL <https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm.>.

[247] COM/2021/420 final. Article 58.

[248] COM(2021) 422 final. Article 14(1)(2).

[249] COM/2020/593 final.

[250] FATF. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paragraph 105.

proposed by the EU in DAC-8[251] and that were suggested by the OECD in the CARF;[252] the EU will be able to remain one of the global pioneers in regulating emerging technologies, while protecting society from the harms of financial crime, safeguarding fundamental rights and maintaining legal certainty in the crypto business within the Union.

[251] European Commission. 2021. *Tax fraud & evasion – strengthening rules on administrative cooperation and expanding the exchange of information*. Accessed on 19.11.2022. Available at URL <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en>.

[252] OECD. 2022. *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*. Accessed on 24.11.2022. Available at URL <https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm.>.

Bibliography

Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg. P. 09.

[2022] SGHC 264. Originating Claim No 41 of 2022 (Summons No 1800 of 2022).

AA v Persons Unknown [2020] 4 WLR 35; Fetch.AI Ltd v Persons Unknown Category A [2021] EWHC 2254 (Comm).

ALHOSANI, Walled. 2016. Anti-Money Laundering : A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Unit. Pp. 3-4.

AMBERDATA. DeFi and the Transformation of Institutional Finance.

BARLOW, Justin. 2021. Axie Infinity: A Deep Dive.

BLIND, Knut. 2012. The Impact of Regulation on Innovation.

Bloomberg. 2022. NFT Market Surpassed $40 Billion in 2021, New Estimate Shows.

BUSCH, Danny. 2021. The Future of EU Financial Law. Capital Markets Law Journal, Volume 17, Issue 1, January 2022, Pages 52–94.

BUTERIN, Vitalik et. al. 2022. P. 02-03. Decentralized Society: Finding Web3's Soul.

BUTERIN, Vitalik. 2014. P. 23. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

Canadian Securities Administration. Types of Crypto Assets.

CHANCE, Clifford. 2020. Security Token Offerings - A European Perspective on Regulation.

CHEN, James. 2022. What Is an Exchange-Traded Fund (ETF)?

CHEVET, Sylve. 2018. Blockchain Technology and NonFungible Tokens: Reshaping value chains in creative industries.

Christie's. 2021. A Record Breaking Year at Christie's: 2021 in numbers.

Coin ATM Radar. Bitcoin ATM Map.

Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.

CUTLER, Jonathan. 2022. CRS for Crypto: Demystifying the OECD's Proposed Crypto-Asset Reporting Framework. Journal of Taxation of Financial Products (Vol. 19, Issue 2).

DELVENTHAL, Shoshanna. 2019. Be Wary of Cryptocurrencies: Ethereum Founder.

Deutsche Welle. 2022. Deutsche Bank under pressure after money laundering raids.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.

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.

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

EU Blockchain Observatory and Forum. NFT – Legal Token Classification.

EUROJUST. 2022. Takedown of Online Investment Fraud Responsible for Losses of Several Million Euros.

European Commission. 2018. Towards fair, efficient and growth-friendly taxes.

European Commission. 2020. Communication on a Digital Finance Strategy for the EU. COM (2020) 591 final.

European Commission. 2020. Financial Stability, Financial Services and Capital Markets Union. Communication on Digital Finance Package.

European Commission. 2021. Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules.

European Commission. 2021. Tax fraud & evasion – strengthening rules on administrative cooperation and expanding the exchange of information.

Europol. 2021. Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

Europol. 2021. Cryptocurrencies - Tracing the Evolution of Criminal Finances.

FATF (2012-2022). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France.

FATF (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris.

FATF. 2018. Financing of Recruitment for Terrorist Purposes.

FATF. 2021. Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

FATF. Report to G20 on So-called Stablecoins.

FATF. Risk-based approach for the bank sector.

FERREIRA, Agata. The Curious Case of Stablecoins—Balancing Risks and Rewards? Journal of International Economic Law, Volume 24, Issue 4, December 2021, Pages 755–778.

FINEMATICS - DECENTRALIZED FINANCE EDUCATION. History of DeFi - From Inception to 2021 and Beyond.

Footprint Analytics. 2022 Q2 NFT Industry Report.

Forbes. August 2021. NFT Sales Top $1.2 Billion In July As Demand For Blockchain Games Soars.

FRANGELLA, Emilio. 2019. Crypto Black Thursday: the Good, the Bad and the Ugly.

FRANKENFIELD, Jake. 2022. Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain.

FRAZIER, Liz. FORBES. 2021. The Coronavirus Crash of 2020 and the Investing Lesson it Taught Us.

GELLMAN, Philippe. 2021. Blockchain: The New Art House, ITNOW, Volume 63, Issue 3, Autumn 2021, Pages 18–19.

HAYES, Adam. 2022. Who is Satoshi Nakamoto?

HELMINEN, Marjanna. 2021. EU Tax Law - Direct Taxation.

HOUSER, Kimberly et al. 2022. Utah Law Review. Navigating the Non-Fungible Token.

HOWELL, James. 101 Blockchains. 2022. What Are Governance Tokens and Why do They Matter?

IREDALE, Gwyneth. 101 Blockchains. 2021. ERC20 Vs. ERC721 - Key Differences. Accessed on 21.10.2022. Available at URL <https://101blockchains.com/erc20-vs-erc721/>.

Joined cases C-37/20 Luxembourg Business Registers and C-601/20 Sovim.

KARASEK-WOJCIECHOWICZ, Iwona. Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. Journal of Cybersecurity, 2021, 1–28.

KOSTER, Harold. 2020. Journal of Money Laundering Control. Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework.

LEE, Edward. 2021. The Cryptic Case of the CryptoPunks Licenses: The Mystery Over the Licenses for CryptoPunks NFTs.

LOW, Kelvin et al., 2021, as cited in COOPER, Gilead. Digital Assets: Chapter 8 of the Law of Personal Property (3rd edition). Trusts & Trustees, Volume 28, Issue 5, June 2022, Pages 447–450.

LYONS T. et. al. 2019. Regulatory Framework of Blockchains and Smart Contracts.

MACKENZIE, Alice. 2022. Bitcoin ATMs - An Easy Guide to Bitcoin Teller Machines.

MAIA, Guilherme et al. 2021. MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). Forthcoming article in "Blockchain and the law: dynamics and dogmatism, current and future".

MARCOBELLO, Mason. 2022. How Rare Pepes NFTs Reclaimed Pepe the Frog - And Why They Remain Relevant.

MOYLAN, Christopher Ignatius. 2022. OECD's Proposed Crypto-Asset Reporting Framework - A Critique.

Nonfungible.com. 2021. Yearly NFT Market Report

OECD (2022). Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, OECD, Paris.

OECD. 2014. Standard for Automatic Exchange of Financial Account Information in Tax Matters.

OECD. 2022. Paying the Price of War.

ORDANO, Esteban. 2017. Decentraland Whitepaper.

POPESCU, Andrei-Dragos. 2020. Decentralized Finance (DeFi) - The Lego of Finance.

POPESCU, Andrei-Dragos. 2021. Non-Fungible Tokens (NFT) - Innovation beyond the craze. Proceedings of Engineering & Technology Journal - IBEM 2021.

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. COM/2021/423 final.

Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (COM/2021/420 final).

Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.

Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. COM/2021/421 final.

Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast). COM/2021/422 final.

QIN, Kaihua et al. 2021. CeFi vs. DeFi - Comparing Centralized to Decentralized Finance.

Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

ROSE, Kalle Johannes. 2021. Lack of clarity in recent Criminal Law Directive gives ground for significant expansion of EU money laundering regulation.

ROSENBERG, Eric. Investopedia. 2022. How to Invest in Crypto without Buying Crypto.

ROSENFELD, Meni. 2012. Overview of Colored Coins.

ROSSEL, Lucia et. al. 2021. The Implications of Making Tax Crimes a Predicate Crime for Money Laundering in the EU.

Ruscoe v Cryptopia Ltd [2020] NZHC 728; Jonathan Dixon v R - [2015] NZSC 147.

SADIKU, Matthew et. al. 2018. Journal of Scientific and Engineering Research. Smart Contracts: A Primer.

SCHMIDT, Alicia. 2022. Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model. International Journal of Law and Information Technology, Volume 29, Issue 4, Pages 332-363.

SERADA, A. et al. 2020. CryptoKitties and the new ludic economy : how blockchain introduces value, ownership, and scarcity in digital gaming.

SILVA, Patrícia Godinho. 2019. New Journal of European Criminal Law. Recent developments in EU legislation on anti-money laundering and terrorist financing.

SITOMPUL, Anggia Debora. 2022. Journal of Pancasila and Law Review. Imposition of Tax Law on Cryptocurrencies and NFT in Indonesia.

Swiss Financial Market Supervisory Authority. 2019. Federal Council wants to further improve framework conditions for DLT/blockchain.

Tax Justice Network. November 2022. EU court returns EU to dark ages of dirty money.

U.S. Department of the Treasury. 2020. Requirements for certain transactions involving certain convertible virtual currency or digital assets.

UK Jurisdiction Taskforce. 2019. Legal statement on cryptoassets and smart contracts.

UNISWAP DOCS. Smart Contracts.

WANG, Tracy. Coindesk. 2022. Crypto Sell-Off Wipes $700B From Industry Market Cap So Far in 2022.

WILLIAMS, Lara. Investment Monitor. 2022. The NFT Market Has Collapsed (But That May Not Be a Bad Thing).

ZENO, A. 2022. The beginning of NFTs - A Brief History of NFT Art.

ZETZSCHE D. et. al. 2017. The Distributed Risks of Distributed Ledgers: Legal Risks of Blockchain.

ZETZSCHE, DIRK A. et al. 2020. University of Luxembourg Law Working Paper Series No. 2020-018. The Markets in Crypto-Assets Regulation(MICA) and the EU Digital Finance Strategy.