# The Anti Money Laundering Regulation of Crypto-assets in Europe

## A Critical Analysis

Giulio Soana

**Supervisors:**

Prof. Antonio Gullo – LUISS Guido Carli University

Prof. Michele Panzavolta – KU Leuven

*Alla mia famiglia per avermi sempre sopportato e supportato*

# Table of Contents

# Glossary

**Application specific integrated circuit (ASIC):** a hardware specifically designed to perform a certain function. In the blockchain field it refers to hardware specifically designed to perform mining function.

**Asymmetric Cryptography:** technique that allows to party to securely share encrypted messages without having to share a common description key.

**Bitcoin**: crypto-asset created. Launched in 2009 by Satoshi Nakamoto, which real identity is still unknown, it is rooted in a permissionless blockchain and a proof of work consensus protocol.

**Block-reward:** fixed amount of newly minted crypto-assets given to the miner that has added a new block to the chain as a reward for its activity.

**Central Bank Digital Currencies (CBDC):** a digital currency issued directly by the Central Bank which translates the characteristics of a fiat currency in the digital arena. CBDCs are not classified as crypto-assets.

**Consensus Protocol:** set of rules dictating how a decentralized network establishes which information is valid and can be validly added to the common ledger.

**Crypto-assets (in this thesis):** a token which functioning is rooted in a decentralized blockchain network.

**Crypto-asset Service Provider (CASP):** service provider of the crypto-market which is included among the covered entities under the anti-money laundering regulation.

**Cypherpunks**: political and philosophical movement formed in the early nineties in the San Francisco area around the figures of Timothy May, Eric Hughes, and John Gilmore.

**Custodian Wallet:** service provider that safeguards the crypto-assets of the customer retaining access to its private key.

**Decentralized Autonomous Organizations (DAO):** organization rooted in a bundle of smart contracts that operate autonomously only following the rules engraved in its code – meaning without any centralized human operator being able to control or influence its actions.

**Decentralized Finance (DeFi):** decentralized autonomous organizations that offer financial services (loan, investment, etc.).

**Distributed Ledger Technology:** network rooted in a distributed a shared ledger safeguarded by a number of nodes which cooperate in its maintenance and update. Blockchain constitutes a subset of DLTs as a network where not only the access but also the control of the ledger is decentralized.

**Ethereum**: Ethereum is a permissionless blockchain launched in 2014 by Vitalilk Buterin. Ethereum, which native crypto-asset is Ether, allows the computation of smart contracts which are then executed in a decentralized fashion.

**Financial Action Task Force (FATF):** independent Agency part of the OECD, based in Paris and founded in in 1989 by the G7. It is widely regarded as the international standard setter in the anti-money laundering field. It operates through Recommendations and mutual evaluation processes.

**Financial Intelligence Unit (FIU):** national, independent agencies tasked with the supervision and implementation of the anti-money laundering regulation as well as with the reception and analysis of SARs. Depending on the national regime the FIU can be incardinated in different sections of the public administration (e.g., Central Bank, Law Enforcement Authority, Ministry of Justice).

**Hard fork**: a permanent split in the blockchain that causes the coexistence of two parallel ledgers.

**Hash Function:** a mathematical function that converts an input of arbitrary length into an output of a fixed length.

**Initial Coin Offering (ICO):** funding instrument mainly used by crypto-related startups. It consists in the emission of a native crypto-assets, the buyers of the token are afforded certain preestablished rights. Depending on the rights afforded to the token holders these can be assimilated to stocks or to bonds.

**Know Your Customer (KYC):** activity carried out by a covered entity to profile their customer in order to monitor their activities and spot suspicious one.

**Layer Two Solutions:** implementation that are rooted in an underlying network not necessarily controlled and developed by the developers of the layer two solution.

**Mining:** activity of solving complex mathematical problems, within the framework of the Proof of Work consensus protocol, to earn the right to add a new block to the blockchain and receive the corresponding block-reward. The individuals/corporations performing such activity are called miners.

**Non-custodian wallet:** service provider that safeguards the crypto-assets of the customer without retaining access to its private key.

**Non-fungible Token (NFT)**: a blockchain-based token computed to be unique. The unicity can be due to the connection of such token with a physical or digital object established through a smart contract.

**Oracle (blockchain):** third party that acts as source of information for the functioning of a smart contract. When, to reach a decision, the smart contract has to act according to external information, the latter can be connected to an oracle that feeds them such information. An oracle can be any source of information from a human (as an arbiter or mediator) to a website (as a weather forecast or newspaper)

**Peer-to-peer:** any type of technology that allows two or more parties to communicate and/or exchange values directly, meaning in the absence of an intermediary.

**Permissioned Blockchain:** decentralized network which allows the establishment of a centralized centre of governance.

**Permissionless Blockchain:** fully decentralized network where anyone can join and see the ledger without any restriction.

**Private key (Blockchain):** the private key is an alphanumeric string that enables to send the crypto-assets associated with an account. It can be likened to a password.

**Proof of Work:** type of consensus protocol used in Bitcoin.

**Public key:** alphanumeric string derived, through hashing, from the private key. It is used to compute, through a second layer of hashing, the crypto-asset address, in turn, used to identify the account on the blockchain.

**Self-hosted wallet:** crypto-asset address not managed by any crypto-asset service provider, hence, only controlled by the owner of the connected private key.

**Smart contracts (blockchain):** self-executing software running on a blockchain network.

**Suspicious Activity Report (SAR):** report filed by the covered entity to the Financial Intelligence Unit when a suspicious activity is identified.

# Introduction

The expression "follow the money" articulates one of the cardinal strategies of modern policing. This strategy views the monitoring and analysis of money and value flows as a key tool in the prevention, investigation, and repression of crime. Within this perspective, the identification and forfeiture of illicit proceeds are primary tools for police forces. To this end, not only law enforcement authorities but also a growing array of private institutions are called to take an active role in the fight against "criminal money". Eminently, the lemma "follow the money" is implemented through a two-pronged approach. The classic investigative, reactive approach is coupled with a preventive strategy based on the analysis of financial data aimed at spotting suspicious transactions. This second prong engages private institutions in an active search for suspicious activities to then be reported to investigators. Administrative law – on which the preventive duties are based on – blends with criminal law to create a holistic approach to the fight against illicitly sourced money.

Two fundamental macrotrends underly this policing strategy, one ideological and one architectural.

First, the emergence of an economistic approach to criminal justice. Ideologically rooted in the rational-choice theory and in a capitalistic view of the individual as *homo economicus*, this approach sees economic incentives as key to the criminal rationale. By hindering the ability of the perpetrator to enjoy the proceeds of their crimes, the policy-maker aims at reducing the rationality of criminal activity.[1] In a pervasively capitalistic society money is the key metric for the evaluation of success,

[1] This vision of the criminal and connected goal is clearly stated by the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) "*With few exceptions, criminals are motivated by one thing - profit. Greed drives the criminal, and the end result is that illegally-gained money must be introduced into the nation's legitimate financial systems*", see FinCEN, *What is Money Laundering?,* FinCEN website, https://www.fincen.gov/what-money-laundering; on a similar note see J. Cassara, *Money laundering and illicit financial flows,* 2020, 1, "*criminals, criminal organizations, kleptocrats and some businesses and corporations are typically motivated by greed (…) the criminal themselves, common sense, and criminal science all tell us that the aim of these activities is not crime itself – but the proceeds of crime";* V. Manes*, Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale,* in *Rivista Trimestrale di Diritto Penale dell'economia,* 2004, 1, "*Il riciclaggio è un nodo essenziale, strategico, nell'approccio al tema della criminalità organizzata. E ciò perché, in genere, la forza motrice di ogni associazione criminale è il profitto*".

criminals are seen as no different. Within this perspective, striking their economic proceeds is perceived as hitting where it hurts the most. Furthermore, the identification of illicit money flows is seen as a crucial first step in the detection of the underlying criminal activity. Law enforcement authorities can use financial data to uncover illicit endeavours and piece together criminal networks.

Second, globalization and digitalization have pushed markets towards centralized, macro-organizations. Particularly, digital environments and financial markets, due to network effects, are mostly oligopolies with few entities controlling the lion's share of the market. This conformation of the market has led to an increasing reliance on these entities by the policymaker. Policing is increasingly delegated by the State to private enterprises which are tasked with the protection of a diverse array of interests through risk-based models – so-called compliance regulation.[2] Examples of such a policy trend are, at the European level, the Network Infrastructure Security Directive (NIS), the General Data Protection Regulation (GDPR), and the Digital Services Act (DSA).

A key product of this strategy is the anti-money laundering regulation. Emerged in the United States during the second decade of the twentieth century, anti-money laundering has become central for modern criminal policing.[3] Its core objective is preventing criminals from integrating the proceeds of their illicit activity into the licit market.[4] To this end, the anti-money laundering regulation introduces a decentralized alarm system, through the regulation of the intermediaries that control the value exchange infrastructure – such as banks, insurances companies, investment funds. The aim is to detect, investigate, and freeze funds of illicit origin.

Within this policy framework, the present analysis will explore how the legislator has responded to the introduction of blockchain technology and crypto-assets. As we will detail, blockchain introduces a new architecture for digital exchanges of value. One that substitutes the central intermediary with a decentralized network of cooperating nodes. By reshaping the architecture of digital exchange systems, blockchain undermines the fundamental premise underlying the

[2] See A. Gullo, *Compliance*, in *Archivio Penale*, 1, 2023, 1.

[3] V. Manes*, Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale,* cit., 2.

[4] For the connection between money laundering prevention and rational choice theory, N. Gilmour, *Understanding the practices behind money laundering–A rational choice interpretation,* in *International Journal of Law, Crime and Justice,* 44, 2016.

preventive prong of the anti-money laundering policy strategy: the necessary intermediation of digital exchanges of value.

The primary aim of the present research is to critically examine the impact of crypto-assets and blockchain on the financial monitoring infrastructure and the connected policy responses. Due to the disruptive nature of blockchain's transaction model, this is a field that has known a great degree of innovation, particularly in Europe. The present decade will be fundamental in the definition of a European policy strategy for crypto-assets. The introduction of the Market in Crypto-asset Regulation (MiCaR) – the first comprehensive regulation of crypto-assets worldwide – and the upcoming Anti-money Laundering Package will shape how the Union approaches crypto-assets and its ability to reap their benefits while mitigating the risks.

However, the present research also has a second, larger, purpose. Digitalization is altering the physiognomy of the world and human action. Rules that have been regarded as essential to human existence for centuries are now called into question. For instance, digital interaction systems allow continuous non-local exchanges freeing humans from their corporeal boundaries, artificial intelligence promises to create non-human autonomous decision makers. Within this changing architecture, the validity of legal tenets developed across eras is challenged forcing the legislator to reimagine its strategies in an unprecedented fashion. Taking anti-money laundering as a case study, the blockchain, by introducing the possibility to exchange value digitally in the absence of an intermediary, challenges the previous intermediary-based legislative strategy.[5] The text will analyse how, and if, the policy maker has adapted to this new playing field. The perspective of the text is that a simple reiteration of pre-existing models is not adequate in the presence of fundamental architectural modifications. The legislator cannot simply stick to an "everything changes, nothing changes" approach. Rather, it should proactively engage with such architectures and imagine new solutions rooted in them. The ability to reinvent its strategy, and even its fundamental tenets, is key for the law to survive in a world that is changing in such a profound manner.

It is with this double perspective that we invite the reader to approach the present analysis.

[5] A. Minto, *The legal characterization of crypto-exchange platforms*, in *Global Jurist,* 22/1, 2021, 150 -151, "*In general terms, the absence of centralised intermediaries who carry out transactions on behalf of customers has led to a lack of transparency in the management of the financial system, which significantly hinders the implementation of traditional anti-money laundering measures*".

Before commencing the analysis, it is necessary to delineate the playing field and define the fundamental elements of the anti-money laundering legislation. The present text will focus solely on the preventive prong of money laundering. The legislation analysed is the one aimed at creating the abovementioned decentralized alarm system through the regulation of intermediaries. Therefore, key to our analysis will be which intermediaries the policymaker has identified within the crypto-market as covered entities and how compliance duties have been extended to them. The repressive prong of anti-money laundering is, hence, out of our scope. Section one of the present chapter provides for a normative and criminological definition of money laundering. Section two details the historical development of the money laundering regulation. Section three presents the structure of the text. Section four details the methodology.

## 1. Understanding money laundering

Money laundering can be defined as a crime consisting in one or more actions carried out by an individual or a group to disguise the illicit origin of the proceeds of a crime.[6]

[6] At a supranational level several definitions have been provided. The most relevant for our ends are the ones provided by the Palermo Convention – United Nations, *United Nations Convention against Transnational Organized Crime and the Protocols Thereto,* 15 November 2000, which is directly referenced as legal basis by the Financial Action Task Force in its Forty Recommendations - Financial Action Task Force, *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations,* Paris, 2012, 12 – and by the European Directive on combating money laundering through criminal law of 2018 - Directive of the European Union, 23rd October 2018, n. 1673. The Palermo Convention defines money laundering at article 6 "*The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action*"; the European Directive on combating money laundering through criminal law identifies, at article 3, three possible conducts that can integrate a money laundering offence *"(a) the conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action; (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity; (c) the acquisition, possession or use of property, knowing at the time of receipt, that such property was derived from criminal activity*"; see also the definition by B. Villányi, *Money laundering: History, regulations, and techniques*, in *Oxford Research Encyclopedia of Criminology and Criminal Justice*, 2021, 1, "*Money laundering is the conversion of criminal incomes into assets that cannot be traced back to the underlying crime",* in a similar sense P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, Springer, 2018, 94.

A first distinguishing feature of money laundering is its connection with the purpose pursued by the agent. When it comes to this crime, the conduct is usually solely defined in general terms. Rather, what matters is the intention and the effect of the conduct: the obfuscation of the illicit origin of the goods being laundered.[7] Money laundering is, therefore, an event-based rather than an activity-based crime. This is mainly due to its multifaced nature. The pathways of laundering are multiple and continuously changing, providing a stable, detailed definition would risk forcing the legislator to continuously play catch with the criminals. Furthermore, the damaging core of the offence is in the event not the actions. Money laundering is usually carried out through perfectly legal activities – as wire transfers, real estate investments, art trading, etc. The societal harm is not caused by the activities but by their effect: the integration of illicit capitals into the licit market. This characteristic of money laundering also poses a fundamental challenge to its detection. Taken singularly money laundering conducts are perfectly legal and mostly indistinguishable from normal commercial transactions. It is only when seen holistically and teleologically that their criminal nature emerges.[8]

A second element characteristic of money laundering is its necessary connection with a previous crime. The structure of money laundering requires the presence of a predicate offence which has generated an economic proceed. The connection between the two crimes needs only to be objective – as the laundering activity has to concern the proceeds of a predicate offence – and not subjective – meaning the individual/s committing the predicate offence do/es not have to be the same laundering the proceeds.[9] Furthermore, the money laundering offence does not have to be

[7] A. Gullo, *Autoriciclaggio e reati tributari,* in *Diritto Penale Contemporaneo,* 2018, 10, "*il riciclaggio, e ancor di più l'autoriciclaggio, si fondano sul pilastro dell'ostacolo all'identificazione della provenienza delittuosa*".

[8] V. Manes*, Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale,* in *Rivista Trimestrale di Diritto Penale dell'economia,* 2004, 2.

[9] The punishability of self-laundering – meaning money laundering activity pursued by the same individual/s who committed the predicate offence – has long constituted a debated issue. In some jurisdiction such punishability was seen as a duplication of the punishment as the perpetrator was simultaneously punished for the predicate offence and for using the proceeds of such offence. In this sense, the Palermo convention allowed at article 6, para. 2, lett. e), "*if required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence*", see in this sense P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 109. The European Directive of 2018 has, however, taken a different stance by clarifying – at art. 3, para. 5 – that "*Member States shall take the necessary measures to ensure that the conduct referred to in points (a) and (b) of paragraph 1 is punishable as a criminal offence when committed by persons who committed, or were involved in, the criminal activity from which the property was derived*". Due to this initial reluctance, certain Member States distinguish money laundering and self-laundering, an example being Italy which provides for a money laundering offence –art. 648 *bis* c.p. – and a self-laundering one – art. 648 *ter* 1 c.p. – the latter under stricter limits and with a milder punishment, see C. Piergallini, *Autoriciclaggio, concorso di persone e responsabilità dell'ente*, in *Criminalia*, 2015.

necessarily perpetrated in the same jurisdiction as the predicate offence. The only requirement being that the predicate offence is a crime in both jurisdictions.[10]

With specific regards to the predicate offence there are two fundamental questions that are key to money laundering policing. First, what type of crimes can constitute a predicate offence.[11] Second, what is the connection that needs to exist between the predicate offence and the money laundering one. At the European level, the Directive on Combating Money Laundering through Criminal Law[12] has responded to both questions establishing a minimum common standard within the Union.

Regarding the first question, the Directive, at article 2, provides for two alternative criteria: a quantitative one, a predicate offence is any offence that is punished with a "*deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal systems, any offence punishable by deprivation of liberty or a detention order for a minimum of more than six months*"; a qualitative one consisting in a list of crimes that are always predicate offences irrespective of their punishment.

Regarding the second question, the Directive clarifies that the connection between predicate offence and money laundering is a weak one. This means there is no need for the predicate offence to be fully ascertained or even for its perpetrators to be identified. As stated by article 3, paragraph 3, letter b), of the Directive *"a conviction for the offences referred to in paragraphs 1 and 2 is possible where it is established that the property was derived from a criminal activity, without it being necessary to establish all the factual elements or all circumstances relating to that criminal activity, including the identity of the perpetrator".*

Finally, regarding object and *mens rea*. The object of money laundering can be any property. Meaning that any proceeds of a crime with economic significance – a car, fine art, a bond, etc. – can be laundered.[13] Concerning the *mens rea*, money laundering is a crime of intent. Particularly, the intent has to encompass not only the laundering activities but also the illicit origin of the proceeds

[10] As clarified by the Directive at art. 3, para. 3, lett. c., and the Palermo Convention at art. 6, para. 2, lett. c.

[11] P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 109-110.

[12] Directive of the European Union, no. 1673, 23rd October 2018.

[13] The Directive defines property at art. 2, para. 2, as "*assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets*".

being laundered. This second element is of specific importance as the activities conducted to launder are usually legitimate. It is, hence, the knowledge of the provenance of the objects of such activities where the discrimen between licit and illicit is traced.

## 1.1 The criminology of money laundering. Layering, placement, and integration

In the previous section we have described the normative definition of money laundering, the present section will delve into its criminological conformation.

As most criminal activity, money laundering can be pursued at different levels of complexity, from a mere series of wire transfers to multinational schemes of great intricacy.[14] Irrespective of the level of sophistication used, laundering is traditionally reconstructed by the literature[15] in three fundamental steps: placement, layering, and integration.[16] Through these three steps the provenance of a property is transformed from illicit to licit. To understand these three steps, we have to keep in mind the purpose of money laundering.

The final goal of money laundering is twofold. On the one hand, grant the perpetrator of the predicate offence the possibility to freely use such property in the licit market so to enjoy the fruits of its crimes. On the other hand, avoiding the criminal is connected with the predicate offence, thus, covering the financial trail of the crime itself. [17]

[14] B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 3.

[15] O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* Georgetown University Press, 2022, 12; J. Cassara, *Money laundering and illicit financial flows,* cit., 28; N. Gilmour, *Understanding the practices behind money laundering–A rational choice interpretation,* cit., 2; V. Manes*, Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale,* cit., 3.

[16] These steps are explicitly mentioned by the US FinCEN, in FinCEN, *History of Anti-Money Laundering Laws*, FinCEN Website, https://www.fincen.gov/history-anti-money-laundering-laws as well as by the UNODC, se United Nations Office on Drugs and Crime, *Money Laundering,* https://www.unodc.org/unodc/en/money-laundering/overview.html; B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 4.

[17] O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* Georgetown University Press, 2022, 13.

Let's then analyse the three phases of money laundering.

The first phase is placement. Placement consists in the introduction of the illicitly sourced property in the licit market. In order to commence the laundering activities, the criminal has to first reintroduce the property into the licit market. This first phase is the most delicate as the link between the predicate offence and the property is still strong.[18] The launderer has to use a series of stratagems to avoid the placement of the property raises suspicions and triggers an investigation. For instance, the perpetrator may smuggle cash in jurisdictions where anti-money laundering controls are scarce or divide the proceeds in smaller sums which are then deposited in multiple accounts (so-called smurfing).[19] Furthermore, the perpetrator usually tries to distance this activity from its identity. To this end, launderers may use dummy corporations, money mules, etc. to shield the identity of the real beneficiary.

The second phase is layering. Through layering the launderer aims at introducing as many layers as possible between the property and the predicate crime. The final aim is to introduce so many layers that retracing the origin of the good is impossible or, at least, exceedingly complex. During this phase, the property is moved across different accounts, jurisdictions and/or transformed (in bitcoin, a foreign currency, fine art, or real estate). Also during this phase, criminals employ tactics to distance the property from the real owner to disguise their ownership and give the perception the money is moving across different accounts and/or legal/natural persons.

The third phase is integration. Integration completes the laundering cycle as the property is introduced in the licit market and can be freely used by the perpetrator. This phase may consist, for example, in the sale of a property the launderer has acquired as part of the layering phase. At this point, if money laundering has been done correctly, it should be nearly impossible to hint the illicit source of the funds. At this stage, it may, hence, be already too late to identify criminal activity and apprehend the criminal.

While this triphasic description of money laundering is a simplification of the laundering process it is still useful to understand money laundering. Many times, the phases are intertwined or may be skipped completely. However, the triphasic distinction is useful to comprehend the fundamental

[18] J. Cassara, *Money laundering and illicit financial flows,* cit., 29.

[19] B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 4.

elements of the laundering cycle: the property has to be introduced in the licit market while disguising its source with the final purpose of integrating it and using it.

## 2. A brief history of the anti-money laundering regulation

Notwithstanding its key importance for modern policing, money laundering is a relatively recent policy field. The idea that financial data can be used to identify and prosecute criminals, especially in large, organized crime cases, is not new.[20] However, it is only recently that a comprehensive, internationally agreed, strategy for curbing the use of the financial market by criminals was devised.[21] Furthermore, the modern anti-money laundering regulation has, for the first time, envisioned a system to use financial data pre-emptively and not solely reactively (i.e., in the investigation phase) through the cooperation of the intermediaries that manage such data.

The push for such a strategy originated in the United States within the framework of the war on drugs.[22] Money laundering was, therefore, initially conceived as an instrument specifically designed to hinder the ability of narco-bosses worldwide to reinvest the proceeds deriving from the drug trade. As time passed the scope of money laundering widened and the legislation morphed into a multipurpose instrument to curb illicit finance.[23] This enlargement process has followed two main avenues: first, a wider list of predicate offences going beyond drug-related crimes; second, the inclusion of an increasing number of intermediaries among the covered entities.

Let's then retrace the fundamental steps of this legislative path.

[20] Famously Al Capone, the Chicago Mobster was finally convicted on tax evasion counts, see New York Times, *Al Capone guilty of tax evasion,* 17th October 1931, https://archive.nytimes.com/learning.blogs.nytimes.com/2011/10/17/oct-17-1931-al-capone-guilty-of-tax-evasion/, W. Muller, *Anti-money laundering–a short history*, in W. Muller – C. H. K¨alin – J. G. Goldsworth (eds.) *Anti-Money laundering: International law and practice*, Wiley, 2007, 3.

[21] A. dell'Osso, *Riciclaggio di proventi illeciti e sistema penale*, Giappichelli, 2017, 5.

[22] B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 9; A. dell'Osso, *Riciclaggio di proventi illeciti e sistema penale,* cit., 7.

[23] A. Gullo, *Autoriciclaggio e reati tributari,* cit., 2-3.

The beginning of the money laundering legislative saga is traditionally seen as the Bank Secrecy Act (BSA) enforced in the United States in 1970.[24] The Act introduced recordkeeping and reporting obligations for US banks and financial institutions. The infrastructure was further strengthened through the introduction in 1986 of the Money Laundering Control Act[25] and in 1990 of the Financial Crime Enforcement Agency (FinCEN). The creation of the FinCEN, a central agency with the mandate of receiving and analysing suspicious activity reports as well as coordinating anti-money laundering efforts, is of particular relevance. Eminently, the idea of a central, independent agency solely devoted to anti-money laundering has remained key in anti-money laundering regulation and has penetrated worldwide with the progressive establishment of National Financial Intelligence Units (FIU).

Starting from the 1980s, the focus on financial integrity increasingly crossed the United States' borders and became central in global supervision efforts. This culminated in a call for action by the Group of Seven in July 1989 at the Paris Summit.[26] There, within the context of curbing drug trafficking, the call for action determined to:

> *"Convene a financial action task force from Summit participants and other countries interested in these problems. Its mandate is to assess the results of cooperation already undertaken in order to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive efforts in this field, including the adaptation of the legal and regulatory systems so as to enhance multilateral judicial assistance. The first meeting of this task force will be called by France and its report will be completed by April 1990".*[27]

[24] FINCEN, *History of Anti-Money Laundering Laws*, https://www.fincen.gov/history-anti-money-laundering-laws; P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 4; 43.

[25] P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 50 as well as M. Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control,* in C. King – C. Walker – J. Gurulé (Eds.), *The Palgrave handbook of criminal and terrorism financing law*, Palgrave Macmillan, 2018, 34.
identify this act as the first real anti-money laundering legislation as the BSA was mainly focused on tax evasion.

[26] P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 3.

[27] G7/8 Summits, Economic Declaration, Paris, 16th July 1989, http://www.g8.utoronto.ca/summit/1989paris/communique/index.html

This declaration laid the ground for the establishment of the Financial Action Task Force (FATF) which would become the key international policymaker in the field.[28] Just one year later, in 1990, the FATF published a report containing forty recommendations to address money laundering.[29] FATF's establishment and issuance of the Forty Recommendations solidified the role of financial institutions in anti-money laundering systems. Particularly, recommendation four emphasized the compatibility of financial institution secrecy laws with FATF's guidelines, similarly, recommendation five compelled financial intermediaries to perform customer due diligence controls and barred anonymous accounts. To reinforce the implementation of the recommendations, the FATF established a list of non-cooperative jurisdictions – so-called blacklist – where noncomplying states would be recorded.[30]

At the same time, the United Nations (UN) started working on the criminalization of money laundering. The foundation for criminalizing money laundering across jurisdictions can be traced back to the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, of 1988.[31] The scope was extended beyond drug trafficking through the United Nations Convention against Transnational Organized Crime[32] (the Palermo Convention). The Palermo Convention extended, at article 6, predicate offences to a list of serious crimes and reiterated, at article 7, the relevance of financial institutions in the prevention of money laundering. The latter article urged states to establish comprehensive domestic regulations for banks, non-bank financial institutions, and susceptible bodies to deter and detect money laundering, emphasizing customer identification, record-keeping, and reporting of suspicious transactions. The Convention marked a turning point as states recognized the necessity to limit bank secrecy in criminal cases in order to ensure the integrity of the banking systems. International agreements like the UN Convention

[28] M. Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control,* cit., 36; A. dell'Osso, *Riciclaggio di proventi illeciti e sistema penale,* cit., 13 – 14.

[29] Financial Action Task Force, *The forty recommendation of the financial action task force on money laundering,* Paris, 1990; for an analysis of the content of such recommendations and their structure see chapter 3, section 1.

[30] W. Muller, *Anti-money laundering–a short history,* cit., 6; B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 10; M. Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control,* cit., 36.

[31] United Nations, *UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, Vienna, 1988; on the origins of this Convention see P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 53; V. Manes*, Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale,* cit., 7.

[32] United Nations, *United Nations Convention against Transnational Organized Crime and the Protocols Thereto,* 15 November 2000; M. Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control,* cit., 35.

Against Corruption (UNCAC),[33] the Strasbourg Convention,[34] and the OECD Convention on Combating Bribery[35] further paved the way for agreements and mechanisms safeguarding financial integrity and supervision.

The international strengthening of the anti-money laundering framework has steadily continued since then. The FATF now counts thirty-nine members and two-hundred-fifteen countries have adhered to its recommendations.[36] Furthermore, a series of regional FATF-style bodies have flourished across the world.[37] At the same time, the scope of the FATF's mandate has been extended to terrorism financing, following the 2001 terrorist attacks. The extension has been followed by the draft of eight special recommendations devoted to terrorism financing.[38] The FATF has continuously revised its recommendations with the last general update being conducted in 2012, when the latest version of the Forty Recommendations was published.[39]

At the European level, the Union has played a key role in the adaptation process to the anti-money laundering standards. Starting from 1991, the Union has passed five anti-money laundering Directives – the last one approved in 2018.[40] The aim is to strengthen the integrity of the Union's financial system while ensuring a level playing field across the common market. As we will further detail in chapter three, part one, section three-three, the Union's anti-money laundering framework is currently undergoing a fundamental upheaval. Following a series of scandals, the Commission has laid out a plan to further centralize the regulation and supervision of the anti-money laundering regulation. The plan consists in the substitution of the current Directives with a Regulation and the creation of a European Anti-money Laundering Authority (AMLA).[41]

[33] United Nations, *United Nations Convention against Corruption,* 31st October 2003.

[34] Council of Europe, *Criminal Law Convention on Corruption*, 27th January 1999.

[35] OECD, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*, 17th December 1997.

[36] For a complete list see https://www.fatf-gafi.org/en/countries.html

[37] See, for instance, for Latin America the GAFILAT (https://www.gafilat.org/index.php/es/) or for West Africa the GIABA (https://www.giaba.org/); P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 57.

[38] Financial Action Task Force, *FATF IX Special Recommendations*, Paris, 2001.

[39] Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit.

[40] M. Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control,* cit., 35.

[41] For a further analysis of this plan and of the connected Package see Chapter 2, Part 2, Section 3.3.1.

## 3. Structure

Now that we have laid out the groundwork, let's delve into the structure of the present research. The thesis is divided into five chapters, followed by concluding remarks.

Chapter one outlines the historical and ideological background of blockchain and crypto-assets. It delves into the history of the movement that first conceived crypto-assets and their ideological motivations. It also examines how crypto-assets and blockchain have evolved since their inception in 2008. The aim is two-fold. First, underline how crypto-assets are not merely a technological innovation. Rather, they are technological means to a political end which strikes at the heart of the financial monitoring infrastructure. Second, analyse how the market has hinged on such ideological premises and influenced blockchain's growth. Blockchain and crypto-assets are not a monolith, but rather a multifaced market where competing views and technologies coexist. Understanding such nuances is key for the policymaker as each implementation poses partially different risks and opportunities.

Chapter two details the technological functioning of blockchain. The aim is to provide a technological, layman background to the reader. The underlying idea is that to regulate a certain technology it is first necessary to clearly understand its functioning. The aim of the chapter is not to turn legal scholars into computer scientists. Rather, to detail the logic behind blockchain technology and its fundamental components so to provide policymakers with the tools needed to act on such logic and adapt their strategies.

Chapter three critically analyses the definition of crypto-assets and crypto-asset service providers as stipulated by the anti-money laundering regulation. Given our scope, we will focus on two legislative sources: the Financial Action Task Force – as the body providing the overarching money laundering framework - and the European Union – as the key source of our analysis. The chapter is composed of an introduction and three parts. The introduction builds on chapters 1 and 2 highlighting how blockchain's transaction model intersects with the anti-money laundering infrastructure. It examines the pain points generated by blockchain as well as the emerging opportunities. Part 1 focuses on the definition of crypto-assets to critically examine the policy choices made so far. We conclude with a proposal for a different definition of crypto-assets customized to anti-money laundering. Part 2 focuses on crypto-asset service providers. It analyses which service providers operating in the crypto-market have been chosen by the regulator as covered entities, also taking a historical perspective. It concludes with a critical assessment of such choices and a proposal for a different approach to intermediaries' regulation. Part 3 summarizes the findings of the chapter and proposes possible avenues for further development.

Chapter four delves into the content of the anti-money laundering duties. After a brief introduction of the overarching duties, it focuses on how these have been customized to crypto-assets. To this end, it considers both primary and secondary sources with a special focus on the European Banking Authority (EBA). It underlines the complexities connected with the extension of a policy framework thought for a centralized, intermediated market to an, at least partially, decentralized and disintermediated one.

Chapter five focuses on one category that has generated an acute debate in the policy arena: Decentralized Autonomous Organizations (DAOs). The governance model of these organizations presents a distinct challenge to policy makers due to their headless, code-based functioning. Furthermore, DAOs epitomize the fundamental hurdles posed by blockchain to regulators: the absence of a centralized point of pressure and the creation of horizontal headless networks of cooperating parties. The chapter examines how the policymaker has responded so far, as well as the policy proposals that have been advanced. It concludes with a series of proposals to reimagine the policy approach and customize it to such organizations.

The text is closed with a series of concluding remarks. As the policy proposals are already advanced at the end of each chapter, the conclusion summarizes our findings and concisely presents the results of the research.

## 4. Methodology

As detailed above, the present text will investigate one primary research question: how has the European anti-money laundering legislature responded to the advent of crypto-assets? This overall descriptive interrogative is complemented by the following critical sub-question: is the European approach to crypto-assets' regulation a mere reiteration of the previous anti-money laundering strategy or does it follow new avenues? This question required in turn the analysis of one further interrogative: how can the intermediary-centred strategy for anti-money laundering be adapted to a decentralized, disintermediated architecture so to guarantee the effectiveness of controls while ensuring legal certainty?

This primary research question is complemented by a second one with a larger scope: how has the legislature responded to an architectural modification in the structure of financial transactions – i.e., their disintermediation – which undermines its former policy strategy? Which is in turn complemented by the following sub-questions: has the response to the analysed architectural modification been conservative[42] or innovative[43]? Is the chosen approach enough to confront the risks to the effectiveness of controls posed by a paradigm-shifting technology?

To answer these interrogatives, the research has developed in subsequent steps.

First, an analysis of the historical and philosophical movement underlying blockchain's development and Bitcoin's launch in 2009. Rather than an isolated event, blockchain's introduction is better understood as a historical process stretching across over fifty years. The community working on blockchain had clear political and social purposes that strike at the heart of the financial monitoring infrastructure. To fully understand the legal conundrum generated by crypto-assets it is significant to appreciate such aims as they have influenced the conformation of the resulting technology. Eminently, as underlined by the historical analysis, the development of crypto-assets is intimately connected with a quest for financial privacy and autonomy from centralized trust-brokers – i.e., States, Central Banks, and Financial Institutions. In this sense, the political objectives that shaped the design of crypto-assets are directly related to the policy strategy underlying the financial monitoring infrastructure. Truly, one of the fundamental objectives of the community developing crypto-assets was to allow individuals to avoid such an infrastructure. It is, hence, crucial to understand how developers tried to achieve this goal to comprehend the risks crypto-assets pose to financial monitoring. Furthermore, the evolution of the crypto-market post-2009 details the hurdles connected with the new decentralized and disintermediated governance

[42] With conservative it is meant a policy approach that reiterates the pre-existing strategy to market regulation – in the case of money laundering, mainly the regulation of intermediaries.

[43] With innovative it is meant a policy approach that introduces a complementary or radically different strategy to market regulation.

infrastructure envisioned by blockchain's developers which hinders anti-money laundering efforts. This evolution, and the connected "tales of decentralization" analysed in chapter one, underline the concrete weaknesses of such a model. Such weaknesses constitute potential points of entry for the policy maker as well as emerging risks the latter has to address and mitigate.

This part was mainly carried out through desk research. The desk research has gone beyond pure legal texts. Historical books, manifestos of the members of the early blockchain community, public statements, and newspaper articles have been analysed. The aim was to achieve a complete understanding of the movement, which, given its fluid and bottom-up nature, could only be acquired through a variety of sources. Furthermore, in the early stages of the research, a series of informal interviews with members of the community – developers and forensics experts - have been carried out. These interviews were conducted informally, solely in order to get a better understanding of the technological issues relevant to the topic.

Second, an analysis of the technology underlying crypto-assets. To regulate a technology the first step is truly comprehending its functioning. In this sense, the functioning of blockchain has been analysed both holistically and in its components - consensus protocols, asymmetric cryptography, etc. Furthermore, the whole spectrum of blockchain infrastructures has been examined. Eminently, blockchain, rather than a monolith, is better understood as a spectrum of solutions spanning from fully decentralized to centralized networks. In this sense, such different infrastructures have been examined with a focus on the impact of each implementation on the governance structure. Following the examination of the infrastructure, the analysis has moved to the analysis of the superstructure – meaning the technological solutions that exploit blockchain networks to build organizations and software. This has entailed the study of blockchain-based implementations such as smart contracts, decentralised autonomous organizations, and non-fungible tokens.

This part has been carried out through desk research. The desk research has mainly entailed the analysis of computer science papers, not only blockchain-specific but also from neighbouring fields, such as cryptography. Furthermore, the researcher has followed specialized courses and used blockchain and connected tools – blockchain analytics software, hashing algorithms, etc. – to gain a first-hand understanding of the technological infrastructure.

Third, problem statement. After having acquired a complete understanding of the technology and its historical background, the research has delved into its connection with financial flow monitoring and anti-money laundering regulation. The aim was to identify the unique risks posed to the pre-existing anti-money laundering policy strategy so as to formulate accurate policy-specific research questions. In this sense, the implications of financial flows disintermediation and governance decentralization have been analysed considering the present anti-money laundering strategy. To garner a better understanding of the problem, real-world cases of crypto-related criminality have been examined. These cases have been used as a testing ground for the risks identified. Eminently, by understanding how criminals concretely exploited crypto-assets to circumvent existing controls, it was possible to test the accuracy of the identified abstract risks. These cases have been used in the analysis to provide the reader with a concrete depiction of the risks identified so to facilitate understanding – i.e., Silk Road, Liberty Reserve, the DAO hack, and ransomware attacks.

This part has been carried out through desk research. The research has prevalently focused on legal academic texts and reports of national and internal organizations (International Monetary Fund, Europol, OECD, etc.). However, the literature review has been complemented with the analysis of crypto-related criminal cases through the examination of National judgments, Financial Action Task Forces' case reports, and publicly available interviews of individuals involved in such cases.

Fourth, policy analysis. The policy analysis has focused on two fundamental sources: the Financial Action Task Force (FATF) and the European Union. Given the territorial scope of the research, the choice has been to solely focus on European sources. The Financial Action Task Force has been included due to its fundamental, overarching role in anti-money laundering regulation. Eminently, as demonstrated throughout the thesis, the European regulation is intimately connected with FATF's Guidances and can only be understood in connection with them. From a European perspective, the two main sources analysed are primary European Union legislations (Directives and Regulations) and the Guidelines issued by the sectorial supervisor, the European Banking Authority (EBA). National legislations have remained out of the scope of the present analysis. This certainly can be seen as a limitation of the present work. However, the European case is one of great relevance. Firstly, the Union has been a pioneer in the regulation of crypto-assets. Particularly, the introduction of the Market in Crypto-assets Regulation (MiCaR) constitutes one of the first attempts worldwide to provide for a comprehensive regulation of the market.

Secondly, the European Union has placed itself, during the last decades, as a global leader in policy making. The impact of the so-called "Brussels effect" is widely recognized by the literature.[44] This makes an analysis of the European legislation crucial not only to understand a regional trend but also at hinting the global direction of the policy strategy. Thirdly, while anti-money laundering regulation has, up until now, been partially a national competence – through the issuance of the Anti-money Laundering Directives – this is about to change. The new Anti-money Laundering Package centralizes the competence of the European Union by establishing a centralized supervisor (the Anti-money Laundering Authority) and partially substituting the Directive with a Regulation. Particularly, the policies concerning crypto-assets are exclusively spelled out by the (directly applicable) Regulation of the upcoming Package. The same goes with the MiCaR which, again, is a directly applicable regulation. This makes a solely European analysis still highly valuable. Finally, by focusing on the European perspective the thesis has a clear policy objective: to provide insights to the European legislator on the efficacy of its policy strategy and advise on possible avenues for amelioration. The present moment is a topical one for the drafting of a European strategy to crypto-assets: the MiCaR has just been approved, as well as the Travel Rule regulation,[45] and the Anti-money Laundering Package is in the making. Academia can act to better inform the legislator on the effectiveness of its choices so to influence the policymaking process and, ultimately, the overall strategy of crypto-assets policing.

An overarching element that has enriched the scope and depth of the research is the three-month research stay of the researcher at the International Monetary Fund (IMF). There the researcher has supported the Financial Integrity Group (the unit of the IMF involved in the development of anti-money laundering related policies) in their work on crypto-assets regulation and specifically Central Bank Digital Currencies. While the information acquired during the stay was for internal use only – hence, not employed for the thesis – the experience has provided the researcher with a unique perspective on the functioning and policy approach of this sectorial policy-making body. Specifically, it has informed the researcher on the challenges such bodies face when providing solutions to the emerging problem of crypto-assets.

[44] See, A. Bradford, *The brussels effect* in *Nw. UL Rev.,* 107, 2012, 1

[45] For more on the travel rule regulation see chapter 4, section 5.

# Chapter One

## From Bitcoin to e-Renminbi

### A brief history of blockchain

## 1. Introduction

Risen from the ashes of the deepest confidence crisis in the financial infrastructure of the last decades, blockchain aims to redesign the way trust is managed and administered in digital, complex economies. Through code-enabled trust, blockchain promises to facilitate secure peer-to-peer interactions making traditional trust-brokers – like banks, notaries, land registries, etc. - obsolete.[1] This shift in the architecture of trust brokerage has profound implications for a wide range of policy fields that take as a postulate precisely such pre-existing architecture.

However, before delving into the intricacies of this technology and its policy repercussions, it is appropriate to briefly draw a timeline of blockchain's development. Namely, if, on one hand, blockchain sinks its roots in times when Lehman Brothers was still a thriving investment bank, on the other hand, fifteen years after Nakamoto's seminal paper, blockchain is far more than just a technology supporting a virtual currency. It is, therefore, appropriate to retrace the origins and development of this technology to fully understand its ideological roots and to catch a glimpse of its future impact.

[1] P. De Filippi – B. Loveluck, *The invisible politics of bitcoin: governance crisis of a decentralized infrastructure*, in *Internet policy review,* 5.4, 2016, 2; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, Banque de France Fintech-Innovation Hub, Paris, 2023, 2.

A *caveat* before we start. The aim of this first brief account is not to go through all the ups and downs blockchain has experienced during the last decade. Given the scope of the present text, the purpose is to identify those elements that are topical to financial integrity and that can help in better understanding the policy actions in the field.

To this end, the present chapter is structured as follows. The first section will analyse the origins of the crypto-assets movement. We will go back in time to understand what problems developers aimed to solve through crypto-assets, and what triggered their launch in 2009. The second section will analyse how crypto-assets have evolved since their creation. It will particularly focus on how the initial full decentralization proposed by blockchain has stood the test of time. We will delve into two "tales of decentralization" to examine the concrete evolution of this concept throughout time. Particularly, the evolution of mining and the DAO case provide insights into the practical hurdles connected with headless, code-based networks and/or organizations. The last section will delve into the future developments of blockchain. It underlines how the fully decentralised model proposed by its initial creators is being modelled by the market. New implementations are being proposed that mix centralization with decentralization. These implementations partially rethink the fundamental tenets underlying blockchain and propose a "gentrified" version of it. The chapter ends with concise closing remarks.

## 2. The origins story. Cypherpunks, cryptography, and Lehman

Let's then start with the origin story.

The roots of the blockchain phenomenon can be traced back to the cypherpunk movement and, specifically, to their quest for enhanced, distributed, and accessible privacy. [2] Cypherpunks are a

[2] As stated by E. Hughes, *a cypherpunks manifesto*, 1993, "*Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one does not want the whole world to know, but a secret matter is something one does not want anybody to know. Privacy is the power to selectively reveal oneself to the world*".

loosely connected and defined movement[3] that formed in the early nineties in the San Francisco area around the figures of Timothy May, Eric Hughes, and John Gilmore. [4]

May, considered the founding father of crypto anarchism, had already laid out his ideological stance in the crypto anarchist manifesto, published in 1988. [5] There he had emphatically announced that "*a specter is haunting the modern world, the specter of crypto anarchy*". Through this manifesto, he predicted that the nascent computer technology would provide individuals with a multipurpose tool for anonymity destined to reshape social and political interactions. [6] Interestingly, already in this very early text, the core trade-offs that, two decades later, would underlie the cryptocurrencies' policy debate were clearly spelled out by May:

> "*The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion.* [7] *Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy*".[8]

[3] The term cypherpunk and the reference to this group is used in this text for reasons of clarity and to avoid unnecessary complexity. It is, however, crucial to underline that under this umbrella coexisted many different souls and perspectives - as underlined e.g., by P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, Routledge, 2022 - and that not all the early proponents of digital currencies were necessarily part of the cypherpunk movement. Eminently, as this movement was fundamentally built around a mailing list and a philosophy of strong decentralization, it is clear that no official or unitary ideology existed. However, as highlighted by C. Jarvis, *cypherpunk ideology: objectives, profiles, and influences (1992-1998),* in *Internet Histories,* 2021, p. 7 – their general objectives were: 1) Unregulated citizen encryption access; 2) Anonymous communications; 3) Freedom to conduct anonymous economic transactions (crypto currencies); 4) Development of leaking platforms to constrain government power.

[4] See among many, C. Jarvis, *cypherpunk ideology,* cit.; P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit.

[5] T. May, *The cryptoanarchist manifesto,* 1988

[6] C. Jarvis, *cypherpunk ideology,* cit., 5.

[7] This reference, in particular, well fits the flourishing dark market economy that has found in cryptocurrencies its means of exchange and funding, see R. Hardy - J. Norgaard, *Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web* in *Journal of Institutional Economics,* 12, 3, 2016, 515, 517; Chainalysis, *The 2022 Cryptocrime Report*, February 2022, 99; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, April 2023, 23. For an example of the use of bitcoin in such dark market transactions see the one analysed by E.W. Kruisbergen - E.R. Leukfeldt - E.R. Kleemans - R.A. Roks, *Money talks money laundering choices of organized crime offenders in a digital age* in *Journal of Crime and Justice,* 5, 2019, 574 – 575.

[8] T. May, *The cryptoanarchist manifesto,* cit.

Building upon this vision of individual anonymity as the digital one-stop-shop for freedom, cypherpunks perceived unregulated and decentralised cryptography as the main tool to achieve such anonymity.[9] Notwithstanding May's earlier predictions regarding the inherently liberating potential of digital technologies, cypherpunks realized that digital technologies were a double-edged sword for privacy. They understood that, without proper precautions, the progressive digitalization of interpersonal interactions allowed governments and corporations to access an unprecedented amount of data to profile and influence individuals.[10] To reinstate an appropriate limit to State control and avoid the establishment of an all-encompassing surveillance State, cypherpunks believed in grassroots organizations based on open-source and choral development of cryptography. Namely, they held that the economic and political incentives of control would have prevented governments and corporations from dispensing free privacy. In the absence of top-down solutions, it was, therefore, up to the citizens to organize and defend themselves from the increasing public and private intrusiveness by using cryptographic means.

As stated in the cypherpunk manifesto,[11] drafted by another of the founders of the cypherpunks, Eric Hughes, in 1993:

> "*We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free (…) We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place*".

[9] C. Jarvis, *cypherpunk ideology,* cit., 7; P. De Filippi – B. Loveluck, *The invisible politics of bitcoin,* cit., 4, "*cypherpunks, who saw strong cryptography as a means of achieving greater privacy and security of interpersonal communications, especially in the face of perceived excesses and abuses on the part of governmental authorities*"

[10] P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 2; as stated by D. Chaum, *Achieving electronic privacy*, in *Scientific American*, 267.2, 1992, 96 "*Every time you make a telephone call, purchase goods using a credit card, subscribe to a magazine or pay your taxes, that information goes into a data base somewhere. Furthermore, all these records can be linked so that they constitute in effect a single dossier on your life, not only your medical and financial history but also what you buy, where you travel and whom you communicate with. It is almost impossible to learn the full extent of the files that various organizations keep on you, much less to assure their accuracy or to control who may gain access to them*".

[11] E. Hughes, *a cypherpunks manifesto,* cit.

In this quest for privacy through cryptography, cypherpunks were famously a vocal piece in the successful opposition to Clinton's government bid to regulate cryptography by mandating the use of a "law-enforcement friendly" encryption language.[12]

Of key importance for our ends is the work of cypherpunks in the field of digital currencies. Namely, the impact in terms of privacy of the shift from cash to digital transactions was a central topic of debate in these circles.[13] Cash, by-design, allows to perform transactions without requiring any counterparties' identification;[14] on the contrary, digital transactions require, by-design, the sender and the receiver to be identified. This shift means that, as clearly spelled out by David Chaum:[15]

> "*the foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions*". [16]

Furthermore, such architecture of digital transactions constitutes the weak link in the cryptography-enabled privacy infrastructure envisioned by cypherpunks: in their view, cryptography would empower individuals to communicate and trade globally and anonymously. However, the non-anonymous nature of financial transactions meant that any digital exchange of value performed by two - otherwise anonymous - users would break the privacy circle permitting

[12] For a brief overview of the root causes of this clash see S. Levy, *Battle of the Clipper Chip*, in *The New York Times*, 12 June 1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

[13] See also the E. Hughes*, a cypherpunks manifesto*, cit., "*When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself*"; for an in-depth account of the growth and development of such fears see F. Brunton, *Digital Cash. The unknown history of the anarchist, utopians, and technologists who created cryptocurrencies,* Princeton University Press, 2019, 51

[14] F. Tronnier - D. Harborth - P. Hamm, *Investigating privacy concerns and trust in the digital Euro in Germany*, in *Electronic Commerce Research and Applications,* 53, 2022, 1; P. Panetta, *Crypto-assets or virtual currencies as they were called before it was realized that they cannot perform the functions of money* in *SUERF Policy Notes*, 40, 2018, https://suerf.org/policynotes/3251/21st-century-cash-central-banking-technological-innovation-and-digital-currencies.

[15] David Chaum is considered the spiritual father of digital currencies, back in 1989 he had started a company, DigiCash with the purpose of providing an anonymous digital means of payment. However, the venture never took off and the company declared bankruptcy in 1998. For an overview of DigiCash journey refer to the interesting interview of Chaum in 1999 see https://firstmonday.org/ojs/index.php/fm/article/download/683/593/; se also F. Brunton, *Digital Cash,* cit., 54 - 55

[16] D. Chaum, *Security without identification: Transaction systems to make big brother obsolete*, in *Communications of the ACM,* 28.10, 1985, 1030.

identification. Only through a peer-to-peer currency based on cryptography, that could mimic the privacy architecture of cash in the digital realm, full-privacy could be achieved.[17]

To this end, numerous members of the cypherpunk circle – and beyond – worked on digital-money solutions.[18] None of them, however, really took hold, until Bitcoin. Behind such failures, there are both technological and socio-political reasons.[19] Namely, if Nakamoto's[20] solution, as we will explore in the following chapter, provides an answer to a series of dilemmas that had prevented decentralized currencies from thriving, the socio-political environment characterizing the second decade of the 21st century also played a crucial role.

Nakamoto chose a strategic moment to release its paper and launch Bitcoin. The 2008 financial crisis was a painful depiction of what can go wrong in an intermediated world. A systemic short-circuit of intermediaries caused by a failure of market and legislative incentives[21] - meant to guarantee their integrity and police risk appetite – sent shockwaves across the globe.[22]

To rub salt in the wound, the crucial role of intermediaries for economies paradoxically forced Governments to flush vast amounts of money to save the same institutions that had caused the crisis, while individuals were largely left stranded. Even though the exact figure is contentious,

[17] C. Jarvis, *cypherpunk ideology,* cit., 9.

[18] P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 68 and *ss;* F. Brunton, *Digital Cash. The unknown history of the anarchist, utopians, and technologists who created cryptocurrencies,* cit.

[19] As affirmed by P. De Filippi – B. Loveluck, *The invisible politics of bitcoin,* cit., 5, "*the creation of the Bitcoin network was in large part motivated in response to the social and cultural contingencies that emerged during the global financial crisis of 2008*".

[20] Satoshi Nakamoto is the phantomatic father of Bitcoin. They appeared in 2008 through the publication of the Bitcoin paper and remained active in the community, which they steered in its first phases, until 2012 when they disappeared. Their identity is still a mystery even though a number of hypotheses have been formulated during the years. For more information see P. Vigna, *Who Is Bitcoin Creator Satoshi Nakamoto? What We Know—and Don't Know,* in *Wall Street Journal,* 7 December 2021, https://www.wsj.com/articles/who-is-bitcoin-creator-satoshi-nakamoto-what-we-knowand-dont-know-11638020231.

[21] While the root causes of the financial crisis are still the object of a heated debate, it is widely recognized that one of the main causes has been the lack of legislative and market constraints to the risk taking behaviour of the financial sector, see G. de la Dehesa, *Twelve Market and Government Failures Leading to the 2008–09 Financial Crisis*, Group of Thirty, 2009; E. Coghlan – L. McCorkell – S. Hinkley, *What Really Caused the Great Recession?*, Berkley Institute for Research on Labor and Employment Policy Brief, 2018.

[22] As underlined by K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, Routledge Handbook of Financial Technology and Law, 2021, 6, the financial crisis of 2008 spurred the introduction and development of a wide array of peer-to-peer lending and transaction platforms besides blockchain.

MIT Sloan professor Deborah J. Lucas calculated that the total direct cost of crisis-related bailouts in the United States amounted to four hundred ninety-eight billion dollars.[23]

Nakamoto was not shy in underlining this paradox: famously, the genesis block of Bitcoin bears the following message "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*". This is a quote to the headline of an article published by the London Times detailing the mounting pressure on the British Chancellor Alistair Darling to flush additional resources into the banking system to avoid systemic failure.[24]

Within this social and political environment, Bitcoin branded itself as a way out of the intermediated system that had just shown its darkest side. Through a payment infrastructure "*based on cryptographic proof instead of trust*",[25] any two willing parties were empowered to transact directly with each other without the need to use a trusted third party – i.e., an intermediary.[26] In brief, Bitcoin promised to allow anyone to "be his own Bank"[27] in a moment when Banks seemed like unreliable business partners.[28]

Bitcoin, furthermore, largely achieved the cypherpunk vision of providing a pseudonymous, decentralized, and cryptographically secure means of payment. As detailed in the following chapter, Bitcoin, through the ingenious use of asymmetric cryptography, allows any two parties to transact securely without any need for personal identification, thus bypassing the traditional design of digital transactions. Additionally, Bitcoin is rooted in open-source code and decentralized governance, which makes any form of unilateral and centralized dictamen extremely difficult to

[23] D. Lucas, *Measuring the Cost of Bailouts*, in *Annual Review of Financial Economics*, 11, 2019, 85-108.
[24] F. Elliott – G. Duncan, *Chancellor Alistair Darling on brink of second bailout for banks*, in *The Times*, 3 January 2009, https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h; A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE,* 2018, 5.
[25] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* EBI Working Papers, 145, 2023, 4. As underlined by K. Werbach, *The Blockchain and the new architecture of trust*, The MIT Press, 2018, 17, Nakamoto's statement that blockchain eliminates the need for trust is fundamentally incorrect, rather, blockchain restructures the way trust is administered and managed in complex societies by substituting trust in the intermediary in trust in the system – or as some would say trust in the code.
[26] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009, https://bitcoin.org/bitcoin.pdf
[27] This sentence together with "in code we trust" has become the anthem of the Bitcoin movement underlining the ideological relevance of disintermediation, at least in the early adopters' community.
[28] For a different interpretation of the relation existing between Bitcoin and the financial crisis, see M. Hütten, *The soft spot of hard code: blockchain technology, network governance and pitfalls of technological utopianism*, in *Global Networks*, 19/3, 2019, 341.

enforce due to the absence of a central point of pressure.[29] This means that, with the introduction of Bitcoin, online users can exchange value online without breaking the anonymity circle. Bitcoin completed the journey towards (pseudo)anonymity through cryptography cypherpunks had embarked on two decades earlier.

The launch of Bitcoin closes, therefore, our origin story.

## 3. The development. On decentralization, or a tale of human nature

Of the years following the launch of Bitcoin much has been said. The present section will, however, focus on one fundamental thread of blockchain's early (and present) years: the increasing challenges and related failures suffered by its fully decentralized model of governance.

As detailed in the previous section, for blockchain's early developers, decentralization was not simply a design feature it was an ideological choice. Even more, the first implementation of blockchain, Bitcoin, was not merely conceived as a decentralized technology but as a conduit of decentralization. Indeed, through a decentralized, private, and cryptographically secure currency, cypherpunks envisioned a system for individuals to transact out of the purview of the – corporate and State – Leviathan.

Decentralization sits, thus, at the core of the original blockchain project and constitutes one of its preeminent ideological as well as technological features. However, when the utopia became reality – as Bitcoin and other blockchain implementations gained mainstream adoption – some cracks in the cypherpunk theoretical structure started to surface. If blockchain was envisioned as a system to substitute trust in third parties with trust in the code, the last decade has shown how third-party intervention may still be needed – at least when crises emerge.

The full decentralization of the archetypal blockchain certainly represents an interesting case study for self-regulation. It is, however, also a clear example of the limits of self-regulation and the

[29] Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* Rome, 2022, 8.

rationale of vertical organizations in modern human societies. Blockchain has shown that code can be a conduit of regulation, it has, however, also shown that it is not a magic wand that will simply make the need for law-making, and law-enforcement disappear.

Two main underlying causes can be identified for this governance failure.

On one hand, in a fully decentralized environment, the code tends to be static. Once engraved in the original infrastructure, code can only be modified through consensus,[30] and consensus is difficult to reach.[31] This means that decentralized organizations tend to be resistant to change and slow in adapting to external stimuli. It is ten years that the Bitcoin community discusses possible modifications to the mining protocol to reduce its energy footprint; however, due to contrasting interests and ideological debates, there is no solution in sight. This makes decentralized organizations a sitting duck to opportunistic behaviour. As will be shown by the example of mining provided in the following section,[32] if there is no centralized authority that can police market failures, individual interest will usually have the better hand over the common one. This way transforming the decentralized dream into a Hobbesian state of nature.

On the other hand, translating complex human interactions into clean, unambiguous code is a complex task.[33] As shown by the case of the DAO,[34] code is blind, and, at least for now, without human overview, it has no ability to discern good over evil. Furthermore, code is a human product and, consequently, suffers from most of those fallacies that it is purported to replace. To think, thus, that unsupervised code can autonomously manage human relations and solve the problem of opportunistic behaviour seems an oversimplification. When the code is cheated or fails, human intervention will still be needed. Namely, if *ex ante* many will agree to be solely regulated by code, *ex post,* the same people, once their savings have evaporated, will usually claim the good old redress.[35]

[30] C. Rueckert, *Cryptocurrencies and fundamental rights*, in *Journal of Cybersecurity*, 1, 2019, 8

[31] See as an example of such complexity the conflict on the block-size of Bitcoins detailed by P. de Filippi – B. Loveluck, *The invisible politics of Bitcoin*, cit.

[32] See Section 3.1.

[33] J. Grimmelmann, *All Smart Contracts are Ambiguous*, in *Journal of Law & Innovation*, 2019, 2, 1.

[34] See para 3.2.

[35] The acronym DAO stands for Decentralized Autonomous Organization. This is a bit of a confusing term as it is used to both describe a specific project – the one I currently refer to and that will be detailed in section 3.2 – and a category of smart contract-based organizations that are purported to act in a completely decentralized fashion. To add fuel to the fire the DAO project is also a Decentralized Autonomous Organization, hence the name. For more information regarding the DAO project please see section 3.2,

A clear example of such organizational failures is Bitcoin itself. Conceived by Nakamoto as a means of exchange alternative to fiat currencies, due to the absence of any regulator with the power to control the monetary supply, the Bitcoin experiences dizzying price fluctuation that has substantially made it unfit to be used as a means of exchange.[36]

To sum up, if the blockchain origin story was largely a tale of decentralization, its development is certainly a tale of conflict. A conflict between the world of forms and the world of substance and, ultimately, between two perspectives on the essence of human incentives.

To better understand the coordinates of this conflict, we will focus on two moments of blockchain's recent history which I believe are telling of these challenges and their underlying reasons. Also, we believe these two moments highlight the limits of full decentralization and remind us of the root causes and benefits of regulation.

### 3.1 The law of the jungle. The centralization of mining

The first of our tales is mining.

Mining is the system envisioned by Nakamoto to permit the creation and addition of new transactions to the blockchain. It constitutes, therefore, the dynamic dimension of Bitcoin's blockchain and is one of the key aspects of the Proof of Work (PoW) consensus protocol.[37] To create and add new blocks (bundles of transactions), miners are required to devote computational power to solve a mathematical puzzle. In exchange for their work, they receive a reward in Bitcoin – so-called blockreward - every time they solve the puzzle and add a new block.[38] The Bitcoin protocol is designed to keep the addition of new blocks stable at a rate of approximately one every

for more information on the concept of Decentralized Autonomous Organizations see https://ethereum.org/en/dao/.

[36] P. de Filippi – B. Loveluck, *The invisible politics of Bitcoin*, cit., 10, for an overview of Bitcoin's price fluctuations see https://www.coindesk.com/price/bitcoin/

[37] For a detailed analysis of mining and Proof of Work see chapter 3, para 4.

[38] G. Hileman – M. Rauchs, *Global cryptocurrency benchmarking study*, Cambridge Centre for Alternative Finance, 2017, 86.

ten minutes.[39] This means that, if the overall ability of miners to add new blocks increases, the algorithm automatically and proportionately augments the difficulty of the puzzle to keep the rate of newly created blocks stable.[40]

The structure of mining generates a classic prisoner dilemma: if no one increases its computational capacity then everyone spends less and earns more. However, if one of the miners increases its capacity then they will have a competitive advantage and, at least until everyone else catches up, will receive a significant extra profit. At the same time, if everyone upgrades its computational capacity, the software will automatically upgrade the difficulty, and everyone will earn the same while spending more.

The mechanism in question is the reason why, in the early Bitcoin era, it was possible to mine with a personal computer, whereas, currently, mining is carried out in so-called farms, comprised of hundreds of servers stored in warehouses, mining all day round. Eminently, as the price of Bitcoin soared, mining has become an increasingly remunerative endeavour. This has led to a mining "gold rush" which exponentially increased the overall computational power devoted to this activity and, therefore, the complexity of the connected puzzles.[41]

Such frenzy is not simply a normal by-product of blockchain's popularity, it is a dangerous development for Bitcoin and, apparently, one Nakamoto had not foreseen.

Let's see why.

First, the spike in computational power needed to mine Bitcoins implies a corresponding growth in the network's energy consumption. This has caused mounting concerns regarding Bitcoin's

[39] L. Cocco – M. Marchesi, *Modeling and Simulation of the Economics of Mining in the Bitcoin Market*, in *PLoS ONE*, 11(10), 2016, 4; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, in *Department of Justice Journal of Federal Law and Practice*, 69, 2021, 61.

[40] K. O'Dwyer – D. Malone, *Bitcoin Mining and its Energy Footprint,* in, *Proceedings of the 25th Joint IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 2014, 283, "*The difficulty, D, is recalculated every 2016 blocks, with the aim of keeping the average time to discover a new block near 10 minutes. At this ideal speed, 2016 blocks will be discovered every two weeks. To calculate the new difficulty, the length of time that it took to calculate the last 2016 blocks is used to estimate the hash rate of the entire Bitcoin network. The new difficulty is selected so that if the same average hash rate is maintained, it will take two weeks to calculate the next 2016 block*".

[41] K. O'Dwyer – D. Malone, *Bitcoin Mining and its Energy Footprint,* cit., 283

environmental impact. As calculated by the University of Cambridge,[42] currently Bitcoin consumes more energy than some relatively big Nations such as Sweden or the Netherlands, and this number is expected to further increase.[43] Such energy consumption for a technology which practical use is, at least currently, merely that of speculative investment, seems to many unjustified. This is causing mounting pressure on Bitcoins by regulators, NGOs,[44] and public opinion,[45] which may even hinder its long-term survival. Symbolic is the – although failed – attempt of a group of Members of the European Parliament to add to the Market in Crypto-asset Regulation (MiCaR) a ban on the use of Proof of Work in the European Union, *de facto* banning Bitcoin, precisely due to environmental concerns.[46]

Second, and topical to our ends, this increase has also caused a corresponding centralization of mining. As mining becomes more energy intensive and single-purpose hardware is developed[47] the possibility for individuals to mine Bitcoin has shrunk to the point of nonexistence. This means that mining is currently primarily carried out by professional players.

The progressive centralization of the mining industry raises both an ideological and a security problem.

From the former perspective, mining was initially conceived as an activity carried out by users in a decentralized fashion.[48] Each user could devote a share of its computational power to the

[42] For this and other information and statistics regarding Bitcoin's energy consumption see the Cambridge Bitcoin Electricity Consumption Index compiled by the University of Cambridge, https://ccaf.io/cbeci/index/comparisons

[43] R. Choo, *Bitcoin's Impacts on Climate and the Environment,* in *State of the Planet (Columbia Climate School Blog)*, 20 September 2021, https://news.climate.columbia.edu/2021/09/20/bitcoins-impacts-on-climate-and-the-environment/

[44] One of such examples is the "Change the code not the climate" initiative by Greenpeace, for more information see https://www.cleanupbitcoin.com

[45] See European Parliament, *Cryptocurrencies in the EU: new rules to boost benefits and curb threats*, Press Release, 14 March 2022, "*Mechanisms used to validate transactions in crypto-assets have a substantial environmental impact, particularly for proof-of-work mechanisms, requiring a lot of energy and resulting in a high carbon footprint and generating electronic waste. According to most estimates, the energy consumption of Bitcoin equals that of entire small countries*".

[46] S. Handagama, *Proposal Limiting Proof of Work is rejected in EU Parliament Committeee vote*, in *CoinDesk*, 14 March 2022, https://www.coindesk.com/policy/2022/03/14/proposal-limiting-proof-of-work-is-rejected-in-eu-parliament-committee-vote-sources/

[47] These are known as application-specific integrated circuit (ASIC), see K. O'Dwyer – D. Malone, *Bitcoin Mining and its Energy Footprint,* cit., p. 283; see L. Cocco – M. Marchesi, *Modeling and Simulation of the Economics of Mining in the Bitcoin Market*, cit., for a description of the historical phases of Bitcoin mining, 5.

[48] For a different analysis regarding the real level of decentralization during the early days of mining see the research by A. Blackburn et al., as reported by S. Roberts, *How 'Trustless' Is Bitcoin, Really?* in *The New York*

maintenance of the common network and, in exchange, earn some pocket money[49]. With the professionalization of this activity, individual users are cut out of one of the fundamental functions of blockchain. This way a piece of the "network by the users for the users" is lost, as mining is no longer in the hands of individuals but is shifted towards increasingly larger corporations.[50]

From the latter perspective, one of the premises of blockchain security is that, to guarantee the integrity of the ledger, no entity can control more than fifty percent of the computational power of the network. If the threshold is passed, the entity could manipulate the content of the ledger at will – wedging what is known as a fifty one percent attack.[51] Such a threshold was not problematic as long as mining was a decentralized activity carried out by individual users. However, as it morphs into a professional and centralized activity, a small number of entities have come to control a large share of the market and its computational power. This means that the risk of a fifty one percent attack is not a theoretical possibility anymore, but a very concrete reality.[52]

The question is, then, how could this happen, and why did nobody stop it. The answer brings us back to the tension between decentralization and centralization. Namely, the centralization of mining offers an interesting cautionary tale to anyone devising a fully decentralized solution, as it displays the limits of full decentralization.

Eminently, one of the fundamental steps in the specialization and professionalization of mining has been the adoption of the so-called application-specific integrated circuits (ASIC).[53] These pieces of hardware are specifically designed for mining and, therefore, are sizably better at performing this activity. Their adoption, thus, creates entry barriers to the market as it gives a competitive advantage to professional miners and reduces the probability for an individual using

*Times,* 6 June 2022, https://www.nytimes.com/2022/06/06/science/bitcoin-nakamoto-blackburn-crypto.html, that unveiled that actually mining was highly centralized also in Bitcoin's early days.

[49] G. Hileman – M. Rauchs, *Global cryptocurrency benchmarking study*, cit., 86.

[50] A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, Cambridge Center for Alternative Finance*,* 2020, 30.

[51] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 20. E. Ittay – E. Gün Sirer, *Majority is not enough: Bitcoin mining is vulnerable*, in *International conference on financial cryptography and data security*. Springer, 2014, actually proved that even a minority pool of miners could manipulate the content of the blockchain through what they call selfish mining.

[52] P. de Filippi – B. Loveluck, *The invisible politics of Bitcoin*, cit., 16; for a different "economic" interpretation of the security impact of mining's centralization see Y. Sompolinsky – A. Zohar, *Bitcoin's underlying incentives*, in *Communications of the ACM,* 61.3, 2018, p. 50 and ss, "*On the other hand , it (ASICs)introduces a form of barrier-to-exit, as miners cannot repurpose their equipment to other economic activities; it therefore contributes to security*"; A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, cit., 30.

[53] A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, cit., 32.

a normal computer to successfully mine a block.[54] Satoshi Nakamoto foresaw the effects of this upgrade and tried to stop it. In one of his last posts,[55] he proposed to:

> "*have a gentleman's agreement to postpone the GPU*[56] *arms race as long as we can for the good of the network. It's much easier to get new users up to speed if they don't have to worry about GPU drivers and compatibility. It's nice how anyone with just a CPU can compete fairly equally right now*".[57]

He was, however, unsuccessful and ultimately unable to stop this development and the connected mining arms race.

The mining saga underlines two glitches in fully decentralized environments. First, in the absence of rules to keep the market decentralized, there is a concrete possibility that a small group of motivated individuals will eventually take over the most remunerative positions and, at least partially, recentralize the system. Second, in the absence of any form of centralized governance, competition is the only rule of the game. In such a situation, if individual and common interests are not aligned, the former is likely to prevail, generating detrimental effects for the commons.

## 3.2 From code is law to code without law. Ethereum and the DAO project

The second of our tales is the DAO[58] project.

To understand the DAO, we must first introduce Ethereum. Ethereum is a blockchain network created by Vitalik Buterin in 2014. Ethereum builds upon Bitcoin to create a multi-purpose

[54] Y. Sompolinsky – A. Zohar, *Bitcoin's underlying incentives*, cit., 50, "*ASIC mining introduces a barrier-to-entry to the system, as ordinary people cannot simply join the mining efforts; it thus reduces decentralization*"; A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, cit., 21.

[55] Satoshi Nakamoto was an active member of the Bitcoin community until 2011 when he announced his "retirement" since then the governance of the currency has been passed to a group of individuals known as core developers.

[56] GPU stands for Graphic Processing Units. These were the first upgrade in the mining arms race as these Units performed hashing much faster compared with a normal Computer Processing Unit (CPU)

[57] K. Werbach, *The Blockchain and the new architecture of trust,* cit.

[58] For an explanation of this term see footnote 29.

platform that applies the innovative trust model of blockchain to implementations that go beyond the currency.[59]

Simply put, Ethereum permits the computation and decentralized execution of smart contracts.[60] The main addition of blockchain, and hence Ethereum, to the pre-existing concept of smart contracts, is precisely its decentralization of governance. Namely, as, at least in theory, no one controls the blockchain, once the smart contract is computed and launched, its execution is blindly carried out by the network. This reduces the need for mutual trust between the parties as the only authority they must trust is the code.[61] Moreover, as smart contracts are automatically executed, their implementation eliminates – again, in theory – the need for courts or other dispute resolution bodies.[62]

While the tag "smart contract" recalls legal agreements, smart contracts can be better understood as rules established through code and enforced automatically by a decentralized network.[63] Smart contracts can be, therefore, defined as a general-purpose instrument to establish rules among two or more individuals or to regulate the behaviour of digital objects or organizations.

[59] See Ethereum's website, https://ethereum.org/en/what-is-ethereum/; M. Hütten, *The soft spot of hard code*, cit., 331; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* London, 2023, 136.

[60] The definition of smart contract was first introduced by N. Szabo, *Smart Contracts*, 1994, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html , who described them as "*a smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs*"; see also R. Caria, *Definitions of Smart Contracts: Between Law and Code*, in L. DiMatteo - M. Cannarsa - C. Poncibò (Eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge University Press, 2019, 20. For an analysis of smart contracts see chapter 2 section 8.

[61] V. Gatteschi – F. Lamberti – C. Demartini, *Technology of Smart Contracts*, in L. Di Matteo - M. Cannarsa - C. Poncibò (Eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge University Press, 2019, 44, "*once a smart contract is stored on the blockchain, its code cannot be changed and can be inspected by anyone (even though some programming skills are required to understand it). Hence, everyone could know and foresee the behavior of the smart contract*".

[62] R. Morrison – N. Mazey – S. Wingreen, *The DAO controversy: the case for a new species of corporate governance?*, in *Frontiers in Blockchain* 3, 2020, 2

[63] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 43 – 44, defines a smart contract as "*a computer protocol that facilitates, verifies and executes transactions. These computer programs are not "smart" in the sense that they do not change their behaviour over time, but instead simply execute code when predefined conditions are met. Smart contracts are also not necessarily contracts in the legal sense. The term "automated clause execution tool" could thus better describe their nature*".

Ethereum's smart contracts, thus, permit the creation of innovative – "trustless" – forms of cooperation and coordination between individuals.[64] Among them, the computation of self-executing rules allows the establishment of horizontal, headless organizations exclusively rooted in the law of the code.[65] The main touted benefits of such organizations are that they reduce costs – eliminating intermediaries, such as directors – and allow the shareholders to directly engage in the management of the common good – reducing the dealignment between shareholders' and directors' interests.[66] Furthermore, as argued by Primavera De Filippi and Aaron Wright, the establishment of the "lex cryptographia" permits *ex ante* enforcement of rules and significantly narrows the possibility for opportunistic behaviour or non-compliance.[67]

The first experiment in such an innovative decentralized management structure was launched in 2016 under the name the DAO[68] – an acronym for Decentralized Autonomous Organization. This project is a great example of the opportunities and limits of decentralization and of the role the law will play in a future decentralized society.

The DAO was an investor-directed venture capital fund. The idea was to create an investment fund in which choices of investment were decided directly by the shareholders eliminating the need for directors and other middlemen.[69] In a nutshell, the DAO's smart contract was entrusted with a budget in Ether – Ethereum's native cryptocurrency. Once the Fund received investment offers by so-called contractors, it would broadcast them among its shareholders who would then vote and decide in which project/s to invest. The smart contract would, then, register the results and autonomously dispense the funds based on shareholder's preferences. Any activity that went beyond the reception of offers and the disbursement of funds – such as hiring employees or paying

[64] R. Morrison – N. Mazey – S. Wingreen, *The DAO controversy,* cit., 3; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 9.

[65] P. De Filippi – A. Wright, *Blockchain and law. The rule of code*, Harvard University Press, 2018; R. Morrison – N. Mazey – S. Wingreen, *The DAO controversy,* cit., 2; for an analysis of such organizations see chapter 5 on DAOs regulation.

[66] As explained in the Ethereum's website "*Starting an organization with someone that involves funding and money requires a lot of trust in the people you're working with. But it's hard to trust someone you've only ever interacted with on the internet. With DAOs you don't need to trust anyone else in the group, just the DAO's code, which is 100% transparent and verifiable by anyone*", see https://ethereum.org/en/dao/; see also R. Morrison – N. Mazey – S. Wingreen, *The DAO controversy,* cit., 9.

[67] P. De Filippi – A. Wright, *Blockchain and law. The rule of code*, cit.

[68] For an overview see, D. Harrison, *Decentralized autonomous organization,* Allen & Overy, 2016, 2 – 3; P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, in *European Company and Financial Law Review* , 4, 2018, 651.

[69] R. Morrison – N. Mazey – S. Wingreen, *The DAO controversy,* cit., 1.

for a service – had to be voted by the shareholders.[70] The whole project was rooted in the idea that the only rule was the rule of code as carved in the DAO's smart contract.

The venture was received with great excitement by the blockchain community, and the DAO raised the equivalent of one hundred and sixty million dollars in financing.[71] Notwithstanding the extensive financing and the general excitement, the DAO never became operational as, before it had ever received any financing proposal, it was attacked by a, still unidentified, hacker that was able to exploit a vulnerability in the DAO's code to drain its funds.[72]

This attack opened one of the biggest crises in Ethereum's history. In deciding how to respond to the hack, the developers were showing how far they were willing to go to uphold their values. Namely, if, as stated in the DAO's terms of service, the only rule was the rule of code, then technically the hacker had legitimately obtained the funds as they had acted in accordance with the DAO's source code.[73] Furthermore, to reverse the attack, Ethereum would have had to retroactively modify the content of its blockchain. This action would have broken the dogma of the immutability of the ledger and proved that Ethereum was not a fully censorship-resistant autonomous network, given that it could be manipulated by a relatively small group of programmers.[74] Finally, and at a more general level, reversing the attack would have proven that the rule of code does not eliminate the need for centralized human intervention: when disputes arise, or crime happens, human societies – even if digital – still need third party involvement. Thus,

[70] D. Harrison, *Decentralized autonomous organization,* cit., 3; P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, cit., 651.

[71] M. Hütten, *The soft spot of hard code: blockchain technology,* cit., 336; P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, cit., 651.

[72] For an account of the facts and of the subsequent investigation see M. Leisig, *My trip Down the Crypto Rabbit Hole in search of the DAO hacker,* in *Bloomberg,* 16 September 2020, https://www.bloomberg.com/news/articles/2020-09-16/a-trip-down-the-crypto-rabbit-hole-in-search-of-the-dao-hacker

[73] As reported by M. Hütten, *The soft spot of hard code: blockchain technology,* cit., p. 337, "*Some members of the Ethereum community even argue that the presumed 'theft' of funds by the hacker was not even 'theft' but in line with the DAO's terms, since they state that whatever the code allows someone to do would be the intention of the code*"; D. Harrison, *Decentralized autonomous organization,* cit., 5, "*in the case of The DAO, the hacker merely used the code to his or her advantage; in that sense, they acted in accordance with the terms of the smart contract and arguably there was no hack*".

[74] D. Harrison, *Decentralized autonomous organization,* cit., 7, "*To circumvent the rules of The DAO by a hard fork is to undermine the principles of immutability, trust, and decentralization which are core tenets of the blockchain and its smart contracts*".

disproving the claim that blockchain would bypass courts and make dispute resolution bodies obsolete.[75]

Notwithstanding all these high level ethical, legal, and philosophical concerns, the community decided that "money is money" and the transactions were reversed.[76] The Ethereum foundation – among which there were some of the most prominent investors in the DAO – and its founder, Vitalik Buterin, convinced the network to proceed with a hard fork[77] that erased the attack. However, to highlight the paradox of such a move in a decentralized environment, not all miners backed the hard fork, and some decided to keep mining the old Ethereum blockchain. *De facto*, this duplicated Ethereum with the original version of the Ethereum's blockchain being renamed Ethereum Classic.[78]

Interestingly enough, notwithstanding the clear conflict between Ethereum's actions and its core values, the network weathered the storm.[79] Ethereum is currently one of the most prominent blockchain platform, and it is the main infrastructure for the market's latest decentralized innovations – as Non-Fungible Tokens (NFT) and Decentralized Finance (DeFi).

## 4. The future. Orwell or Rousseau?

[75] As reported by D. Harrison, *Decentralized autonomous organization,* cit., 4, "*For opponents, a hard fork would be entirely antithetical to Ethereum's cause. Ethereum's stated purpose, after all, is to provide an immutable, incorruptible record and a platform for unstoppable, code-as-law smart contracts. The hard fork would amount to an intervention – a bail-out of The DAO – seemingly at the behest of The DAO's biggest investors (themselves Ethereum developers and influential community members)*"

[76] As noted by M. Hütten, *The soft spot of hard code: blockchain technology,* cit., 330, "*When the highly publicized but faultily crowdfunded venture fund called 'The DAO' (an instance of a decentralized autonomous organization) was deployed on the Ethereum blockchain, the techno-utopianism was suspended, and developers fell back on strong network ties*". As it is obvious, mine is partially a simplification and partially a speculation regarding the root causes of the choice that led the Ethereum community to reverse the blockchain.

[77] A hard fork is a permanent split in the blockchain that causes the coexistence of two parallel ledgers, in the case of Ethereum, Ethereum (the new version where the attack had been erased) and Ethereum classic (the old version where the attack still had happened); for a clear description of the DAO fork see Security and Exchange Commission, *Release No. 81207 / July 25, 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Washington, 2017, 9.

[78] Ethereum classic is still operational today six years after the attacks; see also, R. Morrison – N. Mazey – S. Wingreen, *The DAO controversy,* cit., 7.

[79]G. Hileman – M. Rauchs, *2017 global cryptocurrency benchmarking study*, Cambridge Center for Alternative Finance, 2017, 16, "*The price of ether has also recovered since a series of attacks on the Ethereum ecosystem, starting with the DAO hack in June 2016, and increased 8x since its 2016 low of less than $7 in December*".

The previous section has retraced how the fully decentralized dream of the early blockchain developers was confronted with the hard realities of governance and human nature.[80] The present section will, then, analyse how the market has responded to such failures and the resulting clash between centralization and decentralization that distinguishes the current (and future) blockchain landscape. Namely, if the archetypal blockchain was fully decentralized, both in its logic and governance structure, the last few years have seen a progressive development of (semi)centralized projects.[81]

This is partially a response to the abovementioned failures and inefficiencies of fully decentralized projects, that have reminded the market of the rationale of the traditional intermediated infrastructure.

This is also, however, due to two historical trends.

On one hand, as the price of Bitcoin and other cryptocurrencies soared and the tokens attained larger adoption, "lay" users have increasingly demanded centralized services. Providers – such as cryptocurrency wallets, exchangers, etc. – have moved away from the peer-to-peer model towards an increasingly centralized industry.[82] If (at least some) cypherpunks thought that they needed to free "the people" from the tyranny of intermediaries, the recent history of blockchain seems to raise doubts regarding whether the people want to be freed at all.

On the other hand, as states and corporations jumped on the blockchain bandwagon, they have started to model the technology to their statutory needs and obligations – e.g., privacy regulations and intellectual property protection.

[80] For another tale of centralization see P. de Filippi – B. Loveluck, *The invisible politics of Bitcoin*, cit., p. 13, "*(this conflict) has also emphasised the tension between the (theoretically) decentralised nature of the Bitcoin network and the highly centralised governance model that has emerged around it, which ultimately relied on the goodwill and aligned interests of only a handful of people*".

[81] D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, in *European Business Organization Law Review*, 20, 2019, 674.

[82] For an overview of the industry see G. Hileman – M. Rauchs, *Global cryptocurrency benchmarking study*, cit., 25; I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces* in *Journal of Cybersecurity*, 1, 2021, 3.

Within this prism, a new, less activist, form of blockchain has emerged during the last decade – the private and/or permissioned ledgers.[83] This second stream separates the decentralization of the information from the decentralization of the control. From this perspective, blockchain is envisioned as a trust accelerator or enabler rather than a system to reinvent pre-existing power structures. Through blockchain the information is kept in one common ledger rather than in private fragmented ledgers, this streamlines trust brokerage and lowers information reconciliation costs. At the same time, this type of blockchain does not entail a complete loss of control on the side of the participants as it still provides for a customizable degree of centralized governance.[84]

Central Bank Digital Currencies (CBDCs)[85] - such as the recently launched Chinese e-Renminbi – are a great example of this second stream of development: with blockchain, Central Banks can create a single ledger where to register all transactions performed with the sovereign fiat currency while allowing intermediaries and individuals to interact with that ledger. However, CBDCs do not in any way imply that Central Banks lose control of the monetary supply. Quite the contrary, CBDCs provide to these institutions a larger control, not only of the monetary supply but, in general, of the financial flows as these are now registered in a logically centralized ledger held by the Central Bank.

[83] For an analysis regarding the differences between Public and Private blockchains see P. Jayachandran, *The difference between public and private blockchain*, in *Blockchain Pulse: IBM Blockchain Blog*, https://www.ibm.com/blogs/blockchain/2017/05/the-differen- ce-between-public-and-private-blockchain/; on a possible reversion of this trend towards private blockchains see P. Brody, *How public blockchains are making private blockchain obsolete*, https://www.ey.com/en_gl/innovation/how-public-blockchains-are-making-private-blockchains-obsolete; A. Shahaab et al., *Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review*, in *IEEE Access*, 7/2, 2019 describes and classifies blockchains as "*Public DLTs are fully decentralised. No one controls the network and participation in consensus process is open to everyone and all transactions are visible to the public. This "openness" ensures that the data on the DLT cannot be changed once it has been validated and accepted by the network. Bitcoin and Ethereum are examples of a public DLTs. In private DLTs, only authorized nodes from an organization can take part in the consensus and have read/write permission in private DLTs. One or multiple entities control the access to the private DLTs, restricting the participation in the network. Hyperledger Fabric and Multichain are examples of private DLTs. Consortiums are essentially private DLTs shared between multiple organizations. Different organizations come together to form a consortium and nominate members to take part in the consensus process. Quoram and Corda are examples of consortium DLTs*". For an analysis of permissioned blockchain see chapter 2 section 7.

[84] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 29; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 36.

[85] For an insight in the functioning and rationale of CBDCs see G. Soderberg, *Behind the Scenes of Central Bank Digital Currency Emerging Trends, Insights, and Policy Lessons*, Fintech Notes International Monetary Fund, 2022; see also for a collection of current projects the Bank of International Settlement Innovation Hub work in the field at, https://www.bis.org/about/bisih/publ.htm?m=3103

On a similar note, in the private sector, the implementation of blockchain in the field of supply chain aims to provide the operators with a single source of truth that will guarantee to each one the control of their proprietary data. Just to mention one of such project, Maersk and IBM joined forces in mid-2017 to launch a blockchain project for the shipping industry.[86] This project, called TradeLens,[87] aims at optimizing the flow of documents and thus saving costs and time. The partnership between IBM and Maersk aims to implement a platform that will enable better tracking of goods throughout the supply chain. It will also facilitate the real-time traceability of payments within the shipping industry and clearance procedures that could be subject to fraud. It is programmable based on each business logic of a potential client: the companies aim to bring the industry together on an open blockchain platform whereby all players involved in the global supply chain – i.e., exporters, importers, carriers, freight forwarders, shipping companies, terminals, customs, and government authorities, etc. – can participate to efficiently oversee the exchange of information as well as foster more intense collaboration across the supply chain.

This trend towards, at least partial, centralization is of prime relevance for our ends as it constitutes the most impactful historical development for financial flow control as it could, ironically, turn an instrument conceived for decentralization and anonymity into a vehicle for perfect control. Namely, as explored in greater detail in the following chapters, blockchain's decentralization of control is the crux of the financial integrity conundrum.[88] As correctly predicted by the cypherpunks, a fully decentralized and transnational infrastructure is particularly difficult to police and monitor as there is no single point of pressure to regulate and coerce. However, the same

[86] Y.A. Xia - S. Grover - R.C. Lieb, *Keeping PACE with blockchain in ocean transportation*, in *Supply Chain Management Review*, 2021, 25, 3; A. Schmahl - S. Mohottala - K. Burchardi - C. Egloff - J. Govers - T. Chan - M. Giakoumelos, *Resolving the Blockchain Paradox in Transportation and Logistics*, Boston Consulting Group, 2019, available at https://www.bcg.com/it-it/publications/2019/resolving-blockchain-paradox-transportation-logistics.aspx report that as of March 2020, TradeLens included over 20 ocean carriers and providers, over 100 international ports and terminals, more than 10 government agencies, more than 20 operators ports and terminals around the world (Port of Singapore Authority, Port of Rotterdam, etc.), global container shipping operators (Maersk Line, Hamburg Sud and Pacific International Lines), customs authorities (in Singapore, the Netherlands, Saudi Arabia, Australia) and logistics operators (e.g. CEVA Logistics, Damco, Kotahi, PLH Trucking Company, WorldWide Alliance); for other use cases see The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 38.

[87] See https://www.maersk.com/apa-tradelens.

[88] C. Kuner – F. Cate – O. Lynskey – C. Millard – N. Ni Loideain – D. Svantesson, *Blockchain versus data protection,* cit., 104, "*It is, however, the very openness, lack of permissioning, and potential anonymity that make public block- chain systems like Bitcoin problematic from a legal and regulatory perspective. For example, how can a financial services regulator check that anti-money laundering (AML) and know your customer (KYC) rules are being complied with if a large number of parties can transfer tokens between each other without involving any regulated entity or other intermediary that can be audited?*".

infrastructure, if centralized governance is introduced, could present new opportunities for monitoring as the information structure of blockchain – logically centralized but organizationally decentralized[89] - would provide a single source of truth to oversee and analyse all financial transactions.

This drift is also an interesting cautionary tale for digital enthusiasts in general. Namely, decentralization is frequently presented as a key element of digital innovations. It is, however, seldomly underlined that individuals often prefer to, at least partially, outsource decisions and responsibilities to intermediaries. Internet ideology tends to be characterized by a utopistic understanding of individuals that, in its extreme version, are presented as completely self-sufficient animals only longing "to be left alone".[90] The net effect of this utopia has, however, mostly been to remove the power from established, and highly regulated, intermediaries – as States – to then see new, and much less regulated, intermediaries take their place.

It is important to underline that this trend towards increased centralization in the blockchain market has been all but uncontested. Early developers and users – so-called purists – have pushed back on any form of centralized blockchain. Completely decentralized projects have flourished together with more traditional, corporate ones and the fight is far from over.

However, some have seen in blockchain's evolution a repetition of the Internet saga, from a haven of decentralization to a strictly surveilled oligopoly.[91]

The emergence of this trend has been so marked and relevant to even push one of the ideological fathers of crypto to rethink the impact of digital currencies in terms of individual freedom. Namely, cypherpunks' founder Timothy May has recently declared of Bitcoins:

[89] Quote from K. Werbach, *The Blockchain and the new architecture of trust*, cit., 7. With this sentence it is meant that, while blockchain decentralizes access to the ledger, it also centralizes information, by compiling in a single ledger all the information that were traditionally held by each intermediary. For more on the blockchain privacy structure see chapter two, section six.

[90] P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 31 – 32.

[91] I. Bogost, *Cryptocurrencies may be a path to authoritarianism*, The Atlantic, 30 May 2017, https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/; see also P. De Filippi – M. Mannan – W. Reijers, *Blockchain as a confidence machine: The problem of trust & challenges of governance*, in *Technology in Society*, 62, 2020, "*the governance of most blockchain-based systems is highly centralized: on-chain governance is inherently plutocratic, dominated by a few large operators or individuals who control most of the mining resources and/or token holdings, whereas off-chain governance most often operates as a technocracy, with a few influential players dominating both the front-stage and the backstage*".

*"There's a real possibility that all the noise about 'governance,' 'regulation' and 'blockchain' will effectively create a surveillance state, a dossier society (…) Sorry if this ruins the narrative but I think the narrative is fucked. Satoshi did a brilliant thing, but the story is far from over".*[92]

## 5. Final remarks

Nearly two decades after the publication of the Bitcoin paper, blockchain has lived a roller coaster of emotions. Presented as a one-stop-shop for anonymity through cryptography, it has faced the hard truths and limits of decentralization. Still, it has somehow survived these crises, and, notwithstanding the critics, it continues to foster and promote innovation. At the same time, despite the frenzy and investments, this technology has still not produced any tangible large-scale implementation. Even Bitcoin, arguably the most successful blockchain experiment, has fundamentally failed in its purpose of becoming a stateless global currency and is currently primarily a speculative investment asset.[93]

However, while fifteen years may seem long in our digital age, it may just be that an innovation such as blockchain, that proposes a change in the fundamentals of our economic system, will take longer to take hold. Namely, even though no tangible use for cryptocurrencies has still been found, their value keeps rising[94] – or some would say bubbling – up to a point where it cannot be ignored anymore.[95] Also, new blockchain implementations keep emerging daily and receive a spasmodic, although sometimes brief, attention from the media, public opinion, the business and academic community – as Non-fungible Tokens, Decentralized Finance, and Central Bank Digital Currencies.

[92] Quote reported by P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 72.

[93] P. de Filippi – B. Loveluck, *The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure*, cit., 10; Bank of England, *Financial Stability in Focus: Cryptoassets and decentralised finance*, London, 2022, 7.

[94] Bank of England, *Financial Stability in Focus: Cryptoassets and decentralised finance*, cit., 10.

[95] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 8; E. McCaul, *Mind the gap: we need better oversight of crypto activities*, European Central Bank Blog, 5th April 2023, https://www.bankingsupervision.europa.eu/press/blog/2023/html/ssm.blog230405~03fd3d664f.en.html.

Interestingly enough these implementations still cover the full decentralization spectrum, and no clear winner can be identified in the, abovementioned, fight for the soul of blockchain. On one side of the spectrum, Central Bank Digital Currencies aim to use the technology that promised to make Central Banks obsolete to issue fiat currencies. On the other side, Decentralized Finance (DeFi)[96] promises to restructure the way financial services are offered to eliminate middlemen and promote rule by code.[97] Additionally, several other projects have flourished that mix decentralization and centralization.

These two strands of blockchain development carry very different implications for the anti-money laundering regulation. Their coexistence, thus, requires the policymaker to recognize this historical trend and diversify its approach depending on whether the individual project decentralizes information storage, governance, or both. Namely, if in completely decentralized systems regulating may be too hard, in partially decentralized ones it could, paradoxically, be too easy and, therefore, require safeguards that guarantee privacy rather than transparency.[98] Technological customization is, hence, key in this field.

[96] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, Paris, 2022; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 2, defines decentralized finance as "*a set of crypto-asset services, which are similar to financial services and carried out without the intervention of an intermediary*".
[97] World Economic Forum, *Decentralized Finance (DeFi) Policymaker Toolkit*, White Paper, 2021, 6, "*the goal of DeFi solutions is to provide functions analogous to, and potentially beyond, those offered by traditional financial service providers, without reliance on central intermediaries or institutions*".
[98] This is, for instance, the case when it comes to CBDCs, as is clearly underlined by the great attention paid to privacy in the development of digital euro. As highlighted by the European Data Protection Board in its, European Data Protection Board, *EDPB letter to the European institutions on the privacy and data protection aspects of a possible digital euro,* 18 June 2021, *"an inappropriate design of the forthcoming digital euro would bring significant risks under the data protection perspective. Relevant safeguards shall be put in place in order to avoid, for example, genera lised tracking of user transactions throughout the payment system and to address and mitigate the risk of excessive interference in privacy of the persons concerned by both centralized entities and market operators*", in a similar sense The White House, *Technical evaluation for a U.S. Central Bank digital currency system,* Washington, 2022, 65, "*even if policies exist to prevent this harm at this time, enabling this capacity could allow a future Administration to use the CBDC system to surveil the population in close detail".*

# Chapter Two

## Understanding blockchain

## The technological background

### 1. Introduction

Having explored the historical rise and evolution of blockchain, it is now time to delve into its functioning. The present chapter aims to do this by outlining the main elements of this technology and drawing some internal distinctions. A *caveat* before we start, given the scope of the present work, it is not my purpose to provide an in-depth analysis of the technology. Rather, this chapter will delineate the logic underlying the blockchain so to fill with technical content the subsequent policy analysis and facilitate the reader's understanding.

So, what is blockchain?

Blockchain is, fundamentally, a recordkeeping technology. While recordkeeping may seem like a trivial and inconsequential activity, it sits at the core of our social and economic infrastructure.[1] The who, where, and how of data storage is key in understanding the power balance and functioning of a community. Most importantly, record-keeping relates to one of the most

[1] As argued by B. Sudipta – G. B. Waymire, *Recordkeeping and human evolution*, in *Accounting horizons* 20/3, 2006, 201 "*systematic recordkeeping outside an individual brain is a necessary condition for the emergence of extended economic cooperation that ultimately leads to complex human societies, markets, and economic organizations*", The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26, "*Recording the ownership and movement of value has been a central tenet of human civilisation*".

significant and yet impalpable elements of organized societies: trust.[2] While trust is a complex phenomenon – as it always needs a "touch of magic", meaning a leap of faith that cannot be simply explained through logic[3] – its connection to the availability of reliable information is clear. To thrive and trade, people need to have access to trustworthy information that can guide rational decision-making.[4] Flaws in crucial record-keeping systems – such as land registries, or financial intermediaries – hinder economic growth and ultimately the prosperity of a community.[5]

Not only does the existence of solid record-keeping mechanisms shape a community's fortune, but the way record-keeping is structured is a key element in understanding societal power dynamics.[6] The entities entrusted – by regulation or market – with record-keeping functions gain enormous power from the knowledge they accrue and from their unique role as data sources. From financial institutions to tech giants, the entities managing valuable data wield an enormous influence on our societies.[7]

[2] As underlined by D. Rousseau, et al., *Not so different after all: A cross-discipline view of trust* in *Academy of management review*, 23/3, 1998, the definition and conformation of trust are debated topics; however, most commentators agree that trust entails one party taking a risk – more or less calculated and rational – and relying on another party in order to obtain a desired outcome while having little or no control over the counterparties' behavior. See the definition of B. Devdeepta – C. Camerer, *Trust and Behavioral Economics* in F. Krueger (eds.), *The Neurobiology of Trust*, Cambridge University press, 2021, 37, "*trust is defined as the expectation that another person (or entity) will repay a socially risky action by the trustor that benefited both the trustor and the trustee, in a way that makes the trustor happy that she was trusting*" and the one of D. Rousseau, et al., *Not so different after all: A cross-discipline view of trust*, cit., 395, "*Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*".

[3] As stated by P. De Filippi – M. Mannan – W. Reijers, *Blockchain as a confidence machine: The problem of trust & challenges of governance*, cit., 3, "*trust inevitably comes along with a certain degree of risk and vulnerability*"; see also B. Devdeepta – C. Camerer, *Trust and Behavioral Economics,* cit.

[4] P. De Filippi – M. Mannan – W. Reijers, *Blockchain as a confidence machine: The problem of trust & challenges of governance*, cit., 4; B. Sudipta – G. B. Waymire, *Recordkeeping and human evolution*, cit., 202.

[5] For a review of how trust level impact economic growth see B. Devdeepta – C. Camerer, *Trust and Behavioral Economics,* cit., 48.

[6] C. Findlay, *Participatory cultures, trust technologies and decentralisation: innovation opportunities for recordkeeping*, in *Archives and Manuscripts*, 45/3, 2017, 177.

[7] M. Finck, *Blockchains and data protection in the European Union,* in *European Data Protection Law Review,* 4, 2018, 6.

The blockchain can, thus, be described as a technology of trust.[8] One that strikes at the heart of the traditional record-keeping infrastructure and proposes a new system to store and update valuable data[9] with the normative aim of displacing classic power dynamics.[10]

## 2. Understanding blockchain record-keeping mechanism. Trustless trust?

Let's, then, delve into the blockchain record-keeping system.

Any record-keeping technology has a static element – how data is stored, and its integrity guaranteed – and a dynamic one – how data is updated, and its veracity ensured. Blockchain modifies both, to eliminate (or at least reduce) the reliance on trust intermediaries.[11] As detailed in the historical section, this modification does not simply stem from an efficiency need, rather it is a normative choice – a "code through law" action – aimed (at least in theory) at giving back the control of data to the people.

[8] For a complete overview of the role of blockchain as a trust machine see K. Werbach, *The Blockchain and the new architecture of trust,* cit.; see also P. De Filippi – M. Mannan – W. Reijers, *Blockchain as a confidence machine: The problem of trust & challenges of governance*, cit.; A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, O'Reilly, 2017, 15.

[9] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain* in *University of Chicago, Becker Friedman Institute for Economics Working Paper,* 83, 2022, 1.

[10] R. Auer *Embedded Supervision: How to build regulation in decentralized finance*, CESIFO Working Papers, 9771, 2022, 3; D.A. Zetzsche - R.P. Buckley - D.W. Arner - M.C. van Ek, R*emaining regulatory challenges in digital finance and crypto- assets after MiCA,* European Parliament, 2023, 23, "*DeFi seeks to address through technology what crypto proponents understand as the source of traditional finance's instability: the centrality (if not dominance) of concentrated intermediaries and the 'too-big-to-fail' risks they embody – and the reliance on the weaknesses of states, governments and regulators. DeFi envisages a utopia where technology replaces frail humans and their institutions: a world in which technology eliminates the risks inherent in the concentrated systems central to traditional finance*".

[11] M. Zou, *Code, and other laws of blockchain* in *Oxford Journal of Legal Studies*, 40/3, 2020, 646; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 4; D.A. Zetzsche - R.P. Buckley - D.W. Arner - M.C. van Ek, R*emaining regulatory challenges in digital finance and crypto- assets after MiCA,* cit., 23; E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 3.

To understand the new approach, we need to first appreciate how things have been done until now.

The traditional strategy to create shared trust in data has been the use of third parties.[12] In the classic system, it is up to such trust intermediaries to store and update information. This means, from a record-keeping perspective, that each intermediary holds its private ledger and is solely responsible for its integrity and update.[13] When a transaction involving customers of different intermediaries – hence information stored in different ledgers – is carried out, these must communicate to reconcile their respective ledgers and ensure consistency.

This record-keeping strategy has two main characteristics: it is centralized, in terms of access/control, and is fragmented, in terms of content. From the former perspective, it is centralized as information is privately held by each institution. Each intermediary retains exclusive access to its ledger and is the only one that can consult and adjourn it. From the latter perspective, it is fragmented as there is no shared ledger encompassing the whole market, each intermediary's ledger only records that part of the information trail that pertains to its customer.

To better understand the functioning of this record-keeping strategy let's take financial transactions as an example. In the classic system, to access the digital financial market, everyone must open an account with an intermediary – i.e., a Bank or some other type of Financial Service Provider. The intermediary holds a ledger recording the balance of each customer and the transactions they have performed. When a transaction involves customers of different intermediaries, the two financial institutions communicate to guarantee that the information recorded in the respective ledger is consistent. This system is centralized, from a control perspective, as the ledger is held privately by each institution, and fragmented, from a content perspective, as the transaction trail is partitioned among the different intermediaries with each ledger only recording its side of the information.

[12] A. Blandin, et al., *Global cryptoasset regulatory landscape study*, in *University of Cambridge Faculty of Law Research Paper,* 23, 2019, 14, "*Until recently, digital tokens mostly existed in the form of ledger entries in internal database systems maintained by trusted third parties. Blockchain and DLT systems are new shared accounting tools that enable distributed recordkeeping without the need to rely on a single controlling party*".

[13] D.A. Zetzsche - R.P. Buckley - D.W. Arner - M.C. van Ek, R*emaining regulatory challenges in digital finance and crypto- assets after MiCA,* cit., 23.

The blockchain revolutionizes this record-keeping strategy. With blockchain all transactions carried out within a certain environment – e.g., a crypto-asset – are recorded in a single ledger which is shared and maintained by all the nodes – i.e., the participants – of the network.[14]

The ledger is, hence, contrary to the traditional system, decentralized in terms of access/control, and centralized in terms of content. From the former perspective, the access is decentralized as each node holds one identical copy of the ledger. The information is simultaneously shared among all participants and each node has access to a complete copy of the same ledger. The same goes for the update of the ledger: there is no single authority that unilaterally updates it, on the contrary, this is done by all the nodes in a choral manner following a pre-established consensus protocol.[15] From the latter perspective, the content is centralized as all the information is recorded in the shared ledger. There is no private ledger held by a single intermediary solely recording the balances and transactions of its clients. Rather, there is a common ledger that records all interactions among all the participants in a logically centralized fashion.

Let's go back to our previous example of financial transactions to see how the record-keeping structure changes when blockchain is introduced. A classic example of a blockchain-based transaction system is Bitcoin. Let's then analyse a Bitcoin transaction from a record-keeping perspective. Contrarily to the traditional system, to access the Bitcoin network users do not need an intermediary, although using one is possible. They can directly access the network through a so-called self-hosted wallet.[16] If user A wants to, then, send Bitcoin to user B they create a transaction – meaning a computer command containing A's digital signature, B's address, and the amount to be transferred – and broadcast it to the network.[17] Each node of the network checks if the transaction is valid – meaning that, according to their copy of the ledger, A owns the amount they intend to transfer and their signature is valid – and, if so, the latter is added to the common ledger by a miner node.[18] Every node of the network can then access the ledger and check the

[14] H. Axelsen – J. Jensen – R. Omri, *When is a DAO Decentralized?, in Complex Systems Informatics and Modeling Quarterly,* 31, 2022, 53.

[15] For a detailed explanation of what a consensus protocol is see section 4 of this chapter; P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, cit., 650.

[16] For a more detailed analysis of how blockchain transactions work see section 5 of the present chapter; B. Mesquita – S. Maranhao – J. Seigneur, *Enabling KYC and AML verification in DeFi service*, Crypto Valley Association, Zug, 2022, 4.

[17] A. Trozze, et al., *Cryptocurrencies and future financial crime*, in *Crime Science,* 11/1, 2022, 2.

[18] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain,* cit., 10, "*When a miner finds a lucky alphanumeric string, they publicly broadcast their block — consisting of the transactions, the hash of the previous block, their lucky alphanumeric string, and their block's hash — to all of the other Bitcoin miners. Other Bitcoin*

transaction. Moreover, given that all transactions are stored in a single common ledger, the whole money trail – meaning the chain of transactions preceding the one between A and B – can be pieced together by simply consulting the blockchain.

## 3. The storage model

Having detailed the logic underlying blockchain record-keeping, we must now delve into the nitty-gritty of its functioning.

As mentioned above, any record-keeping technology has two basic components: static and dynamic. This section will examine the static element of blockchain by describing how information is stored and its integrity ensured. To understand blockchain's storage model we must distinguish among two levels: first, where and how the information is stored; second, where and how the ledger – meaning the record containing all the information – is stored.

### 3.1 The storage of the data

Starting from where and how the information is stored, the blockchain, as the name goes, is fundamentally a chain of blocks.[19] Each block of the chain contains a fixed amount of information – in the case of Bitcoin, from one thousand to two thousand transactions[20] – which is inextricably

*miners can quickly check whether the block is valid; that is, does the set of transactions in the block meet the criteria (…) and does the alphanumeric string indeed produce a valid hash with enough leading zeros. Note, critically, that while finding a lucky alphanumeric string is extremely computationally intensive, checking the validity of a given block is computationally trivial. For this reason, a valid block is "proof of work" — proof that the miner who found the block did a large amount of computational work in expectation*".

[19] Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* Paris, 2015, 40; C. Leuprecht - C. Jenkins – R. Hamilton, *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*, in *Journal of Financial Crime*, 2022, 4.

[20] C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 90.

linked with the information recorded in the previous blocks.[21] The way these blocks are linked together is through the inclusion, in each block, of a hash of the data contained in the previous block.[22]

To better understand how hashing guarantees the integrity of blockchain data we need to take a short detour and briefly introduce hashing.

A hash can be defined as:

> "*a mathematical function that converts an input of arbitrary length into an output of a fixed length. Thus, regardless of the original amount of data or file size involved, its unique hash will always be the same size*".[23]

For instance, using the SHA-256 hashing function[24] the hash of the sentence "Hello, how are you?" is "04cdee65fb33653432b0e56abd32c878f2a13286bfc6ddab85472fd3855d7f2e", using the same function, the hash of the entire section two of this chapter is "6cd947fa4ceda20591c14ce78f9d0f8af573fec5c5785975eca23676ea80d031".

A hash is, thus, made up of three elements: the source data, the hashing function, and the hash. When the hashing function is applied to the source data it produces a hash – meaning an alphanumeric string of fixed length. To put it plainly, a hash can be described as a non-descriptive fixed length summary of a certain piece of information to which it is univocally linked. Even a slight modification of the source data will modify the connected hash. This guarantees that, as long as the hash is not modified, the underlying data is intact. To go back to our example, if we change even one letter of section two, this will modify the corresponding hash making any tampering immediately apparent.[25]

[21] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities*, Royal United Services Institute for Defence and Security Studies, London, 2017, 3; M. Finck, *Blockchains and data protection in the European Union,* cit., 18.

[22] This use of hashes to chain together a sequence of blocks of data was first introduced by S. Haber - W.S. Stornetta, *How to time-stamp a digital document* in *Journal of Cryptology*, 3/2, 1991; E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain,* cit., 8; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 60.

[23] Definition provided by J. Frankenfield, *Hash,* in *Investopedia,* 13 January 2022

[24] For further info on SHA 256, N-able, *SHA-256 Algorithm Overview*, 12 September 2019, https://www.n-able.com/blog/sha-256-encryption.

[25] M. Nofer, et al. *Blockchain,* cit., 184.

Furthermore, hash functions are one-way functions. This means that given the message it is easy to compute its hash. However, given the hash it is extremely difficult to compute the initial message.[26] This means that I can publicly share the hash function of a certain message or text while, at the same time, ensuring the secrecy of the underlying message.

These characteristics of hashes have fostered their implementation in several fields where guaranteeing data integrity is crucial. One that is familiar to legal scholars is computer forensics.[27] There hashes are used as digital seals to guarantee the integrity of seized data. If the police wants to seize a digital document, it first computes its hash. This way, by solely checking the hash, anyone can verify whether the underlying document has been modified while in police custody. This method also allows the police or the prosecutor to share with the defence the metadata that guarantees the integrity of the document – i.e., the hash – without having to disclose its content – thanks to hashes irreversibility.

Let's see, then, how this is applied when it comes to blockchain. As previously stated, encoded within each block of the chain is the hash of the previous block. The same goes for each block up to the first one – the so-called genesis block.[28] This means that any modification in the content of any part of the chain would impact its hash and, automatically, the hashes of all those that follow the tampered one in the chain. A change in the content of any block would, thus, be displayed in the hash of each block following the affected one – including the last in the chain – making any attempt to tamper blockchain's content immediately apparent to the whole network.

Not only are the blocks necessarily interlinked through the respective hashes, but the same also goes for the data they contain. A precondition to having a new string of data added to the blockchain is that this must be consistent with the data present in the previous blocks. Each transaction of the blockchain is interlinked with a previous transaction recorded in a previous block allowing to follow that specific transaction trail up to its source.[29]

[26] M. Finck, *Blockchains and data protection in the European Union,* cit., 19.

[27] G. Ranganathan - X. Fernando – S. Fuqian*, Inventive Communication and Computational Technologies*, Springer, 2021.

[28] A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., glossary, blockchain.

[29] S. Hughes, '*Gatekeepers' Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes As Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to'Follow the Money' i*n *Indiana Legal Studies Research Paper,* 408, 2019, 5.

To summarize, data in the blockchain is stored in interlinked and logically consequential blocks connected through hashes that create an append-only, and tamper-proof database.[30]

To help in visualizing this storage model, we could describe it as a series of non-modifiable and inextricably linked PDF files. Each of these PDFs contains a fixed amount of information – that must be consistent with the information contained in the preceding files – as well as a hash of the previous PDF. Any modification in the content of any file in the chain will alter all the subsequent files and will, hence, be displayed in the last file of the chain.

## 3.2 The storage of the ledger

Just describing how data is stored in the blocks is not enough to comprehend the structure of the blockchain record-keeping mechanism. What we are still missing is the distributed nature of blockchain.

Keep in mind, this section only delves into the static aspect of blockchain decentralization – i.e., how the information is stored, and integrity preserved. The dynamic element will be the object of the next section where we will analyse consensus protocols.

What makes blockchain decentralized is how its ledger – meaning the aforementioned chain of interlinked blocks – is stored. Rather than entrusting the ledger to a single party, as in the pre-existing system – the blockchain distributes control among all the participants of the network.[31] Each node of the network holds an identical copy of the blockchain and has full access to the data.

This model eliminates the traditional framework rooted in a central point of control: in the blockchain, all the nodes are in a condition of perfect information symmetry. The lack of a central repository enhances the cyber resilience of the system as it eliminates the central point of failure.[32]

[30] C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 74; A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 1.

[31] D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 668.

[32] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain space,* cit., 18.

As all the nodes are equally in control of the ledger, as long as one node of the blockchain remains online the network can still function. At the same time, this storage model means that, while the infrastructure is resilient to attacks that aim at disabling it, the information stored in the ledger is transparent. Eminently, anyone can become a node and get full access to the data stored in the ledger.[33]

## 4. The Consensus protocol

Having described the static element of blockchain's record-keeping model, it is now necessary to delve into its dynamic dimension to explain what is, arguably, the most ingenious and contentious innovation of blockchain: the establishment of consensus regarding the state of a shared ledger among non-reciprocally trusting parties.[34]

In his seminal paper, Bitcoin: A Peer-to-Peer Electronic Cash System,[35] Nakamoto identified the reliance on trusted third parties as the main setback of online commercial transactions. To solve this problem, he proposed an "*electronic payment system based on cryptographic proof instead of trust*".[36] This idea that the blockchain substituted the need for trust with computer code became one of the recurring themes in the (pro)crypto debate. So much so that the concept was rephrased as "in code we trust" [37], the (un)official motto of the crypto movement. But what is behind this motto, and how does the blockchain create shared trust? To answer this question, we need to analyse the dynamic element of blockchain record-keeping and understand how new information is added to the shared ledger.

[33] M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Federal Reserve Bank of Saint Louis, 2023, 1; H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, in *AMPLIFY,* 35/10, 2022, 2; H. Axelsen – J. Jensen – R. Omri, *When is a DAO Decentralized?*, cit., 53; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, cit., 32.

[34] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

[35] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* cit.

[36] M. Nofer, et al. *Blockchain* in *Business & Information Systems Engineering* ,59/3, 2017, 183.

[37] The motto rephrases the United States of America's motto "in god we trust" that is also engraved in the US dollar, the currency Bitcoin aims at substituting.

In traditional record-keeping mechanisms, as the ledger is centrally held by the intermediary which retains full control over the latter, it is up to this entity to decide when and how to update it. They are the only ones that can add, modify, or delete information. This system, hence, requires users to trust that the intermediary will behave with integrity and not maliciously modify the content of the ledger. One of the main goals of the blockchain is to eliminate such a need for trust bypassing this entity:[38] in the blockchain, there is no intermediary with full control of the ledger, as the latter is contemporarily stored by each node.[39] This also means there is no entity that has the power to unilaterally modify it. This, however, creates a problem. If in the traditional model, it is the intermediary that retains the authority to dictate the state of the ledger, in a shared environment no one has such unilateral power.[40]

So how is the ledger updated and who decides which information is valid?

This is done through a so-called consensus protocol. A consensus protocol can be understood as a digital version of a social contract:[41] as the parties of the network are non-reciprocally trusting, they draw a fundamental law laying down how new information is added, under which conditions, and by whom. This law aims to create a series of incentives and procedures that ensure the integrity of the ledger by guaranteeing that malicious actors cannot bend it to their advantage. This law is directly engraved into the source code of the blockchain and everyone entering the network acknowledges and (implicitly) accepts this as the fundamental law of the (digital) land.

[38] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain,* cit., 7; K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 7; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 27.

[39] M. Finck, *Blockchains and data protection in the European Union,* cit., 19.

[40] P. Bains, *Blockchain consensus mechanisms: A primer for supervisors*, International Monetary Fund, 2022, 5, "*in a centralized single-ledger system, a coordinating actor can make unilateral decisions and ensure a consistent ledger; this actor can read, write, and audit the system unilaterally. In decentralized systems, distributed nodes need to come to agreements, or a consensus, as there is no central authority to assume responsibility*".

[41] See, T. Hobbes, *The Leviathan*, London, 1651, 103 "*The final cause, end, or design of men (who naturally love liberty, and dominion over others) in the introduction of that restraint upon themselves, in which we see them live in Commonwealths, is the foresight of their own preservation, and of a more contented life thereby; that is to say, of getting themselves out from that miserable condition of war which is necessarily consequent, as hath been shown, to the natural passions of men when there is no visible power to keep them in awe, and tie them by fear of punishment to the performance of their covenants*"; J. Rousseau, *Du Contrat Social, ou principes du droit politique* in *Collection Complète des Oeuvres*, Geneva, 1789, 189, "*l'ordre social est un droit sacré, qui sert de base à tous les autres. Cependant ce droit ne vient point de la nature; il est donc fondé sur des convention*".

To sum up, the consensus protocol is the mechanism, expressed in computer code, that dictates how a blockchain network reaches an agreement regarding which new information can be validly added to the ledger and who has the power to do so.[42]

As it happens with fundamental laws there is no one size fits all. Different blockchains adopt different consensus protocols depending on the values and functions they favour.[43] This is not the place to delve into all the consensus protocols as this is a highly technical and continuously changing field. We will rather take as an example one consensus protocol to facilitate the reader's understanding of blockchain's dynamic functioning.

The protocol we will describe is Proof of Work (PoW). This is the primordial model, first designed, like many other pieces of blockchain technology, years before the introduction of blockchain. It is the consensus protocol adopted by Bitcoin and by most major blockchain networks.[44]

The PoW protocol introduces a mechanism to decide which of the participants of the network has, each time, the right to add the latest block of the chain. To do so it establishes a framework that requires participants – so-called miners – to compete[45] and establishes a reward – so-called blockreward[46] – for the one that wins this competition and is, hence, granted the right to add a new block.[47] Essentially, once a certain number of new transactions has been broadcasted to the network by users, miners compete for the right of adding the new block. First, a fixed number of transactions chosen by the miner from those awaiting confirmation are compiled to create a "candidate block". Then, miners devote computer resources to crack a mathematical puzzle that

[42] As defined by A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., glossary, "*Consensus rules: The block validation rules that full nodes follow to stay in consensus with other nodes*".
[43] For an overview of the main consensus protocols see P. Bains, *Blockchain consensus mechanisms: A primer for supervisors*, cit.; see also the discussion by The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 28 – 29.
[44] A. Porat – P. Avneesh – P. Shah – V. Adkar*, Blockchain Consensus : An analysis of Proof-of-Work and its applications*, 2017; R. Houben, Robby – A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion,* cit., 18. PoW was also the consensus protocol adopted, until recently, by Ethereum which has now shifted to a Proof of Stake (PoS) protocol.
[45] A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 1, 229; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 29.
[46] A. Trozze, et al., *Cryptocurrencies and future financial crime*, cit., 2, "*Miners are rewarded for their work—at the time of writing, the reward for finding a correct block is 6.25 Bitcoin. These 6.25 Bitcoin are created and enter circulation once the miner finds a block, through what is called a 'coinbase' transaction (until the maximum amount of Bitcoin, as specified in Nakamoto's paper—21 million—are minted). The reward is halved approximately every 4 years*".
[47] P. Bains, *Blockchain consensus mechanisms: A primer for supervisors*, cit., 9; A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 27; A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges,* cit., 1.

can only be solved through guessing – through a so-called brute force attack.[48] The computer that first guesses the right answer is granted the right to add the new block and is dispensed the attached reward[49] – in the case of Bitcoin a fixed amount of newly minted coins.[50] The winning miner broadcasts the new block with the solution to the mathematical puzzle to the whole network so that each node can add the new block to their ledger and verify the consistency of the newly added transactions to their previous record.[51]

The reasons why PoW is a safe and reliable mechanism are multiple and still debated.

A first computer science argument is that Proof of Work requires miners to devote large resources to create new blocks. This means that, to take control of the network, a miner would need to devote huge resources as it would need to control fifty-one percent of the computing power of the network –launching a so-called fifty-one percent attack.[52] Only in this way could a miner consistently control the outcome of the mining competition and modify at will the content of the blockchain. Further, to change past information, given the interlinked nature of the blocks, an attacker would need to redo the PoW for that block and each subsequent block making such an attack extremely costly.[53]

A second social engineering argument[54] is that miners, to be competitive, need to invest large resources. These investments are rewarded with a payment by the network and/or the users in the connected crypto-asset. This means that miners have skin in the game when it comes to the price and existence of that specific crypto-asset. If a miner cheats the system and breaks the consensus mechanism, they challenge the validity of the fundamental law of the network and, in so doing,

[48] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain*, cit., 8.

[49] A. Porat – P. Avneesh – P. Shah – V. Adkar*, Blockchain Consensus : An analysis of Proof-of-Work and its applications*, cit., 2; D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities*, cit., 4.

[50] C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 3.

[51] C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 90.

[52] A. Porat – P. Avneesh – P. Shah – V. Adkar*, Blockchain Consensus : An analysis of Proof-of-Work and its applications*, cit., 6; A. Trozze, et al., *Cryptocurrencies and future financial crime*, in *Crime Science,* cit., 3. This argument has been the object of numerous criticisms. The most known is certainly the one advanced by two researchers from Cornell that proved that through a process they labelled "selfish mining" to tamper the blockchain it is needed a share much lower than 51 percent, see E. Ittay – E. Gün Sirer, *Majority is not enough: Bitcoin mining is vulnerable* in *International conference on financial cryptography and data security*, cit.

[53] The cost of the attack augments the "older" is the block. Namely, changing a very old block requires huge computing power as it would imply that all subsequent blocks would need to be modified and their PoW redone. For this reason, it is conventionally stated that a block becomes unmodifiable after six confirmations, A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 28.

[54] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain* ,cit.

imperil the existence of the network itself. It is, thus, argued that it is more rational for a miner to act honestly than not.[55] This statement is reinforced by the structure of modern mining. As mentioned in the previous chapter, the growing competition in the market implies that this activity does not only require short-term investments – such as electricity – but also long-term ones – as hardware specifically designed for mining. These investments increase the cost of cheating, as the cost and time to divest are extended, nudging individuals towards compliance.[56]

Whatever the technical explanation, it is a fact that PoW has proven to be a very reliable system. As it has sustained the development of multi-billion endeavours as Bitcoin or Ethereum for more than a decade now. However, it also presents severe drawbacks. In particular, the competition among miners means that an action which, in a centralized database, is generally cheap in terms of time and cost – i.e., updating the ledger – becomes resource intensive due to the absence of a designated trust intermediary.[57]

These hindrances have pushed toward the invention of new consensus mechanisms and even new forms of blockchain that try to address the setbacks of PoW. One of these solutions will be addressed in section seven where we will delve into permissioned blockchains.

## 5. The transaction model. Asymmetric cryptography

Until now we have described how information in the blockchain is stored and added, it is now time to add the final piece to our brief overview of this technology and delve into the way transactions are executed among users.

To understand blockchain's transaction model it is first necessary to briefly introduce asymmetric cryptography, the technique underlying blockchain's accounts and privacy structure. Cryptography

[55] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain,* cit., 26.
[56] E. Budish, *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain,* cit., 29.
[57] As mentioned in the previous chapter Bitcoin mining currently consumes more energy than Sweden. For this and other information and statistics regarding Bitcoin's energy consumption see the Cambridge Bitcoin Electricity Consumption Index compiled by the University of Cambridge, https://ccaf.io/cbeci/index/comparisons

– from the Greek *kryptos*, meaning hidden – is the field that studies and develops solutions to guarantee the security of information.[58]

Now, how do you do that?

The easiest answer is through the encryption of the information that you wish to protect. Encrypting means transforming a text written in plain language into one whose meaning can only be understood by those who hold the decryption key.

An example may facilitate the understanding. One of the simplest encryption techniques is the Caesar cipher,[59] named after the famous Roman general and politician Julius Caesar. When Julius Caesar needed to send a message to his generals, to avoid that the interception of the messenger may compromise his plans, he would encrypt his texts through a substitution cipher. This means that he would replace each letter in the original text with a different letter placed at a fixed distance. For example, if the cipher uses a left shift of two, the A is replaced with the C, the B with the D, the C with the E, and so forth. With this cipher the word "hello" would become "jgnnq". While this is a very basic encryption technique, the main concept we need for our explanation is already there: to encrypt and decrypt a message the two communicating parties need to hold the same encryption key. Caesar and his generals needed to agree on the measure – one, two, three, … - and the direction – left, right – of the shift. Otherwise, they would have not been able to understand their respective messages. This creates a vulnerability: anyone who has access to the key can read the messages. Thus, the parties must find a way to securely store and communicate the key at the risk of seeing their efforts to maintain the secrecy of their communications nullified.[60]

With the introduction of digital communications, as an increasing chunk of information flows shifted online, the need for encryption has multiplied.[61] This growth, paired with the commonplace nature of long-distance communications in digital environments, has magnified the relevance of the abovementioned vulnerability. Eminently, the classic means to safely communicate the decryption key is for the parties to physically meet. If the parties were to use any other non-encrypted long-distance means of communication to share the key, the risk is to be intercepted,

[58] Or as defined by D. Luciano – G. Prichett, *Cryptology: From Caesar ciphers to public-key cryptosystems* in *The College Mathematics Journal,* 18/1, 1987, 2, cryptography "*is the art and science of making communications unintelligible to all except the intended recipients*".

[59] See D. Luciano – G. Prichett, *Cryptology: From Caesar ciphers to public-key cryptosystems,* cit., 2.

[60] N. Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 1996.

[61] D. Luciano – G. Prichett, *Cryptology: From Caesar ciphers to public-key cryptosystems,* cit., 1.

this way compromising the safety of all future communications. In a world where non-physical communication is the norm, the need to physically meet to exchange the key was a crucial drawback.[62] This led to extensive research aimed at developing a solution that would eliminate the need for the communicating parties to share a common key.

The result of this effort is asymmetric cryptography. Asymmetric cryptography allows two parties to securely communicate without having to share a common encryption key.[63]

Let's see how this works.

In asymmetric cryptography, each party has two connected keys: a public key and a private key. The public key can be freely shared publicly, while the private key must remain secret to guarantee the safety of communications. Asymmetric cryptography breaks into two the traditional key, one – the public key – can be used only for the encryption of the message, and one – the private key – only for its decryption. The two keys are linked as the public key is computed from the private key through a process that cannot be reversed, i.e. hashing – meaning that, knowing the private key, the public key can be easily computed, but, knowing the public key, it is (virtually) impossible to reverse compute the private key.[64] This makes secure communications easier as all I need to know to send an encrypted message is the public key of my addressee, which they can securely share. If I want to send an encrypted message, I will ask my addressee to share with me their public key. I will use that public key to encrypt the message and then send it to them. Once received, the addressee will use their private key to decrypt the message without either of us needing to know the other's private key.[65]

[62] P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 19, "*electronic communication from the telegraph to the internet introduced a new problem for cryptographers: Is it possible to share encryption keys without ever meeting in person?*".

[63] P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 20; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

[64] A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 56; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

[65] N. Szabo, *Smart Contracts: Building Blocks for Digital Markets*, cit., "*Alice generates two keys, called the private and public keys. She keeps the private key secret and well protected, and publishes the public key. When Bob wishes to send a message to Alice, he encrypts a message with her public key, sends the encrypted message, and she decrypts the message with her private key. The private key provides a "trapdoor" that allows Alice to compute an easy inverse of the encryption function that used the public key. The public key provides no clue as to what the private key is, even though they are mathematically related*"; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

While the primordial function of asymmetric cryptography is secure communications, this technique can also be used for a second purpose: to guarantee the source of a certain message – i.e., as a digital signature.[66] Namely, given the relation existing between private and public keys, the private key can be used to generate a signature – different each time – which can be then validated by any third party through the public key. This way an individual can use his private key to sign a document/transaction, they will then share their public key with any other interested parties who will be able to verify that the signature was executed through the private key associated with that specific public key and, thus, by the individual holding it.

This system has been implemented in blockchain ecosystems to guarantee the integrity of the transactions while maintaining full decentralization. Let's see how.

In blockchain ecosystems, anyone can create an account by simply generating a private key and from that computing the public key.[67] This eliminates the need for an intermediary providing for an address/account. The private key can be computed by anyone through different methods – including flipping a coin 256 times.[68] If the user, then, wants to send all or a share of their crypto-assets all they need to know is their addressee's address (which is computed hashing their public key) and the addressor's private key. They will, then, generate a transaction – meaning a string of data – stating the amount they wish to send, their addressee's address, and their digital signature – generated through their private key.[69] They will, subsequently, broadcast the transaction to the network, where miners will compile it into a block and, after having verified its consistency with the previous blocks – meaning the addresser has the amount they want to transfer, the signature is valid, and the public key of the addressee is valid – add it to the chain.[70]

[66] N. Szabo, *Smart Contracts: Building Blocks for Digital Markets,* cit.

[67] For a series of examples of how Bitcoin transactions work see A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 9 - 11; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

[68] For a detailed explanation on how to create a private key see A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 58; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

[69] Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit., 40; R. Houben, – A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, 2018, 17; European Banking Authority, *Report on Crypto-assets,* cit., 8; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26; M. Finck, *Blockchains and data protection in the European Union,* cit., 19.

[70] Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit., 41 – 43; European Banking Authority*, Report with Advice for the European Commission on Crypto-assets*, Paris, 2019, 8; C. Pelker

## 6. Privacy within the blockchain. Pseudonymity or anonymity?

Simply reading the preceding sections you may have the feeling that blockchain is a very transparent form of value exchange. Each transaction bears the identifier of the addresser – their digital signature – and the addressee – their crypto-asset address. All the transactions are stored in a consequential manner so that the money trail is immediately apparent. The ledger is public; hence, anyone can download it and check how much money a certain address has, to whom they have sent it, and from whom they have received it.[71]

Going back to our previous chapter, this begs the question, weren't cryptocurrencies envisioned as a system to guarantee individual privacy?

Yes, they are, and to understand how we need to focus on blockchain's key characteristic: disintermediation.[72] Blockchain's disintermediation of control means that there is no entry or exit checkpoint. Anyone can create as many blockchain accounts as they wish without ever needing to identify themselves.[73] Just toss a coin 256 times and you will have a functioning Bitcoin private key; from that private key, you can compute the public key and crypto-assets address and start using your account.

The address will guarantee it is you – meaning the person that has access to the related private key – who is acting but it will not say anything regarding your identity. An address is simply an alphanumeric string that bears no information regarding the person that controls it.[74] Due to this

Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 60; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26.

[71] C. Leuprecht - C. Jenkins – R. Hamilton, *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*, cit., 4; T. Frick, *Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland*, in *Era Forum*, 20/1, 2019, 100; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, cit., 32.

[72] A. Blandin, et al., *Global cryptoasset regulatory landscape study,* cit., 26.

[73] A. Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain*, cit., 11; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26.

[74] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* Paris, 2019, 27, "*the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual.*

privacy structure, cryptocurrencies are usually branded as pseudonymous:[75] everyone can see what a certain address is doing but no one knows who is hiding behind it.[76]

At the same time, the blockchain's privacy structure means that, if an address is deanonymized, the whole transaction history of the individual becomes accessible to anyone.[77]

As stated by UCL professor and blockchain forensic expert Sarah Meiklejohn:

> *"If you catch a dealer with drugs and cash on the street, you've caught them committing one crime but if you catch people using something like Silk Road, you've uncovered their whole criminal history (...) it's like discovering their books".*[78]

This is since, contrarily to traditional record-keeping systems, blockchain is logically centralized. All the information is stored in a single ledger which means that rebuilding the transaction trail is extremely easy once an address is deanonymized.

At the same time, the decentralized nature of blockchain adds an additional layer of privacy. As anyone can create, without any cost and without having to identify, as many accounts as they wish, a user could, theoretically, employ a different address for each transaction.[79] This severely diminishes the usefulness of deanonymizing a public key as it only links the person to a single transaction.[80]

*The wallet address contains a user code that serves as a digital signature in the distributed ledger (i.e., a private key) in the form of a unique string of numbers and letters. However, additional information will be necessary to associate the address to a real or natural person*".

[75] A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 5; C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 3.

[76] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance*, in *Crime, Law and Social Change*, 69, 2018, 286 – 287.

[77] M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 1, "*If someone obtains information that allows them to link a blockchain address to an entity, they may effectively observe that entity's entire transaction history and associated activity*"; M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, in *Proceedings of the 51st Hawaii International Conference on System Sciences,* 2018, 3499.

[78] J. Bohannon, *The bitcoin bust* in *Science*, 351, 2016, 1144; on this point see also A. Trozze, et al., *Cryptocurrencies and future financial crime*, in *Crime Science,* 11, 2022, 2.

[79] M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., 3499; C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 3.

[80] We will further explore how blockchain addresses can be linked and their activity analysed in chapter 4 section 6 on blockchain analytics.

It is relevant to underline the paradox of this privacy structure. If the user does not access the market in a decentralized fashion but through an intermediary that they then use to manage their finances – as it currently happens in most cases – blockchain is much less private than the traditional forms of financial transaction. Namely, if the pseudonymity guaranteed by decentralization is bypassed, the blockchain ledger is more complete and intelligible compared with the private and fragmented ledgers of financial institutions.[81]

To conclude, blockchain's privacy structure is fundamentally rooted in its decentralization which allows users to create as many accounts as they wish without having to provide any information that can be used to identify them.[82] At the same time, blockchain's transparency means that if deanonymization does happen the transaction trail is more accessible and complete compared to the traditional system.

## 7. A key distinction: permissioned and permissionless blockchains

What we have described up to this point is the primordial model of blockchain. However, since 2008, not only have blockchain's possible use-cases multiplied, but the technology itself has morphed and forked.

As states and corporations have started exploring possible use-cases, the technology they envisioned became substantially different compared to the original model.[83] Such blockchain loses some elements of decentralization, especially in terms of governance and transparency, to guarantee greater control and privacy.[84] Indeed, most corporate and state-led pilots employ private,

[81] M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 298, "*The paradox of blockchain technology is therefore that while AML efforts must deal with imperfect knowledge of identities, they may exploit perfect knowledge of all transactions*"; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 91.

[82] C. Akcora et al., *How to not get caught when you launder money on blockchain?*, arXiv preprint arXiv:2010.15082, 2020, 1.

[83] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 36.

[84] P. De Filippi - A. Wright, *Blockchain and the law. The rule of code*, cit., 31; Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 7.

permissioned blockchains[85] contrary to the public, permissionless one typical of Bitcoin and most cryptocurrencies.[86]

This second type of blockchain has seen a marked development in the last years as a tempered form of blockchain. Indeed, contrary to the fully decentralized blockchain of Bitcoin, which grants no central control in terms of access or governance, permissioned, private blockchains ensure a customizable level of centralization.[87] These allow the establishment of a centre of governance that can decide – depending on the design – who can join the network, who can read and write in the blockchain, etc.[88] The, at least partial, recentralization of control makes these types of systems more appealing to public actors. A certain level of centralization is fundamental to permit the implementation of blockchain as a means to pursue public or semi-public functions.[89]

This is for two main reasons.

First, excessive transparency of the information stored in the blockchain could be considered a liability for companies and public players in terms of governance and privacy. Eminently, while decentralization guarantees prompt sharing of robust information, this does not mean that information bearers are open to completely losing control of their information.[90] Furthermore, a certain level of privacy and control over data is required by imperative privacy regulations. Private and public entities not only wish but must maintain a certain level of control over the information

[85] The term private and permissioned are sometimes used together, as in the present section, to jointly identify a network that has a mechanism of centralized governance. Other times, they are used separately to identify different characteristics of this governance structure. When used separately, a permissioned network identifies one where only authorized actors can validate and add new information and a private network is one where only certain user can access the information in the ledger, see P. Bains, *Blockchain consensus mechanisms: A primer for supervisors,* cit., 4; R. Houben, Robby – A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, cit., 15.

[86] A. D'amelio – G. Soana, *Blockchain technology to prevent tax frauds and money laundering in the European Customs Union: quo vadis?,* in *Dirittto e Pratica Tributaria Internazionale*, 2021, 1035; P. Jayachandran, The difference between public and private blockchain, in Blockchain Pulse: IBM Blockchain Blog, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[87] S. Hughes, '*Gatekeepers' Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes As Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to'Follow the Money',* cit., 6.

[88] R. Auer *Embedded Supervision: How to build regulation in decentralized finance*, cit., 4; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 37.

[89] A. D'amelio – G. Soana, *Blockchain technology to prevent tax frauds and money laundering,* cit., 1036.

[90] R. Campbell et al., *Distributed Ledger Technologies in the Public Sector: Learnings on the application of Distributed Ledger Technologies across international public services and their role in realising Scotland's full potential in a digital world*, The Scottish Government, 2018, 22; C. Mohan, *State of public and private blockchains: Myths and reality*, in *Proceedings of the 2019 International Conference on Management of Data*, 2019, 1.

they share. This entails that the sharing of sensitive data has to always occur among trusted parties that guarantee compliance with relevant regulations and avoid unwanted publicity. Private, permissioned blockchains, by only granting access to authorized actors and allowing to customize such access, guarantee this control.

Second, a certain oversight over the governance of these systems is necessary and, in many cases, legally mandated.[91] The fully decentralized governance that characterizes crypto-assets collides with the centralization underlying our political and economic institutions.

Hence, to foster the implementation of blockchain by these players, it is crucial to ensure a certain level of centralized governance. Private, permissioned blockchains permit this control by enabling the governing body to decide who can become a node and who can gain access to the blockchain in terms of reading and writing.[92]

This partial recentralization of governance also impacts blockchain's efficiency. Due to the pre-existing (relative) trust among the participants in a permissioned network – as all participants are identified – the consensus protocol is collaborative rather than competitive, making the update of the ledger less energy intensive and more efficient. The consensus protocol employed by private blockchain is, most of the time, Proof of Authority (PoA). PoA resembles closely the traditional update system, as it identifies certain nodes that have the authority to unilaterally update the ledger. This protocol eliminates the energy-intensive competition among miners typical of Proof of Work but also erodes the trustless and decentralized nature of blockchain as centralized authorities are re-established.

The centralized control permitted by permissioned blockchain underlines a genetic change in this field. The main innovation purported by Satoshi Nakamoto in his seminal paper was the introduction of a reliable system of payment among non-reciprocally trusting parties. When it comes to private, permissioned blockchains the logic changes. Here, nodes are only known players

[91] See the example of custom management in A. D'amelio – G. Soana, *Blockchain technology to prevent tax frauds and money laundering in the European Customs Union: quo vadis?,* cit.; C. Kuner – F. Cate – O. Lynskey – C. Millard – N. Ni Loideain – D. Svantesson, *Blockchain versus data protection* in *International Data Privacy Law*, 2, 2018, 103, on the need to introduce permissioned blockchain to ensure compliance with the data protection regulatory framework.

[92] C. Mohan, *State of public and private blockchains: Myths and reality*, cit., 2; K. Werbach, *The blockchain and the new architecture of trus*t, cit., 107.

that have been admitted to the network. There is, thus, a certain level of trust among them and the governance body. Blockchain's decentralization plays a different role in these networks compared with the permissionless networks. The customizable decentralization of control and access to the information augments trust among already trusting parties while ameliorating the quality and timeliness of data shared. At the same time, it provides a manageable level of automation as well as the establishment of common rules which application is overviewed by each party.[93]

From a financial integrity perspective, this system is of great interest. Namely, in terms of monitoring, permissioned blockchains represent the best of both worlds.[94] As the pre-existing record-keeping system, they have a centralized governance structure. Thus, providing the regulator with a central point of pressure to police and on which to impose financial integrity obligations. As in the blockchain record-keeping system, information is logically centralized, meaning every interaction among the participants of the network is recorded in a single ledger. In these networks, the main question is, hence, how much control is desirable and not how much control is possible, given that the underlying architecture would allow for (virtually) perfect control.

## 8. Smart contracts

Now that we have completed the description of blockchain's basic functioning, we need to add an additional layer to our analysis and examine how the blockchain impacts the execution of computer programs.

[93] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 37, lists three main advantages of permissioned blockchains compared to legacy systems: Immutability, peer-to-peer exchanges, and digital signatures.

[94] On the suitability of private blockchains for compliance purposes see A. Minto, *The legal characterization of crypto-exchange platforms*, in *Global Jurist,* 22/1, 2021, 142 – 143.

To do so, we must introduce the concept of smart contracts. This idea was first introduced by Nick Szabo – a computer scientist who would then move on to become one of the core members of the early Bitcoin community – in a paper he published in 1994.[95]

In this text, he described smart contracts as:

> *"a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries"*.[96]

A textbook example of smart contract is the vending machine.[97] If I want to buy a soda at a vending machine, I tap the number on the keypad, the machine tells me the price, I introduce the money and the machine dispenses me with the drink. This is a sale contract that is concluded and executed in a completely automatized and computerized fashion without the need for any human intervention.

The vending machine is a simplified example of a concept – the computerized conclusion, execution, and enforcement of contractual terms – that can be applied in nearly all fields. The rationale for the development of such contracts is to eliminate the human factor, in the execution and enforcement of legal obligations; through the substitution of sloppy, emotional humans with cold, predictable machines the proponents hoped would *"lower fraud loss, arbitration and enforcement costs, and other transaction cost*".[98]

Until blockchain was introduced, the main setback of smart contracts was that there was still the need to trust a human third party. Any computer software needs to be run on something and by someone. This reintroduces the human factor in the equation and lowers the appeal of smart

[95] N. Szabo, *Smart Contracts*, 1994. M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 3.

[96] N. Szabo, *Smart Contracts*, cit.; see also the definition of A. Porat – P. Avneesh – P. Shah – V. Adkar, *Blockchain Consensus : An analysis of Proof-of-Work and its applications*, cit., 4, "*A smart contract is a computer program stored on the decentralized blockchain network that executes the terms defined inside of it. The contract only runs when it is invoked to do so by an external event or if some predefined condition is met*", and that provided by H. Axelsen – J. Jensen – R. Omri, *When is a DAO Decentralized?*, cit., 53, "*Smart contracts are scripts that automatically carry out specific business logic*"

[97] This example can be found in N. Szabo, *Smart Contracts: Building Blocks for Digital Markets*, cit.

[98] N. Szabo, *Smart Contracts*, cit.; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 2.

contracts. Blockchain promises to solve this problem through decentralized execution and trustless trust. Namely, in the same way as Bitcoin transactions are confirmed without anyone being able to unilaterally stop the process, smart contracts can be executed without anyone really being in command.[99] Blockchain enables developers to compute a smart contract that, once launched, only obeys to the laws engrained in its code.[100]

The main push for the development of these smart contracts came from the introduction of Ethereum in 2014.[101] With Ethereum, anyone can compute a smart contract and execute it in a fully decentralized way.[102] This means that any algorithm – whether it bears the terms of a contract, the source code of a videogame or a regulation – can be executed in a decentralized and, thus, fully automatized fashion. Smart contracts comprise, hence, a much wider category than just contracts: they can be described as rules written in computer language and executed by a network of decentralized computers – meaning without anyone retaining unilateral control over their execution.[103]

[99] H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 2, "*The key difference from a regular agreement is that the blockchain itself executes the code automatically. This, in turn, means that once a smart contract is deployed, no human engagement is required to complete the transactions or other business logic denoted by the contract code (…) This means that once deployed; the smart contract will execute for as long as the version of the blockchain exists; it cannot be turned off*", K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 14.

[100] M. Finck, *Blockchain regulation and governance in Europe*, Cambridge University Press, 2018, 67-68; A. Trozze, et al., *Cryptocurrencies and future financial crime*, in *Crime Science,* cit., 3, "*computer programmes that automatically execute contracts, in the form of if-else statements (e.g., if a product is received, then release the funds. The smart contract code is publicly visible on the blockchain and immutable. Smart contracts allow parties to enter contracts without needing to trust one another, or a third party, for execution. Rather, the parties can be confident that the contract will be carried out as agreed, so long as they trust its code*"; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 7.

[101] M. Nofer, et al. *Blockchain,* cit., 185; D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 669.

[102] M. Zou, *Code, and other laws of blockchain*, cit., 659, "*Blockchain-based smart contracts not only memorialise the details (all or parts) of an agreement between contracting parties in code, but also automate the execution and enforcement of its terms on the distributed ledger, without an intermediary*"; H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 3.

[103] Many scholars have reflected on the impact blockchain based legal norms may have on the society and the law, see M. Finck, *Blockchain regulation and governance in Europe*, cit.; P. De Filippi – A. Wright, *Blockchain and law. The rule of code,* cit.

Smart contracts are purported to reduce the need for trust and intermediaries – such as lawyers, courts, notaries, etc.[104] – when it comes to (commercial) relations.[105] From insurance contracts to complex organizations, blockchain enthusiasts assure that computers can replace humans by guarantying exact and timely execution.

There are, however, three main obstacles on the road toward complete automation.

First, the need to translate the wet code into dry code. In computer science lingo, the wet code identifies human-readable language, and dry code the machine-readable one.[106] Computers need certainties, humans need nuances, especially when it comes to the regulation of their behaviour.[107] Contracts are filled with terms like good faith, best effort, etc. which are nearly impossible to translate into a machine-readable language. This creates a problem when it comes to translating complex legal documents – as the articles of incorporation of a company – into computer code. If simplification is always possible, certain nuances are necessary when it comes to establishing a long-term relationship among humans.

Second, a smart contract may still need information from the outside world to correctly execute. An example will facilitate the understanding. Let's imagine an insurance contract aimed at protecting a farmer from the risk of drought.[108] The smart contract is written in the following way: if in 2022 it rains more than X, do not pay, if in 2022 it rains less than X, pay 50 ether[109] to the farmer. The contract is entrusted with a fund of 50 ether that it solely controls, so that, if option B happens, it can self-execute. Now the problem is, how does the contract know how much it rained? The contract will need a so-called oracle – meaning a source that feeds it with the requested

[104] As stated by N. Szabo, *Smart Contracts: Building Blocks for Digital Markets*, cit., "*Legal barriers are the most severe cost of doing business across many jurisdictions. Smart contracts can cut through this Gordian knot of jurisdictions. Where smart contracts can increase privity, they can decrease vulnerability to capricious jurisdictions. Where smart contracts can increase observability or verifiability, they can decrease dependence on these obscure local legal codes and enforcement traditions*".

[105] P. De Filippi – A. Wright, *Blockchain and law. The rule of code,* cit., 75.

[106] K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 8, argue this translation process actually recreates the trust dilemma as the user needs to trust the coder to correctly and faithfully translate their wills.

[107] M. Finck, *Blockchain regulation and governance in Europe*, cit., 81.

[108] Insurance is seen as one of the fields where smart contracts and blockchain are more promising, see European Insurance and Occupational Pensions Authority, *Discussion paper on blockchain and smart contracts in insurance,* Luxembourg, 2021.

[109] The ether is the native cryptocurrency of Ethereum, which is the most common platform when it comes to computing smart contracts, see https://ethereum.org/en/smart-contracts/.

information.[110] The oracle may be a sensor placed in the farmer's land measuring rain or a weather website. Whatever that may be, the oracle reintroduces a degree of centralization in the contract. Eminently, it allows the parties to manipulate it, give rise to dispute, and block the execution of the contract.

Third, machines are blind. Launching a self-executing, virtually unstoppable machine can be extremely dangerous as it will not be able to discern the nuances that are intrinsic to any human activity. The DAO hack, detailed in the previous chapter,[111] is a good example of this problem. The hacker that attacked the DAO formally did nothing wrong, it simply executed a command that was provided by the smart contract. The reason why the hacker's actions were wrong entailed their intentions, which cannot be assessed by a smart contract that acts based on the binomial valid/invalid. The smart contract "voluntarily" paid the hacker and there was nothing that anyone could do to stop it. The only available solution was to recentralize the network and reverse the transactions, which is what the community eventually did. This, however, reintroduced precisely the arbitrariness factor in contractual relations that they aimed at eliminating through smart contract-based commercial relations.

[110] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 21, "*oracles- who import exogenous data flows into blockchains (it should be reminded that blockchains cannot access external databases). These oracles can be conventionally centralised entities, but they also can be decentralised applications, both from a governance perspective and in the way they collect information: volunteers are called upon to send data; the oracle synthesises the information provided into an average (that is usually weighted); the information providers are then remunerated according to how close they are to this average, which is deemed correct*".

[111] See chapter 1 section 3.2.

# Chapter Three

## Tracing the Regulatory Corral

## An analysis of the object and subjects of the regulation: the definition of crypto-asset and crypto-asset service providers

### 1. A brief introduction to the financial flows control strategy

To understand the logic underlying the anti-money laundering regulation, it is first essential to grasp a historical shift occurred in the second half of the past century. One that has profoundly modified the structure of financial transactions: the progressive digitalization of the financial system. Namely, the digitalization of finance constitutes one of the architectural foundations of the anti-money laundering strategy. If, as detailed in chapter one, the introduction of Electronic Fund Transfer Systems (EFTS) sent chills down the spine of cypherpunks' and crypto libertarians, it was, at the same time, a mouth-watering innovation for the criminal justice system.

The shift from cash to digital currencies[1] meant that the system moved from being token-based to account-based. This is a momentous shift in terms of financial monitoring. The fundamental difference between the two systems is the following.[2]

[1] The term digital currency is hereby used to identify the use of so-called commercial bank money, meaning the use of electronic fund transfer systems rooted in an intermediary (credit cards, debit cards, wire transfers, etc.) that holds the account and provides for the fund transfer system.

[2] For a brief discussion regarding the difference between these two systems see, C. Kahn – W. Roberds, *Why pay? An introduction to payments economics*, in *Journal of Financial Intermediation,* 18/1, 2009, 6 - 9.

In token-based systems, the value is directly incorporated in the object exchanged. This incorporation of the value can be dictated by the market – due to its scarcity, as is the case with gold – or by order of the authority – as with *fiat* currencies.[3] In a token-based system, when receiving a payment, the beneficiary only needs to check the validity of the token and has no interest in identifying their counterparty. This is because the value is received by the beneficiary through the simple act of entering in the possession of a valid – meaning non-counterfeited – token. In this sense, token-based systems are peer-to-peer. Eminently, the exchange of value is carried out directly between the two parties without the need for any third-party intervention.[4]

In account-based systems, in contrast, the exchange of value is carried out through the reallocation of a claim the payer has with a third party – a bank, a credit card company, etc. – to the payee. In these systems, thus, the beneficiary needs to identify its counterparty to correctly execute the transaction. This for two reasons. First, as they need to check that the payer's claim towards the third party is sufficient to honour the payment they intend to perform. Second, as they need to communicate to the debtor the shift in the titularity of the claim so that the former can update its ledger.[5] An account-based system is, hence, not peer-to-peer. To carry out a payment, a third party has to be included. One that certifies the payer has the funds they intend to transfer and reallocates such funds to the payee.

As clearly stated by Charles Kahn:[6]

[3] State currencies are commonly known as *fiat*. The term *fiat* comes from Latin, and it can be translated as "it shall be" signifying its relation with the order of the authority, see I. Asmundson – C. Oner, *What is money?*, in *Finance & Development,* 49/3, 2012, https://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm

[4] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 43, defines a peer-to-peer system as *"An exchange model where each entity in the network is both client and server, as opposed to the client-server model. The terms "peer", "node" and "user" are generally used to designate the entities making up such a system. A peer-to-peer system can be partially centralized (part of the exchange goes through a central intermediary server) or fully decentralised (connections are made between participants without any particular infrastructure)"*; this privacy features of cash has made it one of the preferred means to launder illicit proceeds see the analysis of E.W. Kruisbergen - E.R. Leukfeldt - E.R. Kleemans - R.A. Roks, *Money talks money laundering choices of organized crime offenders in a digital age,* cit., 576.

[5] F. Tronnier - D. Harborth - P. Hamm, *Investigating privacy concerns and trust in the digital Euro in Germany*, cit., 1, "*All new and digital currencies or payment methods create and leave electronic records, which could be tracked and monitored to counteract money laundering or other illegal activities*"

[6] C. Kahn, *Tokens vs. Accounts: Why the Distinction Still Matters,* Federal Reserve Bank of Saint Louis, 5 October 2020, https://www.stlouisfed.org/on-the-economy/2020/october/tokens-accounts-why-distinction-matters,

> "*When you pay with an account, the crucial question for the recipient is your identity: "Are you really the account holder?". When you pay with a token, your identity is irrelevant; instead, the crucial question for the recipient is: "Is this object I'm receiving real or counterfeit?*".

This difference between token and account is crucial when it comes to the digitalization of financial transactions.

The traditional analogic means of payment is cash. Cash is a token-based system as its value is – at least in its modern form[7] – incorporated in the object by order of the authority. To ensure they have correctly acquired the value, the payee only needs to check the authenticity of the banknote/coin. In contrast, in the digital arena no such token exists. To pay online, it is always necessary to use an intermediary[8] – a credit card company, a digital money provider, a bank, etc. – that keeps the balance and transfers the value among individuals. This structural difference means that the progressive digitalization of financial transactions caused a shift from a token-based system to an account-based one.

It is within the historical framework of this changing architecture of financial transactions, that the anti-money laundering regulation was first conceived and implemented. The policymaker intercepted this modification and adopted a synergic strategy aimed at maximizing the monitoring ability.

This strategy is constituted by two main threads.

First, the regulation of an increasing number of intermediaries.

[7] For the shift from gold backed money to fiat currency see I. Asmundson – C. Oner, *What is money?*, cit., "*Until relatively recently, gold and silver were the main currency people used. Gold and silver are heavy, though, and over time, instead of carrying the actual metal around and exchanging it for goods, people found it more convenient to deposit precious metals at banks and buy and sell using a note that claimed ownership of the gold or silver deposits. Anyone who wanted to could go to the bank and get the precious metal that backs the note. Eventually, the paper claim on the precious metal was delinked from the metal. When that link was broken, fiat money was born. Fiat money is materially worthless, but has value simply because a nation collectively agrees to ascribe a value to it*". This shift from a gold backed to a State backed currency is one of the recurring themes of the pro-crypto discourse, as it is perceived as a violation of individual freedom. With gold, it is argued, everyone held a value independently, with fiat currency, contrarily, the individual is subordinate to the whims of the Leviathan. For this reason many crypto project try to re-establish this connection between money and a "real" value as gold, or non-volatile stocks so to free the individual from the choices of the Central Bank – see as an example Tether Gold a cryptocurrency that is claimed to be fully backed by gold, https://gold.tether.to/.

[8] N. Bilotta, *CBDCs and Stablecoins: The Scramble for (Controllable) Anonymity* in N. Bilotta - F. Botti (eds.) *The (Near) Future of Central Bank Digital Currencies*, Peter Lang International Academic Publisher, 2021, 168.

The structure of digital transactions means the market is rooted in a series of information bottlenecks. As digital transactions are necessarily intermediated, digital exchanges of value are overwhelmingly processed by a handful of intermediaries. These intermediaries act as filters of all the exchanges of value carried out in cyberspace.[9] This role of filter means that intermediaries have privileged access to a massive amount of data concerning the financial transactions performed and received by all of their customers. The anti-money laundering legislation exploits this privileged position through the regulation of the companies/individuals holding them. Intermediaries have become the object of increasingly fine-grained monitoring duties with respect to their clients. Within this system, private players are, hence, entrusted with a crime control function: they need to guarantee – up to a reasonable degree – that their customers do not use their services to commit crimes or move and/or enjoy illicitly-sourced funds. The regulator, thus, establishes a system of decentralized policing partially shifting the burden, and the cost, of the, typically public, crime control function onto private actors.

Second, the limitation in the use of cash.

The financial integrity regulation introduces increasingly stringent requirements to limit the possibility for an individual to hold and pay in cash. This regulatory strand is functional to enhancing the effectiveness of the first strand. Namely, it aims at increasing the number of transactions that pass by the intermediated system and are, thus, traceable under the anti-money laundering regulation.

To sum up, the anti-money laundering regulation is introduced concurrently with a historical shift in the architecture of financial transactions that opened new opportunities for the policymaker: the progressive digitalization of the financial market and the corresponding shift from a token-based to an account-based transaction system. The policymaker intercepts this transformation by introducing a regulation rooted in two synergic strands: the limitation in the use of cash and the imposition on intermediaries of a duty to monitor and report their customers.

[9] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023*, 2023, 3.

## 2. Understanding the crypto risk. Governance and access disintermediation

Now that we have introduced the fundamental strategy underlying the anti-money laundering regulation, we can easily understand why blockchain represents a thorn in the side of this policy field.

As explained in chapter one, the crypto-assets movement constitutes a reaction precisely to the abovementioned shift from tokens to accounts in the architecture of monetary transactions. Alarmed by the progressive substitution of cash with digital transactions, and the corresponding social monitoring potential, a group of technologists worked on a digital means of exchange that could avoid this mandatory surveillance with a view to protecting individual privacy.[10]

To achieve this goal, the blockchain is designed to circumvent the main strategy underlying the anti-money laundering legislation: the progressive regulation of intermediaries, the information bottlenecks that, in an account-based system, are the necessary checkpoints of the financial flows infrastructure.[11]

The blockchain, to this end, enables peer-to-peer transactions in the digital realm.[12] This way it circumvents the necessity for the individual to use an intermediary and undermines the logic

[10] P. Armer, *Computer Technology and surveillance,* University of Stanford - Center for Advanced Study in the Behavioral Sciences, 1975, 11 – 12, "*The point here is that it's not enough just to have the option of using cash, the cash option must be used frequently or it becomes useless as a means for privacy (…) an EFTS (Electronic funds transfer system) system (…) was the best surveillance system we could imagine within the constraint that it not be obtrusive*"; D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities*, cit., 1. This is not to mean that promoting individual privacy is the only goal pursued by blockchain's creator. Other key goals include circumventing the need to break the monopoly of Central Banks in the issuance and management of the currency and to trust financial intermediaries. However, given the scope of the present dissertation the financial monitoring goal constitutes the most relevant one.

[11] M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 286; C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 3, "*in the context of traditional,* "*real" currencies, this concept is effective because a person can only participate in the deposit money system with a bank account (and huge amounts of cash are hard to store and transport, especially across borders). In contrast to that, in the Bitcoin system users can create their own "account" (= the wallet) on their own de- vice and create as many key pairs as they want without involving any financial service provider*".

[12] R. Houben, Robby – A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, cit., 17, "*blockchain is all about decentralizing trust and enabling decentralized authentication of transactions. Simply put, it allows to cut out the "middleman*".

behind the financial monitoring regulation.[13] While such a result is momentous and profoundly dents the effectiveness of anti-money laundering controls,[14] it does not constitute a complete return to cash. This is because the mentioned achievement is not obtained through the reinstatement of a token-based transaction system but by tweaking the pre-existing account-based system.

Notwithstanding many associate blockchain with terms such as "tokenization" or "token economy", from an anti-money laundering standpoint blockchain is still an account-based system. In the blockchain, exchanges of value happen through the insertion of a new entry in the common ledger determining the transfer of value from A to B.[15] There is no such thing as a standalone token exchanged between participants only based on its intrinsic value. Counterparty identification is, thus, still a crucial element of crypto transactions. The main difference with traditional electronic value exchange systems is that the financial ledger is not owned and updated by a centralized authority but by a decentralized network of nodes.

This notation is a relevant one as blockchain's privacy structure inherits some elements of account-based systems in terms of traceability. Understanding this privacy structure with respect to the current money-laundering regulation is crucial as it constitutes the premise of any analysis to be carried out in this field.

Let's then start with what makes blockchain more private compared to the previous system and then pass to what makes it more transparent.

[13] G. Soana, *Regulating cryptocurrency checkpoints. Fighting a trench war with cavalry?,* in *Economic Notes,* 2021, 2; Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, Washington, 2013, 34; D. Brown, *Cryptocurrency and Criminality: The Bitcoin Opportunity* in *The Police Journal: Theory, Practice and Principles*, 2016, 328; K Kolachala et al., *SoK: Money Laundering in Cryptocurrencies*, in *The 16th International Conference on Availability, Reliability and Security*, 2021, 1; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* Paris, 2021, 18, "*P2P transactions are not explicitly subject to AML/CFT controls under the FATF Standards. This is because the Standards generally place obligations on intermediaries, rather than on individuals themselves*"; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 286.

[14] C. Accorsi – R. Brening – G. Müller, *Economic analysis of cryptocurrency backed money laundering* in *Twenty-Third European Conference on Information Systems (ECIS)*, 2015, 4

[15] For an in-depth analysis of blockchain's functioning and its transaction system's structure see chapter two, section five.

As analysed in chapter two, the main privacy feature of blockchain is connected to the decentralization of its governance and the pseudonymity of its accounts.[16]

To access the market in the traditional system each customer needs to use an intermediary that holds their account and records their transactions. In contrast, with blockchain anyone can create a private key and from it compute a public key and an address.[17] Through this key the user is fully integrated in the market and can start receiving and sending crypto-assets. This disintermediated manner of accessing the market means that no one can filter – and thus identify (through Know Your Customer procedures) – new participants.[18] At the same time, the system through which participants are identified in the blockchain when performing transactions – the address – does not provide any information regarding the identity of the person using that specific account.

Due to such a privacy structure, these assets are labelled pseudonymous.[19] Eminently, an address is associated with each transaction carried out within the system. However, the address is identified through a pseudonym that does not provide any information regarding the real-world identity of the individual using it.[20] Furthermore, the absence of any mandatory point of access means that, if the user does use an intermediary at any point, no one can pierce the pseudonymity veil.[21]

[16] C. Leuprecht - C. Jenkins – R. Hamilton, *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*, cit., 2; for a detailed analysis of blockchain's privacy structure see chapter 2 section 6.

[17] See chapter two, section five.

[18] L. Haffke – M. Fromberger – P. Zimmermann, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, in *Journal of Banking Regulation,* 2, 2020, 129, "*on a decentralised Blockchain, transactions are not automatically screened for illegal activities by a party that is centrally responsible*"; R. Houben, Robby – A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion,* cit., 54; R. Coelho – J. Fishman – D. Garcia Ocampo, *Supervising cryptoassets for anti-money laundering*, Bank for International Settlements, Financial Stability Institute, 2021, 3.

[19] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 9.

[20] A. Trozze, et al., *Cryptocurrencies and future financial crime*, cit., 2; T. Frick, *Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland*, cit., 100.

[21] See Financial Action Task Force, *Virtual Currencies. Key definitions and potential AML/CFT risks*, Paris, 2014, 9, "*Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal*". This does not mean that deanonymization is not possible through blockchain analytics and other computer forensics methods, on that see S. MeikleJohn et al., *A Fistful of Bitcoins: Characterizing Payments among Men with No Names*, in *Proceedings of the 2013 Conference on Internet Measurement Conference*, 2016, and the section 6 of chapter 4. Rather that no

At the same time, blockchain is not a token-based system. In such systems, value exchanges are carried out by simply shifting the control of the valuable token – whether a bill or a bar of gold – from payer to payee. While pseudonymous, blockchain transactions still need to be recorded on a ledger and connected to the addresses of the two parties to be validly performed. The fact that a certain individual owns a certain amount of crypto-assets does not derive from the possession of a token but by the circumstance that the blockchain ledger assigns to a certain address a claim towards the network: the right to transfer a predetermined number of crypto-assets to another address of their choice. This entails that, in contrast to cash where there is no architectural need to record transactions, blockchain transactions leave a money trail that can be *ex post* analysed and examined.[22]

What is more, is that this trace is public and logically unified. As detailed in chapter two, blockchain's recordkeeping system is, in contrast with the traditional infrastructure, decentralized in terms of access and governance and centralized in terms of content. This means that, while pseudonymity and decentralization present a challenge to the anti-money laundering policy strategy, blockchain's information structure has aspects that may, if correctly exploited, facilitate monitoring.

First, the ledger is public whereas traditional intermediaries' ledgers are private.[23] This creates a new connection between the supervisory authority and the financial information as the first can directly access and analyse the latter. Also, each intermediary can monitor not only the transactions its customer carries out through their systems but also what their behaviour is within the whole network.

entity has access to the identity of the account holder and/or is in a position to deanonymize it through a mandatory identification process.

[22] As underlined by European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, SWD(2022), 27th October 2022, 94, "*We note, however, that crypto-assets transactions conducted on public distributed ledgers leave immutable traces and are there for everyone to see. Persons engaging in ML/TF via such crypto asset transactions expose themselves to public scrutiny of their transactions*"; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 91.

[23] For an analysis of blockchain's recordkeeping system see chapter 2, section 2; D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 5, "*Once the FBI established that a particular Silk Road user was using specific public wallet addresses, it could trace that individual's transaction history on the blockchain.19 The cypherpunks had envisioned cryptocurrencies as a means for engaging in commerce outside of government view, yet the blockchain offered a fully public money trail of Bitcoin transactions for law enforcement to use in its investigations*"; on blockchain analytics and its policy implications see chapter 4, section 6.

Second, the ledger records all the transactions carried out with a certain currency in a consequential manner whereas traditional ledgers only record the transactions carried out by the intermediaries' customer. This means that, in the traditional system, to piece together an individual's money trail, the investigator has to jump from one ledger to the other trying to piece together the respective entries. In contrast, in blockchain ecosystems all the information is saved in a single ledger that is then distributed in terms of access, making this exercise of piecing together the money trail sizably easier.

To sum up, blockchain's disintermediation and decentralized governance[24] challenge the traditional financial flows control strategy rooted in intermediaries as they allow users to directly enter the market and transact with each other peer-to-peer.[25] At the same time, blockchain does not represent a complete return to the token system, hence its transactions still leave the paper trail typical of account-based systems. This paper trail has certain peculiarities compared with those typical of traditional value exchange infrastructures. On the downside, this paper trail is pseudonymous and not controlled by any centralized body. On the bright side (at least for financial monitoring), is accessible and logically centralized.

Having understood the key features of the blockchain risk, it is now possible to critically evaluate the policy strategy that, since 2014, has been enacted to mitigate it.

[24] This risk is specifically identified – along with peer-to-peer transactions – by Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 40.

[25] As underlined by European Banking Authority, *Opinion on "Virtual Currencies",* Paris, 2014, 32, "*The risk arises because senders and recipients can carry out VC transactions on a peer-to- peer basis that do not require personal identification as there are no names attached to wallet addresses. Furthermore, there is no intermediary that could notify authorities of suspicious transactions. The priority of the risk is high*".

# Part one

## Setting the stage

### The definitory conundrum

Our analysis regarding the regulation of crypto-assets cannot but start by exploring how policymakers have drawn the normative boundaries of this concept.

As we will come to understand this is a complex exercise[26] as the object of regulation is, at the same time, elusive and politically sensitive.[27]

First, crypto-assets are an elusive category as they evolve at a dazzling pace with new implementations emerging in the space of months.[28] Also, this is a market that has, since its conception, the explicit political purpose of displacing traditional power dynamics.[29] This means that, on the one hand, the development of crypto-assets mostly happened outside of traditional markets and, at least initially, almost without the participation of traditional, established players, as financial institutions, or large corporations. On the other hand, the participants to this market are particularly averse to regulation and have sometimes shown an almost ideological opposition to

[26] European Central Bank Crypto-assets Task Force, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, Occasional Paper series no. 223, 2019, 7.

[27] C. Kuner – F. Cate – O. Lynskey – C. Millard – N. Ni Loideain – D. Svantesson, *Blockchain versus data protection,* cit., 103.

[28] The blockchain ecosystem, born initially as a network to sustain a private currency – the Bitcoin – has given rise to a baffling number of use cases that have nothing to do with the concept of currency, as Initial Coin Offerings, Decentralized Autonomous Organizations, Non-Fungible Tokens etc., used in areas as different as start up financing, supply chain management, art, and collectibles etc.; C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 2.

[29] See Chapter one on the historical roots of blockchain and crypto-assets.

any State intervention.[30] While the growing maturity of the market and the emergence of established players is softening these macrotrends[31] these can still be regarded as relevant characteristics of the crypto-assets community.

Second, the governance model proposed by blockchain is disruptive. It technically allows (at least in theory) to displace the traditional hierarchical, centralized model of governance in favour of a collaborative, decentralized system.[32] This means that regulators – which are among the central points of control this technology aims at eliminating or bypassing – have been particularly cautious when dealing with blockchain, especially in its permissionless form.

More than a decade after Bitcoin's introduction, the debate concerning how crypto-assets should be defined and regulated is still open and lively. Both the content and the name to be used for this conceptual category are at the fore of the policy debate in and outside Europe.[33]

This lively debate has caused a lack of consistency in the terms used by the legislatures.[34] Clear depiction of such lack of consistency is the fact that, taking the anti-money laundering field and Europe alone, there are three competing terms used to identify them. The FATF adopts the term "virtual asset", the current European legislation the term "virtual currencies", while the most recent Union's legislations (the Market in Crypto-asset Regulation, the Travel Rule Regulation, and upcoming Anti-money Laundering Package) the term "crypto-assets". Furthermore, the

[30] On the necessity for a change of mindset in the community see K Kolachala et al., *SoK: Money Laundering in Cryptocurrencies,* cit., 8.

[31] This trend of gentrification and corresponding shift from ideologically opposing any form of regulation to embracing it is not dissimilar to the one experienced by the internet itself. As described by P. Anderson, *Cypherpunk ethics. Radical ethics for the digital age*, cit., 6, "*the hackers all seemed to share an implicit set of beliefs: that computers could improve people's lives, that access to computers ought to be unfettered, that systems of centralized authority ought to be replaced with decentralized systems, that people should take a hands-on approach to technology, and—perhaps most famously—that all information should be free. By the early 1980s, however, the hacker ethos of openness, sharing, and decentralization had been eclipsed by business imperatives, with emerging computer and software manufacturers facing financial incentives that promoted the development of a closed, proprietary, and centralized culture*".

[32] Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 19.

[33] For an analysis of the labels used by the different regulatory and supervisory authorities see, R. Houben – A. Snyers, *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion,* cit., 20, who conclude that "*there is no generally accepted definition of the term cryptocurrencies available in the regulatory space. Even more, most policy makers have refrained from defining the term altogether*"; World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* White Paper, 2023, 6, "*a DLT-based crypto token may be termed a "virtual asset" in one jurisdiction but a "crypto token" or even a "virtual digital asset" in another (each with differing definitions) and be banned in a third*".

[34] T. Frick, *Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland*, cit., 101.

abovementioned definitions do not only differ in terms of the label used but also as to the content and even as to the regulatory approach.

This definitory instability underlines how, notwithstanding more than a decade has passed since Nakamoto published their seminal paper, the legislation is still in a "pilot phase". Our analysis will, thus, start from a critical evaluation of this definitory debate and of the solution adopted in order to identify its guidelines and weak points. We will then propose possible avenues for the development of a more balanced and customized approach.

## 1. The Financial Action Task Force

The Financial Action Task Force (FATF) is the unavoidable starting point of our analysis for two main reasons.

On the one hand, the FATF is a key player in the financial integrity arena, a field that has known, also thanks to this Body, a great degree of international standardization. [35] FATF's Standard and Guidances, despite their soft law status, are most of the times copy pasted in national legislations[36] and can, thus, be regarded as a golden standard when it comes to financial integrity.[37]

[35] L. Dalla Pellegrina – D. Masciandaro, *The risk-based approach in the new European anti-money laundering legislation: a law and economics view* in *Review of law & economics,* 2, 2009, 935; R. Pol, *Anti-money laundering: The world's least effective policy experiment? Together, we can fix it*, in *Policy design and practice,* 1, 2020, 76, "*FATF's anti-money laundering standards, in effect, dictate policies, laws and regulatory practices in 205 countries and jurisdictions*", M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 292; I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 2.

[36] For a critical review of this policymaking process see P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 145.

[37] A. Moiseienko, *Does international law prohibit the facilitation of money laundering?* in *Leiden Journal of International Law*, 2022, 6-7; C. Leuprecht - C. Jenkins – R. Hamilton, *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*, cit., 12; B. Mesquita – S. Maranhao – J. Seigneur, *Enabling KYC and AML verification in DeFi service*, cit., 1. For a criticism of this approach to policy making in the field see V. Mitsilegas – N. Vavoula, *The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law* in *Maastricht Journal of European and Comparative Law*, 2, 266 – 270, "*the FATF Recommendations has been mostly adopted without criticism by the European Commission in its proposals for Union law in the field and subsequently by Member States in the Council and by the European Parliament as co- legislators. In this manner, a specific agenda developed*

On the other hand, the FATF has been a pioneer in the regulation of crypto-assets. Its first Report on virtual currencies dates back to 2014[38] and the first Guidance to 2015.[39] The first sectorial European legislation – the Fifth Anti-money Laundering Directive[40] – was only introduced three years later, in 2018, and is almost a replica of the FATF Guidance.

The FATF has, thus, been a forerunner of crypto-assets regulation. This status is slowly changing as the market grows and evolves and States adopt a customized approach aimed at injecting their policy perspective in the evolution and architecture of these assets. Such a shift is clearly signalled, at the European level, by the Market in Crypto-asset Regulation (MiCaR) that aims at becoming a global standard in the sectorial regulation and, as further detailed, takes a partially different approach compared to the FATF. Notwithstanding this progressive "nationalization" of the crypto-asset regulation, the FATF definitions and guidelines played, and still play, a crucial role in shaping the way European anti-money laundering policymakers look at this field.

### 1.1 The first definition. The Financial Action Task Force's Guidance of 2015 and the definition of virtual currencies.

The first step in the crypto-assets legislation is the FATF's Report of 2014 and the subsequent Guidance of 2015. These two documents bear the first normative definition of what we now call crypto-assets. At the time, the term adopted to identify these assets was, however, different. In 2014, the FATF labelled this emerging category as "virtual currency".

A virtual currency was defined as:

> "*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not*

*by technocrats and with limited scrutiny at the global level has been legitimized, via the EU decision-making process, and adopted at the Union level to bind both FATF and non-FATF members*".

[38] Financial Action Task Force, *Virtual Currencies. Key definitions and potential AML/CFT risks*, cit.

[39] Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit.; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 293.

[40] Directive of the European Union, 30th May 2018, n. 843.

> *have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status".*[41]

In analysing this definition there are two synergic, and equally important, elements we need to consider: the name chosen to label these assets and the content of the definition.

The name chosen by the FATF to identify this new category of assets is "virtual currency". Both of the terms used tell a story: the term "currency" tells us how the regulator perceived these assets – a perception that will change in time – the term "virtual" tells us about its regulatory strategy – one that, at least at the FATF level, has stuck up to the present day.

### 1.1.1 The "currency" aspect of the virtual currency definition

Let's start, then, with the term currency.

From a historical perspective, the decision of the FATF to choose the term currency underlines the Bitcoin-centric nature of this first Guidance. In 2014, the Regulator saw crypto-assets mostly as a single purpose technology, as Bitcoin is. This single purpose was to provide the digital market with a private, decentralized means of exchange to transact online while staying out of the purview of traditional intermediaries and Central Banks. Such perception of crypto-assets' purpose – while it would prove incorrect in the medium term – is justifiable taking into account the period when this first Guidance was introduced. At the time, Ethereum had just been created and Bitcoin had

[41] Financial Action Task Force, *Virtual Currencies. Key definitions and potential AML/CFT risks,* cit., 4.

the lion's share of the market. Other implementations (as ICOs,[42] NFTs, and DAOs) would be introduced only during the following years.

Furthermore, as detailed in chapter one, this first policy effort was essentially a reaction triggered by a series of highly publicized cases that highlighted the aptitude of crypto-assets to be used as a facilitator of crime.[43] All of these cases – from the first dark market Silk Road[44] to the ransomware CryptoLocker[45] – exploited one fundamental function of crypto-assets: the means of exchange

[42] For a description of what an ICO is see A. Delivorias, *Understanding initial coin offerings. A new means of raising funds based on blockchain*, European Parliamentary Research Service, 2021; A. Ferreira – P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, in *Computer Law & Security Review,* 43, 2021, 5; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 30-31.

[43] For a first-hand depiction of the political climate at the time, see Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, cit., for the videorecording see https://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies.

[44] Silk Road was a digital marketplace, created in 2011, where it was possible to anonymously sell and buy any product – legal and illegal. Bitcoin constituted a fundamental piece of this criminal scheme, as it allowed users to bypass traditional financial institution and, thus, protect their anonymity by circumventing the corresponding anti-money laundering identification and monitoring duties. For this reason, Bitcoin was the only means of payment accepted on Silk Road. The notoriety of this marketplace created a strong sense of urgency among policymakers regarding the need to take action and bring Bitcoin under control. To have an understanding regarding the policymakers' view at the time, see Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, cit. For a brief history of Silk Road see D. Adler, *Silk Road: The Dark Side of Cryptocurrency*, in *Fordham Journal of Corporate and Financial Law Blog*, 21 February 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/. It is interesting to notice how the creation of such a marketplace had been foreseen by the same group that first envisioned the idea of cryptocurrencies, see T. May, *The cryptoanarchist manifesto,* cit., "*crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion*". For the dark market risk see European Banking Authority, *Opinion on "Virtual Currencies",* cit., 33.

[45] Cryptolocker is a ransomware attack that was first launched in 2013. This malware encrypts the files on the victim's computer and then asks for a ransom in exchange for their decryption. If the victim does not pay, they lose access to their files. The role of Bitcoin is, also here, that of means of payment. Namely, the ransom is usually requested by these malwares in Bitcoin so to guarantee that they are out the purview of enforcement agencies that could seize them. For a description of Cryptolocker see, Cybersecurity and Infrastructure Security Agency, *Cryptolocker Ransomware Infections Alert (TA13-309A)*, 5 November 2013, https://www.cisa.gov/uscert/ncas/alerts/TA13-309A; for the risk European Banking Authority, *Opinion on "Virtual Currencies",* cit., 34.

function.[46] Therefore, at the time, the FATF's primary objective was to address the currency aspect of crypto-assets, as this seemed the most pressing one for financial integrity.[47]

The first reaction of the FATF was, hence, to frame this "new thing" as a currency, as it seemed to perform the fundamental function of money: the means of exchange one.

The currency-centric nature of this early definition is also reflected in its content. To explain what virtual currencies are, the FATF refers to what virtual currencies, in its perspective, do. This is that virtual currencies function as *"(1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value*". This function-based definition does not, however, stem from an empirical observation of the real-world use of virtual currencies. Rather it merely replicates the three functions of money as per the classic economic theory.[48]

If classifying crypto-assets as a currency is an understandable choice, taking into account the historical and criminological context, copy pasting the definition of money and using it as the definition of virtual currencies is not. While the means of exchange function is a, although recessive, aspect of crypto-assets, it is quite clear that crypto-assets do not perform and have never performed a unit of account or a store of value function.[49]

This unfitness is clear if we analyse what it means for a currency to serve as a unit of account and store of value.

[46] This aptitude as a facilitator of criminal payments online has remained stable over time as underlined by Europol, *Internet Organized Crime Threat Assessment,* 2020, 17, "*Reliability, irreversibility of transactions and a perceived degree of anonymity have made cryptocurrencies the default payment method for victim-to-criminal payments in ransomware and other extortion schemes, as well as criminal-to- criminal payments on the Darkweb*"; European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 95.

[47] This focus on the means of exchange function is expressly stated in the introduction of the 2015 Guidance that, when defining its scope, says: this Guidance does not address "*non-payments uses of VC (e.g., store-of-value products for savings or investment purposes, such as derivatives, commodities, and securities products) or the monetary policy dimension of VC activities*" in Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit., 4.

[48] M. Carney, *The Future of Money,* Bank of England, 2018, 3; Bank of England, *Central Bank Digital Currency Opportunities, challenges and design,* London, 2020, 11; K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 9.

[49] M. Carney, *The Future of Money,* cit., 7; K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 9, "*Traditionally, money has been defined according to three functions it performs in the economy: medium of exchange, store of value, and unit of account.50 Arguably, given the current state of technology, cryptocurrencies perform none of these functions".*

On the one hand, the unit of account function implies that the currency can be used to keep accounts, transact, and assign a value to goods. A currency is a unit of account when it can, for example, be used to calculate and express the market value of something. To exemplify, when I say that an ice cream costs two euros, I am using the currency Euro as a unit of account.

On the other hand, the store of value function implies that the currency is a reliable instrument to preserve value over time. This entails that market participants can expect to be paid with a currency today and spend it tomorrow, in a month, or a year without significantly losing the underlying value. For this reason, perishable goods – such as wheat – are not efficient currencies. This is because the payor cannot simply hold them and be sure to store a value that can be spent at any time in the future.

There is, hence, one fundamental characteristic that impedes to an asset from serving as a unit of account and/or a store of value: the extreme volatility of its price.[50]

A volatile good cannot serve as a unit of account because no rational business would price its goods using as a reference an asset whose price changes constantly and unpredictably. How could a reliable price be established, so to cover costs and guarantee a profit, if the asset used as a unit of account is worth ten today, twenty in a month, and five in three months?

The practical consequences of this dilemma are clear if we analyse the penetration of Bitcoin as a retail means of payment. Notwithstanding much fanfare at the beginning of the last decade with large retailers announcing that they would start accepting Bitcoin, the retail use of Bitcoin as a means of payment never took off. At the same time, the retailers that do accept payments in Bitcoin (or other cryptos) do not hold the tokens they receive but immediately exchange them in *fiat* currencies to avoid the risks connected to its volatility.[51]

At the same time, an asset whose value fluctuates so dramatically cannot serve as a store of value. The core characteristic of a store of value is precisely to store the value and, hence, keep a relatively stable price over a medium to long period of time. Dramatic fluctuations of the price, while they

[50] S. Schwarcz, *Regulating Digital Currencies: Towards an Analytical Framework*, in *Boston University Law Review*, 102, 2022, 7; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance*, cit., 285; European Central Bank Crypto-assets Task Force, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, cit., 9.

[51] M. Carney, *The Future of Money,* cit., 9; European Banking Authority, *Opinion on "Virtual Currencies",* cit., 17.

can make a speculative asset very attractive – at least for those able to jump on the rollercoaster at the right time – eliminate the core functions of a currency and impede to qualify it as a store of value.[52]

Now, one of the core characteristics of crypto-assets (as well as arguably one of the reasons for their market success) has been, at least up until now, the extreme volatility and unpredictability of their price.[53] To assess that, we can just take the price of Bitcoin, or any other crypto-asset, in any given year. Let's take 2020 as an example. On the 2nd of January 2020, the price of Bitcoin was 7.175 dollars, on the 3rd of June 2020 9.525 dollars, and on the 3rd of January 2021 it was 32.216 dollars. The same pattern is replicated by all other crypto-assets with even more dramatic fluctuations happening with smaller or less relevant ones.[54]

While work is underway to create a so-called stable coin[55] – a crypto-asset that will keep a relatively stable value over time – we seem to be still very far from any credible implementation and were certainly very far from it in 2014. Some of the most relevant proposals have so far failed due to regulatory pushback[56] – as in the case of Lybra/Diem – or to failures of the underlying logic – as happened with the Terra/Luna coin.

This first definition of the FATF, hence, adopts a currency centric approach to crypto-assets that completely equates crypto-assets and fiat currency, at least in terms of function. So much so that it is the same definition that has to explicitly draw a line between virtual currencies and *fiat* currencies. It does so by clarifying that the main difference between virtual and *fiat* is that the former is accepted by agreement within the community of users, while the latter due to the order of the government.

At least for what concerns the currency aspect of this definition, the FATF seems to have not formulated a customized definition for this new category of assets. Rather, it operated a blanket

[52] Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 9.

[53] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 2; K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 8.

[54] M. Carney, *The Future of Money*, cit., 7; on crypto-assets volatility see also E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 7; Bank of England, *Financial Stability in Focus: Cryptoassets and decentralised finance*, cit., 9.

[55] W. Bolt – V. Lubbersen – P. Wierts, *Getting the balance right: Crypto, stablecoin and central bank digital currency*, in *Journal of Payments Strategy & Systems,* 16.1, 2022, 43; E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 7.

[56] K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 9.

equation between crypto-assets and the traditional concept of currency. Virtual currencies are, according to the FATF, nothing more than a privately issued *fiat* currency.

### 1.1.2 The "virtual" aspect of the virtual currency definition

This broad and nonspecific approach to the regulation of crypto-assets is also reflected by the second term chosen by the FATF: the "virtual" part of the expression "virtual currency". The term was preferred by the legislator to the more common "crypto". This is a critical preference as it reflects a specific policy approach that has survived up to the present day.

To understand why choosing the term "virtual" expresses a normative choice, we need to first appreciate what the prefix "crypto" stands for. This prefix is the most common one in the public debate and is the one that was first adopted by market participants and observers to identify Bitcoin and related technologies. The reason for this diffusion is that the prefix crypto directly refers to the branch of knowledge that most contributed to the development of blockchain: cryptography.[57] As detailed in chapter two, cryptography is a key aspect of blockchain, one that underlies its security (through the hashing of blocks), its update (through the proof of work), and its transaction system (through private/public key cryptography). The prefix crypto, hence, directly connects the asset to the technology as it refers to the fact that a certain asset is rooted in cryptography and uses its concepts and methods to function.

The FATF, by choosing the term "virtual", decouples the normative perimeter of the anti-money laundering regulation from blockchain technology. This way, the Guidance aims at embracing a wider category of privately issued currencies. The only "technological" characteristic these currencies need to share is being digital in their static and dynamic sense – i.e., virtual currencies have to be a digital representation of value and be digitally tradable.[58]

[57] See the use made by European Banking Authority, *Report with advice to the Commission on crypto-assets*, cit., 6.

[58] The FATF excludes from the regulatory perimeter all the tokens that cannot be traded and only represent a value assigned by the issuer to the recipient of the token.

This fundamental technological difference connected with the terms virtual and crypto is detailed by the same Guidance. Namely, right after the definition of "virtual currency", the Guidance provides for a series of non-normative definitions. Among them, there is one that is of particular interest to this naming discussion: the definition of "cryptocurrencies". Cryptocurrencies are identified by the Guidance as a *species* of the *genus* virtual currencies.

Cryptocurrencies are defined as:

> "*math-based, decentralised convertible virtual currency that is protected by cryptography —i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block)".*[59]

If we read this definition in light of what has been explained in chapter two, it is clear that this is the real customized definition of crypto-assets. Hidden behind the definition of "virtual currencies", the FATF precisely framed crypto-assets and identified their key elements: the governance system – decentralized and distributed – its identification framework – public/private key – and its update system – a network of mutually distrustfully parties that operate in a cooperative/competitive fashion.

The question is, then, if the FATF had the technical ability and understanding to provide for a customized definition of crypto-assets, why it didn't? Why did it adopt such a generic definition?

The choice can be traced back to two, intertwined, reasons.

The first reason for this choice is that the FATF espoused, when drafting this Guidance, the principle of technological neutrality.[60] Technological neutrality has long constituted a fundamental

[59] Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit., 27.

[60] This adherence to the principles of technological neutrality is not directly expressed in the Guidance of 2015. An explicit reference to this principle can be found in the following Guidance of 2019. The 2019 Guidance clearly states that technological neutrality is one of the key principles underlying the FATF legislative approach and that the Guidance, thus, applies irrespective of the technological platform involved,

tenet in the field of law and technology.[61] As underlined by the literature, this is a vague concept that has yet to receive a clear definition. However, technological neutrality can be broadly defined as the rule according to which the law should "*neither require nor assume a particular technology"*.[62]

The main ideological root of this principle is a market-oriented vision of the role of the legislator. The idea is that it is inefficient for the policymaker to advocate for a specific technology,[63] rather, this choice should be left to the free movement of the market. The legislator should, thus, focus on activities not technologies.[64] In this sense, the role of the regulator is to draw the boundaries of a certain field and/or human activity, irrespectively of the technology used by market participants.

The second reason underlying this choice is the idea of "future proofing"[65] the regulation. In a rapidly and constantly evolving reality, this principle aims at ensuring that a certain policy is designed to stand the test of time. Future proofing is a recurring theme when it comes to the rationale of technological neutrality.[66] The idea is that, in the field of new technologies, a regulation

see Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 9.

[61] For an analysis of the origins and development of this principle see C. Reed, *Taking sides on technology neutrality,* in *SCRIPTed: Journal of Law, Technology and Society*, 4/3, 2007, 263 e *ss.*; M. Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, in *B.U. J. Sci. & TECH. L.*, 18/303, 2012, 306; B. Greenberg, *Rethinking Technology Neutrality* in *Minn. L. Rev*, 2016, 100, 1512.

[62] Quote of the US Government's *Framework for Global Electronic Commerce* of 1997, taken from C. Reed, *Taking sides on technology neutrality,* cit., 263. As underlined by the same author, technological neutrality is a principle that, while being widely used by regulators especially in the field of law and technology, has still not received a clear definition and is frequently used as a catchall concept under which very different policies are implemented; see also the definition of M. Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, cit., 306, "*law should neither help nor hinder a particular type of technology".* As stated by B. Greenberg, *Rethinking Technology Neutrality*, cit., 1512, "*Technology neutrality's lodestar is intent to regulate behavior, not technology; to worry about what occurs, not how it occurs*".

[63] A. Escudero-Pascual – I. Hosein, *Questioning lawful access to traffic data*, in *Communications of the ACM,* 47/3, 2004, 78.

[64] H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 4, "*technology-neutral regulation tends to emphasize purpose and function, subject to context and interpretation*".

[65] C. Reed, *Taking sides on technology neutrality,* cit., 268, who defines future proofing, within the prism of technological neutrality, "*in two senses: 1) drafting of laws in a way which is flexible enough not to hinder the future development of technology; and 2) achieving sustainability in the sense that the law should not require over-frequent revision to cope with technological change*"; M. Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, cit., 308.

[66] B. Greenberg, *Rethinking Technology Neutrality*, cit., 1495, 1512 "*technology neutrality seeks to promote a statute's longevity - that is, to future-proof the law. The more technology specific a law is, the more difficult adapting to unforeseen technologies would seem to be (…) Technology neutrality attempts to invert the consequences of specificity; it presumes that laws untethered to specific technologies will be less disrupted by technological turbulence. Rather than force the law to struggle with new technologies, and in the interest of sparing legislators the time-consuming effort of frequent revisions, technology neutrality attempts to avoid ossification by making a statute more adaptable to technological advances. It does so through broad, open-textured terms*".

too rooted in a specific technological design may rapidly obsolesce as the market evolves and/or the underlying technological architecture changes.[67]

Furthermore, when it comes to a regulation that imposes substantive burdens – as the anti-money laundering one – it is argued that, if a regulation focuses on a specific technology, it may have a counterproductive effect. On the one hand, it may scare investors and developers away from that technology, this way hampering its development. On the other hand, designers may adopt minor manipulations to the technological architecture so to avoid the regulation by falling out of its scope. This way the Regulator would be stuck playing whack-a-mole with every single innovation.

We will return to the validity of this rationale in the next sections. First, we need to analyse the second definition provided by the FATF. Namely, as the two definitions are rooted in a similar strategic approach, we can condense the critique in a single section.

## 1.2 From virtual currency to virtual asset. Same old, same old?

The first definition adopted by the FATF was short lived. Only three years after its introduction the FATF amended its glossary and introduced a new definition. The expression chosen in 2018 was "virtual asset".

A virtual asset is defined as a:

> *"digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations".*[68]

The definition of 2018 does not fundamentally modify the previous policy strategy. Rather, it simply moves away from the currency centric approach of 2015 in favour of a broader vision of crypto-assets. Sign of the shift is, first and foremost, the substitution of the term "currency" with

[67] A. Veerpalu – E. da Cruz Rodrigues e Silva, *Hitting the White Ball: The Technology Neutrality Principle and Blockchain-Based Applications* in *The Indian Journal of Law and Technology,* 15,2, 2019, 304.
[68] Financial Action Task Force, *Glossary: Virtual Asset*, https://www.fatf-gafi.org/glossary/u-z/

the more neutral "asset". Furthermore, the FATF abandons the previous definition rooted in the three traditional functions of the currency (means of exchange, unit of account, store of value) in favour of a more generic reference to the fact virtual assets should be used as a means of payment and/or investment.

This change in the policy strategy is due to political and historical reasons.

Starting from the latter, if in 2014 the crypto market was mainly constituted by Bitcoin, the market in 2019 was a whole different story. The introduction of Ethereum, precisely in 2015, breathed new life into blockchain's evolution. Ethereum is rooted in the same infrastructure as Bitcoin – a public, permissionless blockchain – but is a multi-purpose platform. It allows developers to use decentralized consensus as a means to achieve much more than just exchanges of values among users.[69] This expansion in the perception regarding what crypto-assets can do, spurred the development of new technological categories.[70] Since then, the number of implementations and blockchain infrastructures has multiplied with some building on top of Ethereum (so-called Layer Two solutions) and other proposing alternatives to this primigenial model.

As the scope of the crypto-market grew so did its criminal applications. The introduction of Initial Coin Offerings (ICO)[71] as a means to gather seed funds by start-ups created new opportunities for fraud and money laundering.[72] The quite spectacular failure of the DAO project[73] underlined that a large amount of funds could be attracted by exotic crypto opportunities to then (magically)

[69] G. Hileman – M. Rauchs, *2017 global cryptocurrency benchmarking study*, cit., 15; this evolution in the purpose of crypto-assets was also underlined by the European Banking Authority in European Banking Authority, *Report with advice for the European Commission on Crypto-assets,* cit., 6, "*Today their use extends well beyond tokens for payment-type purposes (the VCs, sometimes also referred to as crypto-currencies or 'payment/exchange' tokens) to include 'investment' or 'security' tokens representing debt or equity claims on the issuer and 'utility' tokens used to provide access to applications or services (commonly involving DLT)*".

[70] European Banking Authority*, Report with Advice for the European Commission on Crypto-assets*, cit., 6, "*The use of crypto-assets, which depend primarily on cryptography and distributed ledger technology (DLT), has evolved rapidly in the last couple of years. Today their use extends well beyond tokens for payment-type purposes (the VCs, sometimes also referred to as crypto-currencies or 'payment/exchange' tokens) to include 'investment' or 'security' tokens representing debt or equity claims on the issuer and 'utility' tokens used to provide access to applications or services (commonly involving DLT)*".

[71] A. Delivorias, *Understanding initial coin offerings. A new means of raising funds based on blockchain,* cit., see also the dedicated website by the US Security and Exchange Commission, https://www.sec.gov/ICO; L. Haffke – M. Fromberger – P. Zimmermann, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, cit., 127.

[72] For an analysis of ICO-related frauds see L. Hornuf – T. Kück – A. Schwienbacher, *Initial coin offerings, information disclosure, and fraud* in *Small Business Economics,* 4, 2022; Europol, *Internet Organized Crime Threat Assessment,* cit., 14; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 30-31.

[73] For a description of this project and of its failure, see Chapter 1, paragraph 3.2.

disappear. Most recently, the skyrocketing value of collectible Non-Fungible Tokens (NFTs) showed that the role of crypto-assets in the money laundering cycle was much larger and complex than that underscored by Bitcoin or cryptocurrencies.[74]

In sum, from the decentralized means of exchange free from the yoke of intermediaries envisioned by Nakamoto, crypto-assets had, at least partially, moved towards a high-risk investment/speculative asset.[75] This shift was correctly perceived by the FATF that translated it in its definition. The "virtual currency" became a "virtual asset" and, between the functions this asset could play, payment was coupled with investment.

While the FATF's move certainly resulted from the evolution of the market, there is also a political factor that played a part. The exponential growth of the crypto-market alarmed regulators and Central Banks worldwide. These entities saw crypto-assets as a potential competitor in the money market and as a systemic risk for consumers and investors. The use of the term currency, in particular, was perceived as misleading as it associated crypto-assets and *fiat* currencies by generating the wrong perception the two shared a similar risk profile.[76] Also, the use of the term currency, especially by official sources, was seen as a sort of legitimization of cryptocurrencies. Central Banks – who had themselves initially adopted the term "currency" – started advocating to move away from the concept of currency towards the more neutral one of asset.[77] This lobbying activity was highly successful as the term currency effectively disappeared from the regulatory lingo in favour of the term asset.

[74] On the connection between NFTs and money laundering see Chainalysis, *The 2022 Cryptocrime Report*, cit., 35; A. Mosna – G. Soana, *When art goes virtual: what status for collectible NFTs under the current EU Anti Money-Laundering regime?,* in *Eu Law Analysis,* 13th of August 2022, http://eulawanalysis.blogspot.com/2022/08/when-art-goes-virtual-what-status-for.html

[75] W. Bolt – V. Lubbersen – P. Wierts, *Getting the balance right: Crypto, stablecoin and central bank digital currency*, cit., 42.

[76] European Central Bank, *Opinion of the European Central Bank on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, 16 February 2022, 14, "*AMLR1 replaces the term 'virtual currencies', which was introduced into Directive (EU) 2015/849 by Directive (EU) 2018/84370, with the term 'crypto-assets'. The ECB welcomes this change, as the term 'virtual currencies' could lead to misperceptions as to the nature of those types of assets, which are not currencies*".

[77] See the remarks by Bank of England's Governor, M. Carney, *The Future of Money,* cit., 9., *"cryptocurrencies are of growing interest to policymakers, many of whom prefer to term them crypto-assets expressly because they are not true currencies — a convention I will adopt for the balance of my remarks*"; the same goes for the remarks of the then Deputy Governor of the Bank of Italy (now ECB board member) P. Panetta, *Crypto-assets or virtual currencies as they were called before it was realized that they cannot perform the functions of money*, cit., 2; this change can also be inferred from the change in the naming by Public Authorities, see the EBA that in 2014 titled its report, Opinion on Virtual Currency to shift, in 2019, to the term crypto-assets.

Having analysed the roots of this definition, let's shift to the analysis of its content.

Although partially different, this second definition does not fundamentally alter the policy approach adopted in 2015. Apart from the, certainly appropriate, shift from a currency-centric approach to a multipurpose one – also underlined by the elimination of the reference to the unit of account and store of value function – the strategy adopted in 2015 is fully reiterated.

The new definition does not restrict or customize in any way the scope of the legislation. Quite the opposite, the previous definition restricted its scope only to a very specific category of assets: currencies that were privately issued in a digital form. In contrast, the current definition creates an amorphous category that encompasses any digital token that has two characteristics: one, can be digitally traded and, two, can be used for payment or investment purposes. The only real limit to this potentially all-encompassing category is that virtual assets should not be regulated elsewhere by the FATF Recommendations.

In brief, under the definition of 2018, virtual assets become a residual category that includes any digital token not otherwise regulated. It is clear that, with such a definition, customization becomes extremely complex. Namely, even drawing *ex-ante* the boundaries of what constitutes a virtual asset is exceedingly difficult.

### 1.3 Missing the target. A critique of the FATF approach

Now that we have analysed the fundamental elements of the FATF's first and second definition, we can draw some initial conclusions.

In brief, these two definitions encompass all those assets that share three characteristics: they have a digital form, are digitally tradeable, and are used for payment or investment purposes. In this sense, the FATF's Guidance is, at least *prima facie*, completely decoupled from any underlying technological consideration.

The main shortcoming of this approach is that, as analysed above, blockchain poses a fundamentally new challenge to the anti-money laundering legislation compared to traditional electronic value exchange systems. It can be argued that a system like Bitcoin can hardly be equated, in terms of anti-money laundering risk, to a token that is issued and governed by a centralized authority – be it a private or public entity.[78] If the risk is qualitatively different so should the connected mitigating measures.

This need for customization based on the risk factor is in line with the fundamental principle underlying the anti-money laundering regulation: the risk-based approach.[79] The risk-based approach requires regulators, supervisors, and covered entities to customize their actions to the specific risk identified. Eminently, the anti-money laundering regulation is not envisioned as a monolithic, rigid regulation. Rather, as a flexible instrument to be adapted to the multifaced characteristics of the connected phenomenon. [80] In this sense, given the different risks posed by crypto-assets such a principle calls for an approach that embraces rather than rejects the difference. The FATF's equation of centralized and decentralized assets seems to miss such a different risk factor.

To put it plainly, you cannot use the same weapon to hunt a lion or a shark.

This qualitative difference in terms of risk factor between centralized and decentralized networks is well depicted by a case occurred just a couple of years before Bitcoin came into the picture: Liberty Reserve.[81]

Liberty Reserve was a Costa Rica-based money transmission service that offered its products through a native currency – the Liberty Dollar. Due to the lack of anti-money laundering checks

[78] The different risk generated by decentralized assets compared to centralized one is highlighted by the same FATF that in its Guidance of 2015 states "*When assessing the ML/ TF risk of convertible VC, the distinction between centralised and decentralised VC will be one key aspect. Due to anonymity and the challenges to conduct a proper identification of the participant, convertible decentralised VCPPSs in general may be regarded of higher risk of ML/FT which would require the application of enhanced due diligence measures*", Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies*, cit., 8.

[79] For more on the risk-based approach see chapter 4 section 2.1

[80] M. Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control,* cit., 39.

[81] Interestingly this case is mentioned by the first FATF Guidance. However, the structural differences between Liberty Reserve and Bitcoin are not underlined nor explored, see Financial Action Task Force, *Virtual Currencies. Key definitions and potential AML/CFT risks*, cit., 10.

– especially in terms of customer identification[82] – the Liberty Dollar became a safe haven for international criminal transactions. Criminals could exchange illicit proceeds into Liberty Dollars and send them globally to their partners or use the currency as a way to blur the money trail. It is estimated that, during its operating period, Liberty Reserve processed more than eight billion dollars in transactions.[83] The service came to a brutal halt in 2013 when United States enforcement authorities arrested Liberty Reserves' founder and successfully downed the system.[84]

It is precisely the demise of Liberty Reserve that underlines the qualitative difference between a centralized virtual currency and a decentralized one. Enforcement actions such as those carried out in the Liberty Reserve case – i.e., arresting the administrators and shutting off the website – would not be feasible with crypto-assets.

This both from a technical and a legal perspective.

From a technical perspective, crypto-assets are rooted in a decentralized network of mutually distrustful nodes. In this sense, blockchain governance, at least in its permissionless form, does not depend on any centralized entity. Rather, it is based on the cooperation of a network of nodes acting according to the fundamental law of the blockchain – i.e., its underlying code. This means that these types of network keeps functioning as long as at least one of its nodes is online.[85] If the nodes are scattered across the globe and belong to different entities and/or individuals, it is extremely complex, if not impossible, for a State to single-handedly disrupt it. With blockchain, unilateral action – as the one used against Liberty Reserve – cannot simply target one entity.[86] To successfully down the network it is necessary to target all the entities controlling each and every node in a nearly simultaneous fashion.

[82] While certain identification measures were implemented, they were far from being effective as no validation mechanism was put in place, with accounts established under clearly false names as "John Bogus", "Hacker Account", see Financial Action Task Force, *Virtual Currencies. Key definitions and potential AML/CFT risks*, cit., 10.

[83] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 15.

[84] See, United States Department of Justice, *Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars*, 6th May 2006, https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars

[85] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain space,* cit., 19.

[86] See Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies*, cit., 11, "*law enforcement cannot target one central location or entity for investigative purposes*".

From a legal perspective, a (truly) decentralized governance model means no one is squarely in charge of the network's management. Individual responsibility and choices may, therefore, be hard to ascertain in these cases.

In a centralized network, individual responsibility is relatively easy to ascertain. When it comes to these networks, criminal prosecution is mostly a matter of reach: the main question for the enforcement authorities is if the individual/s managing the network are within their reach. If this is the case, then they can be arrested, and traditional prosecution follows. Going back to our example, with Liberty Reserve it was clear who was in charge of the network and enabled illicit transactions. While exotic, the actions of Liberty Reserves' executives clearly fall in the traditional framework of money laundering. Prosecution was, hence, relatively straightforward, once the individuals were materially apprehended.

In contrast, in a permissionless blockchain network, even though many entities contribute to its functioning – nodes, miners, developers, etc. – none of them really controls it. All these entities act according to the underlying code, and none of them can unilaterally modify it.[87] For this reason, it would be arguably complex to charge one of the abovementioned entities[88] for not properly identifying Bitcoin users, as happened with Liberty Reserve's executives. No entity in a blockchain network could unilaterally impose identification duties: the non-identification rule is determined by the code itself, to which all network participants must abide. In a decentralized network, all participants are (at least formally) equal and none of them can unilaterally control or impose anything on others. If this was not so, the same concept of decentralization would be refuted. There is only one entity whose action could be considered causal to the way the system works: its initial creator, the person/s that designed the technological architecture and wrote the code.[89] This is, probably, one of the reasons why Nakamoto, the creator of Bitcoin, never revealed their identity.

In brief, the main risk posed by crypto-assets to the anti-money laundering infrastructure is new and specific to these ecosystems as it is connected to blockchain's governance structure: the

[87] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 16.

[88] World Economic Forum, *Decentralized Finance (DeFi) Policymaker Toolkit*, cit., 18,

[89] Such a technological reality has opened a debate regarding whether developers of crypto-assets and decentralized applications should be qualified as covered entities under the anti-money laundering regulation. For more see chapter 5, section 3.

creation of a truly decentralized value exchange system, rooted in cryptography, enabling peer-to-peer transactions.[90]

In blockchain environments, no one is in control of the infrastructure or the access/exit points. This challenges the traditional financial flows control strategy rooted in intermediaries. In contrast, a centrally issued and governed private digital asset/currency does not pose any new or specific problem. In centralized ecosystems, there is an entity – the issuer – that can be potentially controlled and be subject to anti-money laundering obligations. The only problem in these cases is whether the enforcement agency can concretely implement the legislative command. This is, however, a classic problem of cybercrime legislation and in no way new or specific to virtual currencies. In a global and dematerialized environment, the State does not always have the political and economic power to reach and coerce individuals or, alternatively, shield its system from them. When it comes to privately issued assets, centralization eliminates the main risk posed by blockchain to anti-money laundering governance: the lack of a centralized point of pressure that can be targeted by the policy maker.

Equating centralized and decentralized assets is, thus, mixing apples and oranges, at least from an anti-money laundering perspective.[91] The choice of linking the regulation of these two assets, through a common definition, is crucial as it reverberates in the whole regulatory strategy. If crypto-assets are associated with centralized assets, then the pre-existing regulatory strategy is conceivably extended to them. This association between the two assets at the definitory level can be regarded as the "original sin" of the sectorial regulation. Eminently, by equating traditional and new assets, it has hampered the creation of a regulatory strategy that could specifically address, and exploit, the peculiarities of blockchain's governance structure.

Up until now our critique has been essentially rooted in an empirical comparison between centralized and decentralized assets. However, to fully analyse the strategy adopted by the FATF

[90] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 13

[91] As underlined by K. Fatjon – E. Martino – A. M. Pacces, *fintech and The Law and Economics of Disintermediation*, cit., 9 "*Several central banks are experimenting with digital currencies. This is a way to exploit the promise of the blockchain in terms of management of money supply and efficiency of settlements, while maintaining the role of central banks as gatekeeper of money and monetary policy. Libra and government-controlled digital currencies could scale up in the coming years. Nevertheless, these projects hardly imply disintermediation of money and payments, as governments are either directly involved or require intermediaries to have a license in order to convert digital into traditional currencies. Rather, these projects change the way money and payments are intermediated, exploiting the blockchain*".

in its definition, we need to go back to its ideological driving forces and examine whether those premises are reasonable and have been reasonably applied in the case at hand.

As examined in the previous paragraph, technological neutrality is certainly one of the driving forces, if not the driving force, of this legislative approach. Let's then delve into how this principle applies to the situation at hand. It is, in particular, appropriate to question whether this principle should always be the fundamental parameter driving the policymaker.

Critiques to technological neutrality have already surfaced in the literature.[92] Reed[93] notes that a blanket application of the principle of technological neutrality can generate over-generic regulations. Escudero-Pascual and Hosein[94] underline how technological neutrality can be used as an excuse by the legislator to avoid addressing technologically specific challenges.[95] On that note, Thompson argues that technological neutrality impedes to address crucial socio-political problems by narrowing the scope of the legislative action.[96]

A part of the literature, thus, suggests that technological neutrality should not be a rule carved in stone but one to be adopted when necessary and in the measure necessary.[97] In certain occasions a technology specific regulation may be appropriate to implement solutions that better address the problem at hand.[98] Greenberg, in particular, proposes to adopt technological discrimination

[92] C. Azar – B. A. Sandén, *The elusive quest for technology-neutral policies* in *Environmental Innovation and Societal Transitions,* 1/1, 2011; M. Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, cit.; B. Greenberg, *Rethinking Technology Neutrality*, cit., 2016, 100.

[93] C. Reed, C., *Taking sides on technology neutrality,* cit., 282, "*technology neutral regulation cannot be very specific about the subject matter which it regulates",* on a similar note M. Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, cit., 308 - 310*,* sees technological neutrality as expressing a general principle of legislative vagueness.

[94] See the discussion by A. Escudero-Pascual – I. Hosein, *Questioning lawful access to traffic data*, cit., 78 of how technology neutral language hinders the protection of individual rights, due to a lack of specification in terms of the quality of data processed, when it comes to law enforcement's access to traffic data.

[95] A. Escudero-Pascual – I. Hosein, *Questioning lawful access to traffic data*, cit., 78. "*technology-neutral language may be used to ignore the challenges and risks to applying powers to different infrastructures*".

[96] M. Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, cit., 314, "*If law is to address these problems, it will need to choose between different possible technological models and do so by regulating technological artifacts themselves through properties other than their functions. The vagueness principle, however, restrains such choices by directing the law to focus only on the functions of technological artifacts*".

[97] B. Greenberg, *Rethinking Technology Neutrality*, cit., 1547.

[98] C. Reed, C., *Taking sides on technology neutrality,* cit., 283-284; as underlined by B. Greenberg, *Rethinking Technology Neutrality*, cit., 1498, "*technological discrimination sometimes enhances social welfare (…) Conversely, technology specificity has unappreciated bene- fits. By embracing the need for more frequent updates, technology-specific laws can be drafted more carefully than technology- neutral laws and be coupled with judicial tools and regulatory processes that help technology-specific laws achieve the policy goals of technology neutrality, and without the costs*".

instead of technological neutrality.[99] In his opinion, this would help generating customized solutions that address the specific problems posed by each specific technology.

All of these critiques resonate when it comes to crypto-asset regulation. The legislative equation of centralized and decentralized assets creates an over-generic regulation that does not address the challenges specifically posed by blockchain to financial flows monitoring. At the same time, through this equation, the policy maker avoids facing the fissure opened by crypto-assets in the financial monitoring infrastructure. This way failing to innovate and revise its traditional approach. This is a comfortable choice, hardly an effective one.

Digging deeper, there is a systemic reason why an anti-money laundering regulation addressing blockchain should be customized to its underlying logic. Blockchain, rather than a new technology, meaning an instrument or technique that allows to perform a certain activity in a new form, is a class of technologies united by a common logic. It is this logic – the possibility for a digital network to reach consensus without needing a central authority – that constitutes the true innovation purported by blockchain. Based on this fundamental logic, a whole new batch of implementations has surfaced – from currencies, to digital art, to autonomous contracts and organizations.

In this sense, blockchain proposes an alternative rationale in the structure of data storage and management. One that changes the fundamental approach to governance and challenges the pre-existing regulatory strategy[100] in the field of anti-money laundering. With such a fundamental innovation, customization should be warranted.[101]

As stated by Greenberg with regard to the regulation of the Internet:

[99] B. Greenberg, *Rethinking Technology Neutrality*, cit., 1547.

[100] Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, cit., 7, "*Tale rilevanza della componente tecnologica e degli stessi fornitori di tecnologia realizza una sorta di "governance algoritmica" che scardina gli schemi di governo tradizionali e della quale è necessario tenere conto*".

[101] H. Axelsen – J. Jensen – R. Omri, *When is a DAO Decentralized?*, cit., 69, "*The concept of technology-neutral regulation is challenged by DLT/Blockchain. DAOs exist and realize benefits through increasing degrees of decentralization. DAO legal design should therefore support the internal decentralization accomplished by the DAO so that a balance is achieved between external and internal decentralization [11], not the other way around. When regulators in the coming years design technical requirements for the supervision of DAOs, they need to acknowledge this underlying premise and embrace that DLT/blockchain is a transformative technology that requires unique regulatory approaches*".

*"The Internet, like the combustion engine to the farmer, is a technological discontinuity - a rapid spike on the timeline of innovation that moves the future of technology onto a new plane. And the principles underlying the law, whether technology specific or neutral, are disrupted".*[102]

The disruption of the principles underlying the law, operated by a paradigm shifting technology, cannot be addressed through the simple extension of the previous legislation. Rather, it is a change that calls for new, customized, solutions and strategies.

In short, if the absence of intermediaries and governance centres in blockchain infrastructures is not addressed, the blanket will always be too short. The legislation needs to face and address this absence and it cannot do that if it treats centralized and decentralized infrastructures in the same way.

The regulator has chosen a technologically neutral definition to avoid playing whack-a-mole with crypto-assets. What it seems to have missed is that the only mole to whack (at least in the financial flows control debate) is the blockchain. The whole "crypto risk" is intimately connected with blockchain's governance structure; without it, the risk morphs in such a drastic way that it is not regulable in a comparable way.

Every part *destruens* needs a part *construens*. What should be, then, a definition that, while being general enough to be future proof could still allow the legislator to address the new challenges decentralized governance generates?

We will come back to this argument in a few pages, but first let's continue our analysis of the legislative saga.

## 2. The European Dimension

[102] B. Greenberg, *Rethinking Technology Neutrality*, cit., 1527.

The FATF was the first to provide a legislative response to the emerging crisis posed by crypto-assets. A response that anticipated and paved the way to National legislations. However, the soft law status of FATF's Guidances meant that, for concrete implementation, national law was needed.

At the Union's level, such a hard law response came in 2018, three years after the first FATF's Guidance. Precisely when the FATF was revising its approach to crypto-assets regulation by introducing the new definition of "virtual asset".

The European Union's definition – provided by Directive n. 843 of 2018 (so-called Fifth Anti-money Laundering Directive)[103] – is one that, hence, mixes elements of the FATF's first and second definition. With this first definition, the European Union completely followed the FATF's definitory strategy both in approach and content.

This initial consistency between the FATF and European legislation lasted until 2023 with the introduction of the first comprehensive Regulation of the crypto-assets market – the Market in Crypto-assets Regulation (MiCaR). With this piece of legislation, the European Union distances itself from the FATF's approach. The MiCaR expressly focuses on decentralized assets and, hence, aims at providing a legislative framework customized to crypto-assets and the specificity of their governance model. Although not an anti-money laundering regulation per se, the definition provided by the MiCaR is referenced by all the pieces of legislation that compose the Anti-money Laundering Package whose introduction is planned in 2024, making it paramount for any study in the field.

With the introduction of a definition of crypto-asset, one that directly addresses decentralized technologies, the Union aims at pursuing an independent strategy in the regulation of crypto-assets one customized, at least in theory, to their characteristics.

## 2.1 The first definition. The Fifth Anti-money Laundering Directive

[103] Directive of the European Union, 30th May 2018, n. 843

At the European level, the in-force anti-money laundering legislation disciplining crypto-assets is Directive no. 843 of 2018. This Directive was initially thought as a means to implement the FATF's Guidance of 2015. However, the introduction of this legislation coincided with a turning point in the FATF's strategy. In 2018, when the Directive was being approved, the FATF was already partially revising its approach with the amendment of its glossary and the second Guidance on virtual assets of 2019.

Probably due to this specific timing, the definition provided by the Directive constitutes somewhat of a combination of the first and the second definition of the FATF. In particular, article 3, paragraph 2, letter d, point 18, of the Directive chooses the term "virtual currency" but then introduces a somewhat broader definition than that used by the first FATF Guidance. A definition that partially resembles the second FATF's definition of "virtual asset".

Under Directive n. 843 of 2018, a "virtual currency" is defined as:

> *"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".*

Building upon the critique developed in the previous section we can appreciate how this definition presents similar problems as the FATF's ones. Compared to the first FATF definition this one is somewhat broader and less currency specific – in this sense, it is more similar to the second definition of virtual asset. Eminently, the Directive abandons the reference to the store of value and unit of account functions. At the same time, compared to the second FATF's definition of virtual asset, it is more currency specific as underlined by both the use of the term currency and the reference solely to the means of exchange function and not to the investment one.[104]

This textual restriction paves the way for two opposing interpretations.

[104] At the same time recital 9 of the Directive seems to contrast with the letter of the law and expands the scope of the Directive beyond the monetary function as it states "*although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies*"; on the meaning of the expression means of exchange and for a critique to recital 9 see L. Haffke – M. Fromberger – P. Zimmermann, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, cit., 132.

A strict textual interpretation would subsume under the anti-money laundering compliance duties, only currency tokens. This interpretation reads the "means of exchange" expression as a reference to the three functions of the currency. In this sense, a virtual currency is only that which is used as an intermediary asset to exchange goods without any interest of the trader in the use or consumption of the virtual currency.[105] This interpretation finds a textual anchor in the use of the term currency to identify these tokens. The use of this term to frame crypto-assets suggests a connection between the means of exchange function and the theory of the currency.

Such a restrictive interpretation would, however, menace the effectiveness of the Directive. Considering the conformation of the market, excluding investment tokens from its purview would restrict its application to a, mostly obsolete, conception of crypto-assets.

A second broader interpretation would subsume under the definition of article 3 all tokens that are used as a medium in an exchange. This interpretation would hence also include investment tokens. To support this reading three arguments can be used. First, a textual one. Recital 10 of the Directive states:

> "*Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies".*

Second, the broader interpretation would be in line with the aim of the European Union to conform to FATF's standards. As underlined by the same Directive[106] and by the legislator's statement, the European anti-money laundering infrastructure is informed by the FATF's guidance. The Guidance is seen as a fundamental point of reference. In this sense, the updated Guidance and definition of virtual asset could be used as an external interpretative means to clarify the scope of the Directive and include non-currency tokens.

This second interpretation seems to, hence, be more appropriate if a broader perspective is taken.

However, going back to our previous distinction among centralized and decentralized arrangements, the Directive does not seem to innovate or ameliorate in any significant way the

[105] L. Haffke – M. Fromberger – P. Zimmermann, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, cit., 131.
[106] See the frequent reference made to the FATF's Standard by the Directive at e.g., recital 4 and 12.

pre-existing FATF's definitory strategy. The definition crystalized by the Fifth Directive is as generic in terms of underlying technology or governance structure. In this sense, it equally fails to focus on the elements that characterize crypto-assets and/or their specific risks. We can, thus, fully refer to the analysis developed in the previous section.

## 2.2 A new European approach. The Market in Crypto-assets Regulation

The last definition we will analyse is fresh out of the regulatory box.

Introduced in 2023, the Market in Crypto-assets Regulation (MiCaR),[107] aims at becoming the European (and possibly global) gold standard for the regulation of crypto-assets.[108]

The MiCaR constitutes the key piece in the growing body of European legislations devoted to crypto-assets. The MiCaR was initially proposed in 2020 as part of the Digital Financial Package.[109] However, its introduction gained increasing momentum in the years following. The causes underlying such an increased regulatory momentum are multifaced. On the one hand, the crypto-winter of 2021/2022 made the crypto-market too big to ignore.[110] The failure of exchangers as

[107] Regulation of the European Union, 31st May 2023, n. 1114. For a more detailed analysis of this regulation and of its fundamental provisions please see the section devoted to MiCAR in Chapter 4, section 3.

[108] A. Ferreira – P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, cit., 3. The Market in Crypto-assets Regulation is part of the Digital Financial Package presented by the European Commission in September 2020. Explicit aim of this Package is "*paving the way for Europe to become a global standard-setter*" in line with the ambitions of the EU to be able to further expand its so-called "Brussels effect". See European Commission, *Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses (Press Release),* 24 September 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684 and G. Maia – J. Vieira dos Santos, *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*, 2021, 2, on the Brussels effect see A. Bradford, *The brussels effect,* cit., 1. More on this Package D. Zetzsche – F. Annunziata – W. Douglas - R. P. Buckley, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy* in *Capital Markets Law Journal*, 16.2, 2021, 203-204.

[109] For more on the Package see European Commission, *Digital Financial Package,* Press Release, 24th September 2020, https://finance.ec.europa.eu/publications/digital-finance-package_en.

[110] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 8; for a description of this period and its effects see G. Gorton – J. Zhang, *Bank Runs During Crypto Winter*, in *University of Michigan Law & Econ Research Paper*, 2023.

FTX and stable coins as Terra Luna caused an aggregated loss of billions of dollars.[111] The losses are also alleged to have had spill-over effects in the traditional market, with failures menacing regional and global economic stability.[112] On the other hand, the criminal risk connected with crypto-assets has reached geopolitical dimensions. Crypto-assets are increasingly identified as facilitators for sanctions circumvention and state-sponsored acts of cybercrime.[113]

If the legislative goal is shared, at least among Western Countries, the strategies differ. The United States has, so far, primarily adopted a regulation-through-enforcement approach.[114] Financial supervisors commenced a series of actions against crypto-companies under the same activity, same risk, same regulation standard. In contrast, the European Union has devised a body of regulations customised to crypto-assets. The Market in Crypto-assets Regulation (MiCaR), the DLT Pilot Regime, and the Travel Rule Regulation are all part of the same strategy. The idea is to create a clear playing field to foster the safe development of the crypto-market.[115] In this sense, the MiCaR provides for a comprehensive framework to police crypto-asset offerings and service providers.

This piece of legislation is not an anti-money laundering policy per se. Quite the opposite: MiCaR solely covers aspects connected with the protection of the market and its customers and is explicitly framed as a financial regulation. The definition bore by MiCaR is, however, of direct relevance for the anti-money laundering strategy. In compliance with the Commission's ambition

[111] E. McCaul, *Mind the gap: we need better oversight of crypto activities*, cit., https://www.bankingsupervision.europa.eu/press/blog/2023/html/ssm.blog230405~03fd3d664f.en.html

[112] Examples of such spill over being the failure of the three US banks, SVB, Silvergate Bank and Signature Bank, E. McCaul, *Mind the gap: we need better oversight of crypto activities*, cit.; see also E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 8; for a contrasting view G. Gorton – J. Zhang, *Bank Runs During Crypto Winter*, cit., 20 that argue the current crisis didn't have a spill over effect due to crypto-lending circularity, but that the next crypto-crisis will probably have such spill over effects due to a modification in the crypto-companies' business model, "*what happened in crypto space largely stayed in crypto space. But that might not be the case going forward. The next generation of crypto innovations are becoming "interoperable" with the real economy—that is, facilitating financial transactions in the real world, not just in crypto space*".

[113] European Banking Authority, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, Paris, 2023, 95.

[114] T. A. Moffett, *CFTC & SEC: The Wild West of Cryptocurrency Regulation, U. Rich. L. Rev*., 52, 2022, 713, E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 13.

[115] A. Minto, *The legal characterization of crypto-exchange platforms*, cit., 139; 153, "*very few pieces of law are so evocative and powerful in shouting out the urgency that justified them. And very few pieces of law open setting out that "the first objective is one of legal certainty". The European Commission overtly account for other goals, such as "supporting innovation and competition", ensuring "consumer and investor protection", fostering "market integrity" as well as maintaining "financial stability". Yet, on top of such list of objectives, as if it was a "hierarchy", legal certainty comes first and reminds us all how pressing the crypto qualification issue is".*

for this Regulation to become the cornerstone of the European strategy on crypto-assets, its definition is to be applied in all sectors of the European legislation, including anti-money laundering.

For this reason, each piece of legislation composing the upcoming Anti-money Laundering Package[116] refers to the MiCaR when defining its scope.[117] The Travel Rule Regulation,[118] the First Anti-money Laundering Regulation,[119] and the Sixth Anti-money Laundering Directive[120] all refer in their definitory section to the definition of crypto-asset laid out by MiCaR. The definition of crypto-asset is, hence, deemed to become the new gold standard for the anti-money laundering regulation in Europe.[121]

Let's, then, analyse the content of the MiCaR's definition.

As mentioned, the Regulation revolutionizes the strategy rooted in technological neutrality we have analysed so far by introducing, for the first time, a crypto-specific definition.[122] This change of approach is already apparent from the expression used by the MiCaR to identify the object of its regulation: crypto-assets. As underlined above, the shift from the expression "virtual asset" to "crypto-asset" is a momentous one as the term "virtual" articulated the decoupling of the legislation from blockchain technology. In contrast, for the MiCaR to use the term "crypto" means, at least potentially, customizing the legislation to a specific technology, one that has cryptography at its core.

[116] The Anti-money laundering package, presented by the Commission the 20th of July 2021, is a series of reforms of the anti-money laundering infrastructure (including the institution of an AML European authority, an AML Regulation, the Sixth AML Directive, and the Travel Rule Regulation) that aims at further standardizing the legislation at the European level, for more information see https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en

[117] A. Minto, *Riflessioni sull'applicabilità della disciplina antiriciclaggio ai Non-Fungible Tokens ("NFT")*, in *Rivista di Diritto Bancario*, 1, 2023, 54.

[118] Regulation of the European Union, 31sr May 2023, n. 1113.

[119] Proposal for a Regulation of the European Union, 20th of July 2021, n. 0239.

[120] Proposal for a Directive of the European Union, 20th of July 2021, n. 0250.

[121] This extension to the AML sector is already stated by the same Regulation; see recital 16 of the MiCaR "*Any legislative act adopted in the field of crypto-assets should also contribute to the objective of combating money laundering and terrorist financing. For that reason, entities offering services falling within the scope of this Regulation should also comply with applicable anti-money laundering and counter-terrorist financing rules of the Union, which integrate international standards*".

[122] European Central Bank, *Opinion of the European Central Bank on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing,* cit., 14.

Consequently, article 3, paragraph 1, number 5, of the MiCa Regulation defines crypto-asset as a:

> *"a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".*

To better refine its scope MiCaR introduces three connected definitions:

Article 3, paragraph 1, number 1, defines Distributed Ledger Technology:

> *"means a technology that enables the operation and use of distributed ledgers".*

Article 3, paragraph 1, number 2, defines Distributed Ledger as:

> *"means an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism".*

Article 2, paragraph 1, number 3, defines a consensus mechanism as:

> *"the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated".*

The definition of crypto-assets is, hence, based on two pillars.

First, the identification of the minimum characteristics a token needs to hold to be qualified as a crypto-asset. Second, the definition of the technology a token needs to be rooted in to be qualified as a crypto-asset – i.e., Distributed Ledger Technology (DLT).

### 2.2.1 The definition of the token

Starting from the token, crypto-assets inherit some elements of the previous definitions. As virtual assets and virtual currencies, to qualify as a crypto-asset a token has to be digital, and it needs to be possible to electronically store and transfer it.

Apart from these similarities, the Regulation impresses a decided change of strategy. The definition abandons the functionalistic approach that focused on the tokens' function – payment, investment, means of exchange, store of value, etc. Instead, the definition traces its scope by defining what a token is.

Following MiCaR, a crypto-asset can be two things: a digital representation of value or a digital representation of a right.

The concept of a token representing a value was already familiar under the previous legislation: for a token to be used for payment or investment, it needs to bear value for the person holding it and for the market in general. The MiCaR, in speaking about a digital representation of value, simply expands the concept of a digitally tradable value beyond the two functions the definition of virtual asset and virtual currency restricted it to.

This is a welcomed innovation both in terms of market structure and legislative technique.

In terms of legislative technique, the definition focuses on the common prerequisite that an investment and a means of payment share: they are a representation of value. Compared to the previous approach, which enumerated every single function of the token, this definition is more principle based, hence, flexible. With MiCaR, the legislator does not have to chase each new implementation or use, rather it has a general definition that encompasses all possible digital tokens that bear a value independently from their use. In terms of anti-money laundering, this is a sensible choice as what makes a token significant for money laundering is its economic value. A worthless token could hardly be used by criminals to launder, move, or exchange value online.

In terms of market structure, the definition is well suited to the most recent evolutions of the crypto market. The main idea that is emerging is that crypto-assets may become a multi-purpose token to incorporate any type of value and then exchange it peer-to-peer. In this sense, crypto-assets are perceived as a means to achieve real property of digital assets, one that is full and exclusive and not dependent on Internet Service Providers or other intermediaries. Such a tendency is clearly highlighted by their proposed use in the nascent Metaverse. There crypto-assets – in the form of NFTs – are being used to incorporate goods – from pieces of virtual land to a Gucci bag. In this sense, a definition that focuses on what a crypto-asset is – a digital representation of value – rather than what it does will make the MiCaR comparatively more future proof and avoid continuous amendments of the legislation.

More problematic is the clear identification of the meaning of the term "value". On the one hand, value is a polysemous term, even more so when not complemented by an adjective that clarifies its scope (such as economic, financial, or sentimental). On the other hand, the rest of the Regulation doesn't in any way better delineate this concept. Quite the contrary, recital 2 states that:

> *"Representation of value also includes external, non-intrinsic value attributed to a crypto-asset by parties concerned or market participants, meaning the value can be subjective and can be attributed only to the interest of someone purchasing the crypto-asset".*

Such a lack of a clear delimitation is problematic in terms of legal certainty. Even more so, in an area as money laundering, where noncompliance can lead to – individual and corporate – administrative, and criminal liability. If framing crypto-assets as tokens holding a value is a sensible choice, the genericity of the term "value" should have been counterbalanced by a rigorous demarcation of its scope. The legislator should have, first, clarified what type of value was relevant and then connected it to external and clearly identifiable indexes.

In its current formulation, the definition seems to be in contrast with the principle of legal certainty. While this is a principle which clear delimitation is debated and hard to grasp,[123] foreseeability is certainly one of its key elements.[124] As detailed by the Venice Commission of the Council of Europe foreseeability means that laws "*must be formulated with sufficient precision and clarity to enable legal subjects to regulate their conduct in conformity with it*".[125] The current definition of crypto-asset does not seem to be precise enough to allow regulated entities to assess *ex ante* whether they fall within the purview of the anti-money laundering legislation.

For anti-money laundering purposes, it would be advisable to circumscribe the concept of crypto-asset only to those tokens that have an economic value. The presence of such economic value should be connected to external, objective parameters shelving the subjective evaluation prescribed by recital 2. These could include: whether the token has a market value and is listed by

[123] J. Van Meerbeeck, *The principle of legal certainty in the case law of the European court of justice: from certainty to trust*, in *European Law Review,* 41, 2016, 280.

[124] This connection has been most recently confirmed, in 2022, by the Court of Justice of the European Union, Republic of Poland v European Parliament and Council of the European Union, Case C-157/21, "*the principle of legal certainty requires, on the one hand, that the rules of law be clear and precise and, on the other, that their application be foreseeable for those subject to the law, in particular, where they may have adverse consequences. That principle requires, inter alia, that legislation must enable those concerned to know precisely the extent of the obligations imposed on them, and those persons must be able to ascertain unequivocally their rights and obligations and take steps accordingly*".

[125] Venice Commission of the Council of Europe, *The Rule of Law Checklist,* Venice, 2016, 26.

major exchangers, whether the token incorporates an underlying asset of economic value, whether the asset or the network reaches a threshold turnover.

The suggested delimitation of the analysed definition is not only required by the principle of legal certainty but also by the logic of the sectorial regulation. Eminently, the current anti-money laundering legislation is rooted in a risk-based approach.[126] Following this approach, not all tokens should be regulated based on a general principle of precaution. Rather, compliance duties should be imposed only on those tokens that pose a significant enough risk. In terms of anti-money laundering, a prerequisite to this risk is for the token to have an economic value. Namely, it is such value that enables criminals to use it – whether to invest, pay, be paid, or launder.

It will, thus, be up to the Supervisory Authority, and in particular the European Banking Authority, to issue guidelines that clarify what is meant by value so to guarantee the Regulation is compliant with European law and with the spirit of the anti-money laundering legislation.

In sum, the definition of crypto-asset as a "digital representation of value" constitutes a welcomed modification of the previous approach as it shifts to a principle-based definition not focused on each single implementation of the token. At the same time, the absence of any specification regarding what is meant with the term "value" seems in breach of the principle of legal certainty and risks to impose relevant burdens on tokens that cause no significant concern.

The second category a token can fall into is that of "digital representation of a right". This second category is less on point than the first, at least from an anti-money laundering perspective.

This is one of the areas where the friction created by the use of a definition envisioned for a financial regulation in the anti-money laundering field emerges.[127] From a financial law perspective,

[126] The risk-based approach is one of the founding principles of the anti-money laundering regulation since the beginning of the 21st century. This approach was introduced to promote a proactive approach by National regulators and supervisors as well as regulated authorities and avoid the so-called "tick-box compliance". The risk-based approach requires these entities to calculate the risk of each sector/customer/transaction and apply a corresponding level of compliance efforts; as defined by the FATF itself in Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 31: "*The risk based approach to AML/CFT aims to develop prevention and mitigation measures that are commensurate with the ML/TF risks that countries and the relevant obliged entities identify*". For an evaluation of such approach see L. Dalla Pellegrina – D. Masciandaro, *The risk-based approach in the new European anti-money laundering legislation: a law and economics view* in *Review of law & economics,* 2, 2009. For more on the principle and its underlying logic see Chapter 4 Section 2.1.

[127] For more on this friction see the following section.

the aim of the MiCaR is clear: to encompass the issuance of any tradeable token even if it does not have an intrinsic value as it may be connected with the exercise of rights of economic significance or in connections to entities of economic significance. From an anti-money laundering perspective, monitoring the exchange of digital representations of non-economic rights seems trivial and, again, in contrast with the risk-based approach. At the same time, if the right does have an economic value, then it would already fall in the first category of a "digital representation of value" making this second category redundant.

This term should then be interpreted, at least in the anti-money laundering domain, in a sense that is coherent with the purpose and logic of the sectorial regulation. Tokens that are a digital representation of non-economic rights should, thus, be excluded as non-relevant and the term be interpreted as a clarification that also crypto-assets that incorporate economically valuable rights should fall under the monitoring duties. This second expression also calls for a clarificatory action by the Supervisory Authority to customize the general definition provided by the Regulation to the needs of the anti-money laundering legislation.[128]

### 2.2.2 The definition of the technology

Having analysed the fundamental elements that make of a token a crypto-asset, it is now time to delve into the second pillar of the European definition: the technology.

The distinctive element of MiCaR, compared with the previous regulations, is that it is technology specific. This means that, to qualify as a crypto-asset, a token has to be rooted in a specific technology. The technology that has to underpin crypto-assets is, following article 3, Distributed Ledger Technology (DLT). In principle, Distributed Ledger Technology is an expression that

[128] Such a clarificatory power of the European Supervisory Agencies (ESAs), while not directly provided for the crypto asset definition, is dictated by various parts of the MiCaR as art. 2, art. 19, etc.

identifies all those technologies that use, to store their data, a distributed repository – the distributed ledger – in contrast with a centralized one.[129]

The relation between blockchain and DLT is rather vague as the two terms are either used alternatively[130] or, more frequently, blockchain is framed as a subcategory of DLTs.[131] In the latter sense, blockchain is seen as a DLT that not only decentralizes data storage but also the governance of the network. To further complicate the matter, the term blockchain – accompanied by the adjective permissioned – is used to identify technologies that only decentralize data storage and retain, at least in part, centralized control.

The expression "Distributed Ledger Technology" does not, therefore, identify a clearly defined technology or class thereof. Rather, the interpreter must analyse the content of the definition to understand what conception of DLT is adopted by the legislator. The Regulation seems to adopt a broad interpretation of the expression Distributed Ledger Technology. One that encompasses any technology that presents at least some elements of decentralization.[132]

There are three elements that the Regulation identifies as key to a DLT: a decentralized ledger, a consensus mechanism, and a set of nodes. The Regulation frames a Distributed Ledger Technology as any technology that is rooted in a shared, distributed ledger safeguarded and updated by a series of nodes according to a preestablished consensus mechanism.

If we go back to our previous distinction between centralized and decentralized networks, we can see the definition can be interpreted to encompass both. Eminently, MiCaR's definition does not distinguish between technologies that centralize the governance and those that decentralize it: the

[129] The European Banking Authority*, Report with Advice for the European Commission on Crypto-assets*, cit., 8, defines it as a technology that "*enables the storage, update and validation of information in a decentralised way*"; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 26, "*DLT refers to a group of technologies that use different techniques and structures to store, synchronise and maintain a shared ledger of digital records across a network of computing centres*".

[130] A. Ferreira – P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, cit.; C. Kuner – F. Cate – O. Lynskey – C. Millard – N. Ni Loideain – D. Svantesson, *Blockchain versus data protection,* cit., 103; M. Finck, *Blockchains and data protection in the European Union,* cit., 18.

[131] In this second sense see D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 3 and European Banking Authority*, Report with Advice for the European Commission on Crypto-assets*, cit., 8; H. Axelsen – J. Jensen – R. Omri, *When is a DAO Decentralized?*, cit., 53.

[132] This also emerges from recital 1 of MiCaR that clearly qualifies blockchain as one of the possible applications of DLT, see "*It is expected that many applications of DLT, including blockchain technology, that have not yet been fully studied will go on to create new types of business activity and business models which, together with the crypto-asset sector itself, will lead to economic growth and new employment opportunities for Union citizens*".

nodes could all be owned or controlled by a single entity and/or the consensus mechanism be designed so to fully centralize control of the ledger and still the technology would qualify as a DLT under MiCaR.[133]

What is relevant for our ends is that, irrespective of the governance mechanism implemented, any technology that decentralizes the physical storage of data among a set of nodes and establishes a protocol to enable a consensus to be formed among these nodes regarding the state of the ledger is qualified as a DLT under MiCaR.

When it comes to financial flows monitoring, such a choice is highly problematic as it misses the key risk factor generated by blockchain: the decentralization of governance. A decentralized ledger is no different than a centralized ledger when is controlled by a single (or even by multiple) entities that can be clearly identified and regulated.[134]

We will return to this point in the following section.

### 2.2.3 Assessing the Market in Crypto-assets Regulation. Customized, just not enough?

The previous section has analysed the definition provided by the Market in Crypto-assets Regulation to identify its scope and strategy. The present section will critically examine it in light of the specific risks crypto-assets create for financial flows monitoring.

The Market in Crypto-assets Regulation undoubtedly constitutes a step towards the customization of the legislative response to the specificities of blockchain technology and of decentralized tokens. The adoption of a crypto-specific regulation and definition, and the generalization of the concept

[133] As we have discussed in the section on Permissioned Blockchains (Chapter 2, Section 7) these types of consensus protocol have already been envisioned and implemented. Proof of Authority, above described, entrusts the power to update the ledger to nodes that hold a permission given by the network administrator and/or the underlying protocol.

[134] Examples of such centralized networks in terms of governance are permissioned blockchains that allow the creation of centres of governance, for more on permissioned blockchains see Chapter 2 Section 7, for an example of such network see the one created by IBM and Maersk described in Chapter 1 Section 4.

of crypto-assets not to encompass single implementations but any token that incorporates a value are, within the above outlined limits, welcomed innovations. To customize is, however, not enough, if the customization does not encompass the key elements that differentiate one conceptual category from the other. The MiCaR fails exactly at doing this by providing a definition that does not distinguish the key elements that make a crypto-asset qualitatively different in terms of financial monitoring compared with a digital asset. The present section will delve into this failure to then identify possible adjustments.

The MiCaR certainly adopts interesting and welcomed innovations when it comes to framing crypto-assets.

First and foremost, the MiCaR partially abandons the strict adherence to the principle of technological neutrality. With the introduction of a crypto-specific definition, the European legislator goes beyond the previous approach that completely decoupled policy and technology. Rather than a complete desertion, the Regulation seems to reframe technological neutrality.

As clarified by recital 5.

> *"a Union framework on markets in crypto-assets should not regulate the underlying technology. Union legislation avoids imposing unnecessary and disproportionate regulatory burdens on the use of technology, since the Union and the Member States seek to maintain competitiveness on a global market".*

The recital distinguishes between two targets a regulation can aim at: the technology and its use. The former is out of the purview of the Regulation that should instead focus on the latter. Technological neutrality is, thus, for the legislator not to meddle with the architecture of the technology but only with the actions of the individuals that interact with it. In this sense, the legislator can regulate the market created by a specific technology and the use individuals make of it (as long as it avoids unnecessary burdens) but not the underlying technological architecture.

To exemplify this distinction between regulation of the technology and regulation of its use we can take as an example the discussion regarding the limitation of the Proof of Work (PoW) consensus protocol.[135] This protocol is at the centre of a harsh debate due to its environmental

[135] For a description of this protocol see Chapter 2 paragraph 4.

impact.[136] It was precisely because of environmental concerns that, as part of the legislative procedure in the Parliament, MEPs proposed a series of amendments to the MiCaR aimed at limiting, if not banning, the use of Proof of Work in the European Union.[137] These amendments would have constituted precisely what was excluded by recital 5: a direct regulation of the underlying technology. By banning or limiting Proof of Work, the regulator would have acted directly on the technological architecture and not on its use. This direct regulation of the technology was ultimately rejected by the Parliament[138] as it was perceived as an intrusion in a field that should be within the sole purview of the market: choosing which type of technology (i.e., consensus protocol) is more convenient.

It is clear how this interpretation of the principle of technological neutrality differs from the one previously embraced by the Financial Action Task Force and the same European legislator as part of the Fifth Anti-money Laundering Directive. There being neutral meant regulating the activity regardless of the technology,[139] that was not to be mentioned. With the Market in Crypto-assets Regulation, being neutral means regulating the use of a certain technology without directly targeting its architecture. In the first sense, the neutrality was directed towards the choice of the technology: the legislator did not have to influence players in choosing between different types of technologies when performing a certain activity. In the second sense, it is directed towards the architecture of the chosen technology: the legislator can regulate a technology but should not influence its development.

This is certainly a welcomed reinterpretation.

[136] See L. Wintermeyer, *Bitcoin's Energy Consumption Is A Highly Charged Debate – Who's Right?,* in *Forbes,* 10th May 2021, https://www.forbes.com/sites/lawrencewintermeyer/2021/03/10/bitcoins-energy-consumption-is-a-highly-charged-debate--whos-right/?sh=756343e87e78; D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 2019, 668

[137] See European Parliament, *Amendments 503 – 838 Markets in Crypto-assets, and amending Directive (EU) 2019/1937 2020/0265(COD),* 3rd of June 2021, https://www.europarl.europa.eu/doceo/document/ECON-AM-693741_EN.pdf

[138] E. Nicolle – L. Pronina, *EU Crypto Proposal Seen as De-Facto Bitcoin Ban Fails in Vote*, in *Bloomberg,* 14th of March 2022, https://www.bloomberg.com/news/articles/2022-03-14/eu-crypto-proposal-seen-as-de-facto-bitcoin-ban-fails-in-vote?leadSource=uverify%20wall; see also, European Parliament, *Cryptocurrencies in the EU: new rules to boost benefits and curb threats,* Press Release, 14th of March 2022, https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats.

[139] As clarified by Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 9, technological neutrality means that the FATF's requirements "*apply irrespective of the technological platform involved*".

On the one hand, with paradigm shifting technology – as blockchain[140] – a blind equation between different architectures is very similar to a discrimination as the same rules are applied to technologies which functioning and underlying logic are completely different. At the same time, focusing on the specificities of a certain technology enables the legislator to address the specific challenges it poses without having to restrict itself to generic rules.

On the other hand, excluding from the legislative purview the technological architecture seems a reasonable choice. To carve in a normative text fixed standards regarding what a technology ought to be is a tricky exercise. Miscommunication and misunderstanding between policymakers and market participants can lead to illogical solutions that curb innovation and mummify the market. Further, the rapid evolution of new technologies, and of the underlying architecture, does not match the pace of policy making with the risk of having legislations that are born obsolete. It seems, hence, more reasonable for the Regulator to demand the market – including the developers – that a technology achieves certain goals or upholds certain standards without directly dictating the how.

Notwithstanding the customization purported by the MiCaR, the focus of this tailoring effort is not the governance structure – meaning the decentralization of control – but the data archiving structure - meaning the decentralization of the storage of information. This is exemplified by the definition of Decentralized Ledger Technology (DLT) adopted by the Regulation. Article 3 MiCaR defines DLT as *"an information repository that keeps records of transactions and that is shared across, and synchronized between, a set of DLT network nodes using a consensus mechanism".* It is clear how, under this definition, there is no distinction between governance structures: all technologies that adopt some form of decentralization in their record-keeping strategy are equated.

Now, mixing centralized and decentralized assets is, at least in terms of anti-money laundering legislation, an incorrect equation. As explained above, the crux of the problem, when it comes to financial flows monitoring, is not the way data is stored but the way the network is governed. If data is stored in a decentralized manner but centrally controlled, then there is no real difference with a centralized system: the policymaker can regulate the network's controller and impose on

[140] A similar technology-specific approach to the policing of new technologies has been taken by the European Union concerning the regulation of Artificial Intelligence; see Proposal for a Regulation of the European Union laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*,* 21st of April 2021.

them identification and monitoring duties. In contrast, if the network fully decentralizes governance, then there is no centralized controller, and anyone can enter and exit the market without a filter. This is where financial monitoring becomes qualitatively different as it, at least partially, lacks its usual point of pressure: intermediaries.

To clearly understand how governance, and not data storage, is the key element of differentiation for anti-money laundering purposes, let us return to our analysis of permissioned ledger.[141]

A permissioned blockchain is a type of DLT that partially or completely recentralizes control. This means that for the participants to perform certain key actions – e.g., access the market, transact, access all or certain parts of the ledger, etc. – they need a permission from the governance body. Examples of these networks are the (now defunct) DIEM stable coin and the European Blockchain Services Infrastructure (EBSI) created by the European Union.[142]

In a network as such, the problem of control is primarily a matter of reach.[143] If the National Authority can force the governance body to comply, then there is no architectural limit to control.[144] The governance body can be required to only grant access to those users that are identified (following the Know Your Customer procedures) and can then be compelled to monitor and report individual transactions.[145] The identification limitation, which is a design feature in fully

[141] For an analysis of how a permissioned ledger works see Chapter 2, Section 7.

[142] For a description of the European Blockchain Services Infrastructure see https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

[143] This is also underlined by Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit., 32, "*Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies (…) may seem to exist in a digital universe entirely outside the reach of any particular country*".

[144] Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 7, "*una distinzione rilevante va fatta tra DLT permissioned o permissionless. Le prime richiedono che un utente, per accedere e apportare modifiche al registro (ledger), debba ottenere il permesso da parte di un soggetto o entità centrale, che de facto assume responsabilità di governance. Nelle DLT permissionless invece è difficile o impossibile individuare tale responsabile*".

[145] This is clearly stated by the same FATF in Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Paris, 2020, 13, "*The central developers and governance bodies of so-called stablecoins are in a unique position to undertake ML/TF risk mitigation, as they determine how the functions of the so-called stablecoin arrangement (e.g. the stabilisation mechanism, transfer of coins and user interface) will operate. They make key design and functionality decisions and they determine the extent to which functions are centralised or decentralised and whether AML/CFT preventive measures are built into a so-called stablecoin. They can also control the access points to the arrangement (e.g., who can participate as an exchange or transfer service or whether a person can only access the system through a VASP) and impose AML/CFT standards setting out expectations or operating requirements for key entities in the arrangement, including exchanges and custodial wallet providers. They are also best positioned to undertake centralised AML/CFT functions, such as transaction monitoring across the so-called stablecoin arrangement*".

decentralized ledgers, is not present in permissioned ones, completely changing the possible legislative strategies. The same goes for the limitation connected with the seizure of assets. If in permissionless blockchains seizure is not possible – without the account's private key – as these networks process transactions in a mostly blind and trustless manner, the same does not apply in permissioned networks. With a consensus mechanism as Proof of Authority (PoA),[146] that affords to certain nodes the authority to approve new transactions, there is always the possibility to require such nodes not to process certain transactions, this way, *de facto*, freezing the assets.

The crux of the anti-money laundering risk is, hence, not how the data is stored or processed but how the governance is structured.

Here the fallacy of applying a definition thought for a financial regulation to a crime control legislation emerges again. The risk posed by crypto-assets to the former legislation does not completely collide with the latter.

For financial regulation the main risks are financial stability, market integrity, client/investor protection, and market efficiency.[147] In this sense, the elements this regulation targets are such as the issuer's solvency, the provision of correct and transparent information to customers and investors, etc. In contrast, the money laundering regulation is solely aimed at avoiding the use of the financial infrastructure – whether traditional or crypto – to finance crime and/or launder the proceeds of criminal activity. The elements this regulation targets are, thus, the identification of the market participants, their correct profiling, the monitoring of transactions, and the freezing and reporting of suspicious ones.

The discrepancy between the objectives pursued is momentous when it comes to crypto-asset. The elements of crypto-assets that graduate their risk level for financial regulation do not completely coincide with those relevant to anti-money laundering. A common definition will most likely end up being inadequate for one or the other.

The emergence of a global stablecoin is a good example of how these risks differ.

[146] For an analysis of the functioning of Proof of Authority see Chapter 2, Section 7.

[147] See D. Zetzsche – F. Annunziata – W. Douglas - R. P. Buckley, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, cit., 208; A. Ferreira – P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, cit., 3.

For global stablecoin it is meant a crypto-asset, issued by a private entity, that maintains a stable value[148] and is available on a global scale.[149] Such a coin would *de facto* be in direct competition with national *fiat* currencies. A global stablecoin is deemed to generate relevant risks in terms of financial regulation as it imperils financial stability challenging the role of the Central Bank and the functioning of the credit system.[150] This risk is clearly highlighted by MiCaR that regulates in detail such tokens and even provides for a veto power when such coins "*serious threat to the smooth operation of payment systems, monetary policy transmission or monetary sovereignty".*[151]

In contrast, the same type of tokens does not generate a clear risk in terms of anti-money laundering. Of course, as underlined by the FATF's Report on Stablecoins,[152] the potential for mass adoption and global reach does constitute a risk as it widens the potential for misuse of the system.

However, as underlined by the same Report:

> *"the FATF consider that so-called stablecoins with potential for mass-adoption will be centralised to some extent, with an identifiable central developer or governance body. The FATF considers that these developers and governance bodies will be, in general, financial institutions (e.g., as a business involved in the 'issuing and managing means of payment') or a VASP (e.g., as a business involved in the 'participation in and provision of*

[148] A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, cit., 38; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 8; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 74; E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 7.

[149] See the definition of European Banking Authority, *Report with advice to the Commission on crypto-assets*, cit., 7 '*Stablecoins' are a relatively new form of payment/exchange token that is typically asset-backed (by physical collateral or crypto-assets) or is in the form of an algorithmic stablecoin (with algorithms being used as a way to stabilise volatility in the value of the token)*"; E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 8.

[150] A. Ferreira – P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, cit., 7, "*The biggest risks of global stablecoins are attributed to their scale, which could affect monetary policy, monetary sovereignty, financial stability, fair competition, and the in- ternational monetary system overall*"; E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 9 -10; Bank of England, *Financial Stability in Focus: Cryptoassets and decentralised finance*, cit., 20.

[151] See art. 24 para 2, Regulation on Markets in Crypto assets, see also the similar provisions of art. 21, para 2, lett. e.

[152] Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, cit., 8-9.

> *financial services related to an issuer's offer and/or sale of a virtual asset') under the revised FATF Standards. This is an important control to mitigate the ML/TF risks poses by such so-called stablecoins".*[153]

The Report identifies two key risk factors: that a stable coin may be issued by an entity located in a non-compliant jurisdiction (the abovementioned problem of reach) or that it could have a "*decentralized governance structure*".[154] The FATF's analysis hence clarifies that, for money laundering purposes, the crux of the risk generated by stablecoins is their governance structure and not their potential to collapse the current monetary and financial market.

The repercussion of the different risk profile on the definitory strategy is clear. The financial regulation will devise a definition that encompasses all possible tokens as they all generate a risk for financial stability, with share of the market being the key risk indicator. The anti-money laundering one will (or rather should) distinguish between centralized and decentralized assets, with the main risk factor being the absence of a governance body that can be regulated.

To sum up, the main fallacy of the definition of crypto-asset laid out by MiCaR is that, while a crypto-specific definition, this is not an anti-money laundering specific definition. This means that the definition is not customized to those characteristics of crypto-assets that generate a risk for financial flows monitoring. The aim of MiCaR is to provide for a definition ample enough to encompass any crypto-asset irrespectively of their anti-money laundering risk.[155] The purpose of an anti-money laundering definition should be to distinguish between assets that create qualitatively different risks so to customize the policy strategy to each one of them.

[153] Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, cit., 3, 8; of the same advice O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 25.

[154] Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, cit., 4.

[155] This is clearly underlined by recital 16 of MiCaR that states "*Any legislative act adopted in the field of crypto-assets should be specific and future-proof, be able to keep pace with innovation and technological developments and be founded on an incentive-based approach. The terms 'crypto-assets' and 'distributed ledger technology' should therefore be defined as widely as possible to capture all types of crypto-assets that currently fall outside the scope of Union legislative acts on financial services"*; A. Ferreira – P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, cit., 12 – 13, "*This definition aims to capture the entire universe of crypto assets, but for those expressly excluded from MiCA. This broad application is intended to ensure there are no crypto assets outside of the regulato ry framework*".

This especially when one category of assets creates such a different risk to require a qualitatively new strategy. Equating centralized and decentralized assets in a single definition has a direct impact on the content of the regulation itself. Namely, if all tokens – both centralized and decentralized – are treated in the same way, the traditional strategy (thought for centralized assets) is likely to prevail. The way the scope is drawn directly influences the ability of the policymaker to customize the anti-money laundering duties depending on the type of assets. This does not mean that each asset should be in a micro category and that duties should be minutely customized to each one of them. Such a customization would make the regulation overly intricate and compliance unnecessarily complicate. However, when a category of assets presents such specificities, as decentralized crypto-assets do, then a distinction should be introduced at the definition level so that a specific strategy can be devised.

In the face of such an inadequate strategy, the European legislator still can adjust its course without any direct modification of the MiCaR. As we have highlighted, the original sin in the definition of crypto-assets is the discrepancy in the purposes pursued by the financial and anti-money laundering regulation. This mismatch can be solved without modifying the overarching definition laid out by MiCaR.

The problem with the analysed definition is that it does not distinguish between different categories of crypto-assets, not that certain crypto-assets that should be regulated are not. The definition is thus over-generic, not over-specific. To solve this problem, the needed distinctions could be introduced directly at the anti-money laundering level. The legislations composing the Anti-money Laundering Package could be modified to include sub-definitions to allow the establishment of a customized strategy.

This legislative technique would be in line with the overarching purpose of MiCaR: creating a common European definition of crypto-assets. It would leave untouched a general definition that would be generic enough to become the gold standard the European Union is aiming at. At the same time, it would allow to create subcategories to customize the generic definition to the needs of each specific legislation.

Furthermore, such a specification is already present in the MiCaR itself. Article 3 of the Regulation distinguishes between three subcategories of tokens to which it applies slightly different rules: the e-money tokens, the asset-referenced tokens, and the electronic money tokens.[156] In a similar way as these three categories adapt the overarching definition of crypto-assets to the specific needs of the financial regulation, sub-definitions could be introduced to adapt the same generic definition to the specific needs of the anti-money laundering legislation.

So, what should these categories be? The next section will delve exactly into this.

## 3. Going back to the roots. A proposal for a money laundering specific definition of crypto-asset

Until now we have talked about the 'is' of crypto-assets regulation. The present section will focus on the 'ought'. This section will, building upon the previous analysis, propose the fundamental elements a definition of crypto-assets should have to be truly customized to the anti-money laundering field.

It is out of question that the key element of innovation introduced by crypto-assets is decentralization. This is a conviction shared by both the crypto-specific and the crypto-neutral definitions we have analysed so far. However, the Market in Crypto-assets Regulation showed that not any type of decentralization necessarily constitutes an element of differentiation from previous assets – at least for anti-money laundering purposes.

The facet of decentralization that underlies the capsizing of the anti-money laundering infrastructure is the decentralization of the governance. For decentralization of the governance is meant that blockchain networks do not entrust to any single authority the management of the network. Rather, blockchains are managed by a collection of mutually distrustful nodes that operate according to the encoded rules of the network. This makes the functioning of the network *de facto* autonomous as none of the participants can disobey the encoded rules of the network and these are automatically enforced through the coral, blind action of the nodes. The decentralization of the governance does not entail that blockchain's code is immutable: minor amendments and

[156] For more on these three categories see Section 2.

updates are carried out regularly in every blockchain. Rather, that major changes need a near-unanimous approval and are hence very hard to carry out.[157]

The first element that is of crucial relevance for our distinction is the presence of a centralized governance body. As underlined in the discussion concerning permissioned blockchain,[158] if such a body is present then it can be forced to implement network-wide compliance and traditional anti-money laundering regulatory themes would re-emerge. The first characteristic of a decentralized token is, hence, that it should be rooted in a network not governed by any centralized entity.

The second element of decentralization that is key to our distinction is disintermediation. A disintermediated network is one that enables users to access it and exchange the token in the absence of any intermediary. Even if the network's governance is decentralized, nothing hinders the creation of a decentralized but fully intermediated network. Decentralized networks are far from anarchic machines which functioning is left to the wisdom of the crowd. Rather, the blockchain replaces the centralized human authority – typical of traditional infrastructures – with a set of encoded rules that dictate how the network functions and that, lacking a governance centre, are very difficult to modify – hence the blockchain motto "in code we trust".[159] If such rules were to envision a fully intermediated network, there would be no significant difference with traditional networks and, again, the intermediary-centred strategy would apply. This does not mean that the network has to be fully disintermediated; intermediaries can exist, the key element is that their use should not be compulsory but merely an option. The second key characteristic of a decentralized token should, thus, be that it allows users to access the network and exchange value in a disintermediated fashion: peer-to-peer.

[157] This is clearly depicted both by the Ethereum split after the DAO hack (described in the previous Chapter) and by the debate regarding how to enhance the efficiency of Bitcoin that has been dragging for the last decade without achieving any significant result precisely due to the choral nature of any major amendment, see P. Ennis, *An Anatomy of Bitcoin's Great Scaling Debate,* in *Coindesk,* 15th May 2016, https://www.coindesk.com/markets/2016/05/15/an-anatomy-of-bitcoins-great-scaling-debate/. This does not mean that decentralized networks have no governance structure rather that such governance mechanisms are informal, for an analysis see R. Thapa – P. Sharma – J. Hüllmann – B. Savarimuthu*, Identifying Influence Mechanisms in Permissionless Blockchain Communities: The Bitcoin Case* in *42nd International Conference on Information Systems (ICIS)*, 2021.

[158] See chapter 2, section 7.

[159] G. Maia – J. Vieira dos Santos, *MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and'Decentralised Finance'),* cit., 16.

In line with the approach taken by MiCaR, which introduces one general definition (crypto-assets) and three sub-definitions (e-money tokens; asset-referenced tokens, and utility tokens) our proposed definitions could be introduced as sub-definitions at the anti-money laundering level.

The Anti-money Laundering Package could distinguish between two types of tokens: decentralized and centralized tokens. In line with MiCaR's approach, there would be common rules applied horizontally to all crypto-assets and then a set of specialized rules to be applied to each category of tokens.

The two tokens could be labelled "decentralized tokens" and "centralized tokens"[160] and could be defined in the following way:

*"Decentralized token" means a type of crypto-asset that is not governed by any centralized entity and that allows users to access the network and exchange value in a peer-to-peer fashion".*

*"Centralized token" means a type of crypto-asset that is governed by a centralized entity that manages the access and/or exchange of value in the network".*

These two definitions would enable the creation of a new regulatory strand customized to the characteristics of decentralized crypto-assets. One that allows to address the peculiarities of the decentralized governance model these assets introduce and to adapt the previous intermediary-centred strategy to disintermediated environments.

We will further delve into how these duties can and should be customized to decentralized networks in the following chapters.

[160] This bipartition is also adopted by C. Leuprecht - C. Jenkins – R. Hamilton, *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency,* cit., 4, that respectively defines Centralized cryptocurrency as those that rely "*on a third-party administrator to issue the currency, maintain its blockchain and decide the rules for its use*" and Decentralized cryptocurrencies as those that "*use open source and math-based peer-to-peer blockchains that function without a central administrator*". In terms of content such a definition is similar to the one above proposed as it similarly distinguishes the two categories based on the governance structure; however, given the AML focus of our definition we have added together with the governance the two elements of access and value exchange management as these two elements are key in establishing the concrete ability of the network administrator to control value exchanges in the network. Also, in terms of structure we have used a similar phrasing as that employed by MiCaR to guarantee consistency with the other sub-definitions.

## 4. Outside of the Regulatory corral. The strange case of unique and non-fungible tokens (NFTS)

Having completed our analysis, there is one topic we still need to analyse as part of our excursus on the definition of crypto-assets: the exclusion of unique and non-fungible tokens from the regulatory perimeter of both the MiCaR and the anti-money laundering regulation.

Non-fungible tokens are one of the latest implementations of blockchain. They exploit blockchains' immutability and decentralization to create unique, unalterable, and programmable tokens that can be freely traded among the participants of the network.[161] On the one hand, blockchain's publicity and immutability safeguards the authenticity and uniqueness of the token while allowing anyone to verify it by, simply, accessing the ledger. On the other hand, blockchain's decentralization means that there is no single entity that can unilaterally modify or control the status of the token once it is created. The token can both be a digital representation of a physical or digital asset – as a work of art, a song, or a ticket to a concert – or solely exist as a digital token.[162] In this latter case, the value is determined exclusively by the characteristics intrinsic to the token, its rarity being an important factor.[163]

The exclusion of Non-Fungible Tokens from the anti-money laundering regulatory perimeter is particularly momentous for three main reasons.

[161] For a definition of NFT see EU Blockchain Observatory and Forum, *Demystifying Non-fungible Tokens (NFTs)*, 2021, 4, "*An NFT is a special type of digital asset or token that can be proved to be unique and not interchangeable with another digital asset token (i.e., fungible). This is why it is referred to as a "non-fungible token. Typically, the record of the uniqueness of the NFT exists as a cryptographic record on a blockchain, or distributed ledger, and can readily be viewed by anyone. While that is not always the case, NFTs are not just digitised information about an asset – they are a digital asset*"; Chainalysis, *The 2022 Cryptocrime Report*, cit., 30; for another definition see US Congressional Research Service, *Non-fungible Tokens (NFTs)*, Washington, 2022, 1, which provides the following definition of NFTs "*as unique and non-interchangeable units of data that can signify ownership of associated digital items, such as images, music, or videos*".

[162] A. Lennart, *The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum*, in *FinTech*, 1.3, 2022, 216; US Congressional Research Service, *Non-fungible Tokens (NFTs)*, cit., 2; M. Nadini – L. Alessandretti – F. Di Giacinto – M. Martino – L. Aiello – A. Baronchelli*, Mapping the NFT revolution: market trends, trade networks, and visual features,* in *Scientific reports*, 11,1, 2021, 6.

[163] For how NFTs can gain value see EU Blockchain Observatory and Forum, *Demystifying Non-fungible Tokens (NFTs)*, cit., 4

First, unlike the other exceptions provided by MiCaR, NFTs are the only category of assets not excluded because they are already regulated under other European legislations – as crypto-assets that qualify as insurances, or pension products[164]. This is a qualitative difference and is clearly underlined by the fact that the exclusion of "*crypto-assets that are unique and not fungible with other crypto-assets*" is dictated by a different paragraph, article 2, paragraph 3, than all the other exclusions, that fall under article 2, paragraph 4.

Second, all the anti-money laundering legislations currently under discussion, including the most recent Travel Rule Regulation[165], in their definition of crypto-assets only refer to the exclusion of paragraph three and not to those of paragraph four. This means that only NFTs will be excluded from the anti-money laundering regulatory perimeter, making this exception particularly momentous.

Third, NFTs present a high risk of money-laundering. Eminently, these tokens add to the pseudonymity, globality, and immateriality typical of crypto-assets, the absence of a clear market value typical of artworks and collectibles.[166] NFTs representing nothing more than an emoticon or a quite simple image have been sold for hundreds of thousands of euros due to their artificial rarity. The same goes for the emerging Metaverses' assets that are frequently incorporated through NFTs. How can you calculate the value of a digital piece of land, in a nascent digital world? With a market estimated between seventeen and forty-four billion dollars in annual sales,[167] NFTs risk to become (and have already partially become)[168] the next haven for criminal transactions.

Notwithstanding these characteristics, NFTs have been mostly considered as excluded from the purview of anti-money laundering compliance duties.

[164] For an analysis of MiCaR's exclusions see G. Maia – J. Vieira dos Santos, *MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and'Decentralised Finance')*, cit., 2.

[165] For an analysis of this Regulation see chapter 4 section 5.

[166] K. Busch, *Non-Fungible Tokens (NFTs),* Congressional Research Service, 2022, 18, "*NFTs may be particularly susceptible to money laundering since they are easily sent across geographic borders without incurring the financial or regulatory costs of physical shipping. Additionally, the price of digital art is highly variable, which enables money launderers to set the desired value with little historical context in which to compare prices*"; V. von Wachter - J. R., Regner – O. Ross, *NFT wash trading: Quantifying suspicious behaviour in NFT markets,* in *Financial Cryptography and Data Security. FC 2022 International Workshops,* 2022, 2.

[167] K. Busch, *Non-Fungible Tokens (NFTs),* Congressional Research Service, cit., 3.

[168] Chainalysis, *The 2022 Crypto Crime report,* cit., 29 e *ss*; Europol, *Policing in the Metaverse. What law enforcement needs to know,* 2022, 19; Financial Action Task Force, *Targeted update on implementation of the FATF standards on virtual assets and virtual asset,* Parigi, 2022, 20.

The Financial Action Task Force has been the first to rule on the topic. In its latest Guidance of October 2021, the FATF, while not modifying the definition of "virtual asset" introduced in 2018, provided a series of clarifications regarding its reach.

In particular, the Guidance states that:

> *"Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as a non-fungible tokens (NFT) or crypto-collectibles. Such assets, depending on their characteristics, are generally not considered to be VAs under the FATF definition".*[169]

The Guidance provides for two clarifications to this exclusion. First, following the substantial approach of the FATF legislation, the Guidance directs national authorities to look at the concrete function of the NFT rather than its tag. Thus, to be excluded are only those tokens that are *in concreto* unique and not fungible. Second, the fact that NFTs are not regulated as virtual assets does not exclude that they could fall under another category of regulated instruments.

The exclusion has been most recently confirmed by the FATF in its Targeted Update of June 2022.[170] However, the same Guidance has included NFTs among the most relevant market trends for money laundering purposes.[171]

Notwithstanding the above-outlined differences between the FATF's and the European approach, the MiCaR takes an identical stance with regard to NFTs as the FATF's Guideline. Article 2, paragraph 3, of the MiCaR excludes crypto-assets that are unique and not fungible for its purview.

The Regulation, like the FATF's Guidance, takes a very narrow approach to this exclusion, one aimed at only excluding those crypto-assets that are *in concreto* unique and not fungible.

As clarified, by recital 10:

[169] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 24.

[170] Financial Action Task Force, *Targeted update on implementation of the FATF standards on Virtual Assets and Virtual Asset Service Providers,* cit., 20.

[171] See also European Banking Authority, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, cit., 99 which lists non-fungible tokens among the emerging risks in the crypto-assets sector.

> *"The fractional parts of a unique and non-fungible crypto-asset should not be considered unique and not fungible. The issuance of crypto-assets as non-fungible tokens in a large series or collection should be considered as an indicator of their fungibility. The sole attribution of a unique identifier to a crypto-asset is not sufficient to classify it as a unique or not fungible. The assets or rights represented should also be unique and not fungible for the crypto-asset to be considered unique and not fungible. The exclusion of crypto-assets that are unique and not fungible from this Regulation is without prejudice to qualification of such crypto-assets as financial instruments".*

> *"This Regulation should also apply to crypto-assets that appear unique and not fungible, but whose de facto features or features linked to de facto uses would make them either fungible or not unique. In this regard, when assessing and classifying crypto-assets, competent authorities should adopt a substance over form approach, under which the features of the asset in question should determine the qualification, not its designation by the issuer".*

To underline the politically sensitive nature of this topic, this exclusion was the result of the negotiation as part of the legislative process. Indeed, the first draft of the MiCa Regulation, as proposed by the European Commission in 2020, did not include article 2, paragraph 3. The proposal only comprised a limited exclusion of unique and non-fungible tokens from certain specific duties provided for IPOs. In the previous version, NFTs were hence included in the definition of crypto-assets. It is only in the political agreement that they were excluded from the scope of the Regulation.

At the same time, it is the same MiCaR to demand, at article 142, paragraph 2, letter d), to the Commission to present, eighteen months after the entry into force of the Regulation.

> *"an assessment of the development of markets in unique and not fungible crypto-assets and of the adequacy of regulatory treatment of such crypto-assets, including an assessment of the necessity and feasibility of regulating offerors of unique and not fungible crypto-assets as well as providers of services related to such crypto-assets".*

The policy evolution, when it comes to Non-fungible Tokens, is, therefore, far from being over. Rather, the MiCaR seems to provide for a momentaneous exclusion to be reassessed in the near future.

# Part two

## The regulated entities

### How to find intermediaries in a disintermediated world

The previous part has analysed the object of the regulation, it is time to turn our attention toward its subjects – i.e., the covered entities. As examined in the previous chapter, the anti-money laundering regulation of crypto-assets has, so far, followed a strategy in line with the traditional approach. This means the regulation of intermediaries still constitutes the crux of the policy effort. These are required to identify and profile their customers and monitor their activity acting, in a sense, as proxies of Law Enforcement Authorities. Regulated entities in the crypto-world are under the same – except for very few exceptions – duties as traditional intermediaries.[172] The identification of the regulated entities is, hence, a fundamental element in the analysis of the policy strategy as it constitutes one of the key elements of differentiation compared to the pre-existing anti-money laundering regulation which, for the rest, fundamentally coincides with the traditional one.

The identification and definition of regulated entities in the crypto-world has experienced a marked evolution during the last decade. If the FATF Guidance of 2014 only identified one regulated entity, the MiCAR now lists ten categories of Crypto-assets service providers (CASPs). The definition of covered entity (VASP in the FATF lingo or CASP in the European one) has, hence, seen a progressive expansion.

[172] For a detailed analysis of the anti-money laundering duties applicable to crypto-assets, see the next chapter.

The expansion is due, on the one hand, to the growth and diversification of the crypto-market. As new implementations were introduced, and crypto-assets increasingly shifted from currency-like tokens to general-purpose digital assets, the number and type of players involved grew. On the other hand, during the last decade, the strategy of the policymaker has experienced a marked evolution. If, initially, the aim was mainly to fence the crypto-market – to limit any spill over effect in the traditional market – as time passed, the Regulator has become increasingly interested in the regulation of the crypto-assets market *per se*.

## 1. The first phase. Fencing the market

The crypto-assets regulatory strategy, with regards to the choice of the covered entities, can be divided into two fundamental phases.[173] During the first phase, the policymaker's main aim was fencing the crypto market through the regulation of its entry and exit points. Key examples of this approach being the 2015 FATF Guidance and, although only partially, the Fifth Anti-money Laundering Directive. During the second phase, the policymaker entered the market through the regulation of a growing number of intra-market operators. Key examples of this approach being the FATF Guidance of 2019 and 2021 as well as the Market in Crypto-assets Regulation.

Besides from these two, clear cut, phases, there is a third phase that can be glimpsed at the horizon. In this third phase, the policymaker seems to be pushing for an increasingly architectural regulation. Architectural regulation means a type of legislative action that regulates directly the technological infrastructure and not the actions of those who interact with it. This approach uses regulation as a means to shape the technological infrastructure in a form that facilitates the pursuance of policy goals. Examples of this trend are the imposition of the Travel Rule to self-

[173] This two-step approach is clearly outlined by the EBA that in 2014 (European Banking Authority, *Opinion on "Virtual Currencies",* cit., 44) advises for an immediate regulatory response followed by a long-term approach. The immediate regulatory response consists in addressing "*those risks can be mitigated that arise in the interaction between VC schemes and the regulated financial services sector (but not those that arise from activities within or between VC schemes). This would include risks of money laundering and financial crime*".

hosted wallets and the (for now only hinted) qualification of Decentralized Autonomous Organization's (DAOs) developers as VASPs in the 2021 FATF Guidance and MiCaR's proposal.

The present section will delve into the first phase. The following section will analyse the second phase with a special focus on the MiCAR and its connection with the upcoming Anti-money Laundering Package. The third phase will be analysed in the following two chapters.

## 1.1 The 2015 Financial Action Task Force Guidance

As we have detailed in the previous chapter, the first regulatory response to crypto-assets was essentially reactive. When the dark market Silk Road hit the global headlines in 2013, there was an urge for a strong and swift political response.[174] Shortly after, such a response was provided by the global policymaker in the field: the Financial Action Task Force. In 2014, the FATF published its Report on virtual currencies and, in 2015, its first Guidance. In this first policy strand, the FATF had overtly one purpose in mind: fence the crypto-market and avoid, or at least limit, spill over effects.

This was clarified by the same Guidance:[175]

> *"The focus of this Guidance is on the points of intersection that provide gateways to the regulated financial system (…) The risk assessment also suggests that AML/CFT controls should target convertible VC nodes—i.e., points of intersection that provide gateways to the regulated financial system—and not seek to regulate users who obtain VC to purchase goods or services".*

Eminently, the key risk identified for crypto-assets was that these assets could pollute the traditional financial market introducing ill-sourced funds.[176] The main idea was, then, to enclose

[174] A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, cit., 49.

[175] Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* cit., 6.

[176] European Banking Authority, *Opinion on "Virtual Currencies",* cit., 44, *"The immediate response specified above would 'shield' regulated financial services from VC schemes. As a result, the response would mitigate the risks arising from the interaction between VC schemes and regulated financial services*".

the market and police all its entry and exit points,[177] as intra-market transactions were deemed to generate a very limited risk. In line with this approach, the Financial Action Task Force solely focused on one category of covered entities: Virtual Currencies Exchangers.

These were defined as:

> *"a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third-party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts".*

The FATF's definition identified three key characteristics for an entity to qualify as an exchanger. First, the provision of the service professionally – as a business – irrespectively if in individual or corporate form. Second, the activity had to consist in the exchange of crypto-assets for another valuable asset. Third, the entity had to charge a fee for its activity.

In line with the abovementioned fencing approach, not all exchange activities were deemed relevant. Eminently, the Guidance restricted its purview only to those exchangers that engaged in crypto-to-*fiat* transactions, this way leaving crypto-to-crypto exchanges outside the regulatory radar.[178]

Besides the regulation of exchangers, the Guidance also left the door open for the inclusion of other types of entities that may have acted as points of intersection with the traditional market. In line with the fencing strategy, the Financial Action Task Force advised States to include "*any other types of institution that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system*".

[177] See also European Banking Authority, *Opinion on "Virtual Currencies",* cit., 6, "*The EBA also recommends that EU legislators consider declaring market participants at the direct interface between conventional and virtual currencies, such as virtual currency exchanges, to become 'obliged entities' under the EU Anti Money Laundering Directive and thus subject to its anti-money laundering and counter terrorist financing requirements*".

[178] See Financial Action Task Force, *Guidance for a risk-based approach Virtual Currencies,* cit., 7, "*Providers of VCPPS conducting activities which fall within the FATF definition of a financial institution are subject to the applicable FATF Recommendations. This includes convertible virtual currency exchangers where convertible VC activities intersect with the regulated fiat currency financial system*" and 9.

## 1.2 The Fifth Anti-Money Laundering Directive

The 2015 FATF Guidance was transposed by the European Union in 2018 with the introduction of the Fifth Anti-Money Laundering Directive. The Directive constitutes the first European legislation in the field of crypto-assets witnessing the relevance of financial flows control in this field. Notwithstanding three years had passed since the FATF's Guidance, and a new Guidance was in the pipeline, the Directive stuck quite strictly, even though not completely, to the FATF's initial approach.

The Directive - at article 1, paragraph 1, letter c) – introduced two categories of regulated entities: providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers.

The first category perfectly collides with the one recommended by the FATF. The Union, in line with the Guidance, stuck to the fencing approach and restricted the purview of the Directive only to crypto-to-*fiat* transactions, hence excluding all intra-market transactions (crypto-to-crypto).[179] In contrast, the second category constituted an original addition of the European legislator. Wallet providers were not mentioned by the Guidance and could not even be framed within the residual category of "*institutions that act as nodes with the traditional market*" as these offer an exclusively intra-market service – i.e., the custody of crypto-assets. The inclusion of wallet providers is, hence, a novelty introduced by the Union and one that hints at the upcoming legislative strategy that introduced an increasing regulation of intra-market players.

Here a brief digression is needed to understand what wallet providers are and their role in the crypto-market.

[179] In contrast, the FinCEN Guidance of 2019 extends the purview of the Bank Secrecy Act to any exchanger irrespective of whether it pursues crypto-to-crypto or crypto-to-*fiat* exchanges, see FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, 9th of May 2019, 13; this approach was criticized by the EBA in European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU*, cit., 36 that advised for an extension of the regulatory perimeter to also include crypto-to-crypto.

As detailed in chapter two, to hold and exchange crypto-assets there is no architectural need to use a third party or an intermediary. The user can autonomously generate a private and a public key and enter the market. However, the absence of a third party is a double-edged sword. On the one hand, it means there is no entity the user has to trust. Its crypto-assets are solely controlled by them. No bank failure, financial crisis, or fraud can deprive them of what they own (although the market value of the token owned can be affected by external events and price fluctuations). The flip side of full autonomy is full responsibility. The user has no resort if their crypto-assets are lost due to negligence or fraud. If the user loses or forgets their private key, there is nothing they can do to recover their crypto-assets.[180] It would be as if, by losing the password to a bank account, the owner would lose all the money they had therein deposited. The same goes in case of a cyberattack, if someone else gains access to a user's private key and sends money to its account (as it would happen with a cloned credit or debit card), no entity can offer a resort.

This characteristic of crypto-assets, paired with their growing value, caused the emergence of multiple entities that offered services to safely store the private key, in a certain way mimicking the activity of traditional banks: wallet providers. The type of services offered by wallet providers differ widely depending on the business model of the single provider.

The fundamental bipartition, in terms of business model, is between custodian and non-custodian wallet providers.[181]

A custodian wallet provider retains control over the funds of their customers.[182] There are two main business models a custodian can follow. First, the provider simply stores the private key of the customer. Instead of having a non-replaceable private key, the user has a (modifiable and, most importantly, recoverable) password that can be used to transact. If the password is lost, or for any

[180] European Banking Authority, *Report on Crypto-assets,* cit., 8. Since crypto-assets, and particularly Bitcoin, have gained an increasing value there have been multiple reports of people losing their private key and, hence, access to millions of euros. See R. Browne, *Man makes last-ditch effort to recover $280 million in bitcoin he accidentally threw out*, in *CNBC*, 15 January 2021, https://www.cnbc.com/2021/01/15/uk-man-makes-last-ditch-effort-to-recover-lost-bitcoin-hard-drive.html; N. Popper, *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes,* in *The New York Times*, 12 January 2021, https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html.

[181] FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, cit., 15, distinguishes among hosted and unhosted wallets; for an overview of wallet providers' business models see G. Hileman – M. Rauchs, *Global cryptocurrency benchmarking study*, Cambridge Centre for Alternative Finance, cit., 47- 65.

[182] European Banking Authority, *Opinion on "Virtual Currencies",* cit., 15; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 14.

other reason compromised, the user can always ask the wallet provider to replace it. Second, the provider can store the crypto-assets in their personal accounts, together with those of other customers. The entity has direct control of the funds and manages them according to the orders received by customers. The flip side of the coin of custodian wallet providers is that they reintroduce precisely those risks of intermediated markets that crypto-assets were created to bypass. Custodian wallet providers, as any bank in the classic market, can be hacked – as in the Mt. Gox case[183] – or can defraud their customers – as in the FTX case.[184]

To avoid the reintroduction of the trust dilemma, a token holder can choose a non-custodian wallet provider. These entities simply offer a means to safely store the private key.[185] Non custodians can provide cold wallets or hot wallets.[186] A cold wallet is one where the private key is stored offline. A hot wallet is one where the private key is stored online.[187] Non-custodian wallet providers only partially solve the issues connected with the use of crypto-assets. These provide a secure means to store the key and for a seed that replaces the private key and is easier to remember. However, they do not protect against loss as there is no third party to whom the private key is entrusted.

To simplify, we can assimilate custodian wallet providers to a bank and non-custodians to a provider of strongboxes.

The Fifth Directive encompasses among the regulated entities, only the first of the above-outlined categories: custodian wallet providers. These are defined – by article 1, paragraph 2, letter d-19) - as:

[183] Mt Gox was a Japanese exchanger and wallet provider, the largest in the market, that was the object of a cyberattack which resulted in the loss of nearly half a billion dollar worth of Bitcoin, for more info see J. Wagstaff, *Mt. Gox bitcoin debacle: huge heist or sloppy glitch?,* in *Reuters,* 28 February 2014, https://www.reuters.com/article/bitcoin-mtgox-heist-idUSL3N0LX2SP20140228

[184] FTX was one of the largest crypto exchangers that also acted as a wallet provider that filed for Bankruptcy in 2022 leaving hundreds of account holders stranded, for more information on the causes see K. Huang, *Why Did FTX Collapse? Here's What to Know,* in *The New York Times,* 10 November 2022, https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html. see also O. Fliche – J. Uri – M. Vileyn, *Decentralised" or "disintermediated" finance: what regulatory response?,* cit., 39. The mentioned cases are just two of the most popularized one but there are numerous other instances of failed exchangers in the last decades.

[185] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 14.

[186] European Banking Authority, *Report with advice to the Commission on crypto-assets*, cit., 9.

[187] European Banking Authority, *Report on Crypto-assets,* cit., 8; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 7.

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

The text of the disposition opens two interpretative avenues in terms of custodian wallet providers. Eminently, a literal reading of the Directive would restrict its purview solely to those providers that safeguard the cryptographic key of their customer (the first business model above detailed). This means that a literal reading of the law would exclude all those businesses that, while *de facto* custodian, manage their clients' funds directly and not by storing the private key. However, a more inclusive, teleological reading of the disposition may point towards the inclusion of any type of custodian wallet provider. Eminently, even though custodian wallet providers that hold crypto-assets in their accounts do not store their customers' private key, they still safeguard the crypto-assets to enable them "*to hold, store and transfer virtual currencies".*

This second interpretation seems to better reflect the purpose of the Directive: to regulate any CASP that retains control of their customers funds. Whether such control is exercised storing the private key or the crypto-assets is *in concreto* irrelevant. Most importantly, is irrelevant in terms of anti-money laundering risk: the relevant factor here is whether the intermediary controls the funds and can, hence, monitor the customer activity, not how it retains such control. This interpretation is also confirmed by the FATF's Guidance of 2019[188] which explicitly includes other types of wallet providers' business models stating that "*VA wallet providers, such as those that host wallets or maintain custody or control over another natural or legal person's VAs, wallet and/or private key(s)*".

Certainly, this interpretative dilemma underlines how the legislator should be careful regarding the level of specificity it wants to adopt when phrasing a technology-related disposition. Eminently, by being over-specific regarding the technological means to use there is always the risk to create an unintended lacuna.

### 1.3 The thorns in the side of the first regulatory strategy. Short- and long-term trends

[188] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit., 14.

With this first wave of regulations, the policymaker dips a toe in the crypto-water. The 2015 Guidance and the Fifth Directive provide a first response to the emerging issue, educate public stakeholders while inciting academic research, and send a message to the market that crypto-assets are not exempted from State's sovereignty. This first effort can, hence, be seen as a positive and needed development.

At the same time, certain criticalities emerge from this first approach. Such criticalities are both short-term issues but also highlight long-term problems that still characterize the sectorial regulation.

The fundamental and overarching criticality of the policymaker's approach can be condensed in two *loci* that characterize blockchain's architecture*:* disintermediation and decentralization.

First, is disintermediation. Particularly, it seems dubious whether focusing solely on intermediaries to regulate a technology and a market that makes of disintermediation its *raison d'être* is an effective choice.[189] If the intermediary-centred approach was fit for a fully intermediated environment it seems, at least partially, inefficient in a disintermediated one.[190]

The fallacy of the approach is acknowledged by the same policymaker. Recital 9 of the Directive clearly states:

*"the inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large*

[189] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 18, "*P2P transactions are not explicitly subject to AML/CFT controls under the FATF Standards. This is because the Standards generally place obligations on intermediaries, rather than on individuals themselves*"; B. Mesquita – S. Maranhao – J. Seigneur, *Enabling KYC and AML verification in DeFi service,* cit., 2.

[190] As underlined by O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 27, "*The first pitfall lies in trying to replicate the existing regulatory framework only and exhaustively, without taking into account the specific characteristics (and therefore the potential benefits) of DeFi. This tempting approach leads to restricting the focus of analysis to the identification of intermediaries to whom requirements should be applied –and there are in fact intermediaries in DeFi, although not necessarily at all levels*"; World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 7; World Economic Forum, *Decentralized Finance (DeFi) Policymaker Toolkit*, cit., 18.

*part of the virtual currency environment will remain anonymous because users can also transact without such providers".*[191]

At the same time, the approach is understandable, at least as a first reaction. Faced with a completely new technology, with a clear criminogenic potential, it is only normal that the first reaction is to resort to the previous strategy. What is certainly more questionable is maintaining the same approach going forward. Furthermore, while the crypto-assets' market was conceived as a decentralized and disintermediated way for individuals to transact, as detailed in chapter one, intermediaries have been gaining an increasingly central role. In this sense, extending the anti-money laundering regulation to these entities seems like a sensible choice. Namely, while it is true that peer-to-peer transactions remain a possibility, using intermediaries makes, especially exchange activities, much easier. It is, hence, important to police these players to guarantee they do not become large-scale crime facilitators.

Second, is decentralization. The extension of an intermediary-centred approach to a decentralized market makes it difficult to fit a decentralized organization into the classic concept of the firm. As analysed in chapter two, blockchain's decentralization enables the establishment of "headless", horizontal organizations that permit innovative forms of collaboration. Such autonomous organizations challenge the classic categories of management, investors, etc. A prime example of this trend is Decentralized Finance (DeFi)[192]. DeFi aims at substituting the highly centralized traditional financial institutions with decentralized, autonomous organizations rooted in smart contracts and based on peer-to-peer networks.[193] Dealing with such headless organizations, the legislator has been struggling to draw the line between regulated and unregulated and, most importantly, to ascertain on who should compliance duties, and related liabilities, fall.

Namely, if, from a macro-perspective, the system relies on intermediaries to control financial flows, from a micro perspective, it relies on the management (a form of intra-business intermediary) to guarantee the controls are applied by each firm.[194] Decentralized infrastructures have led the

[191] On a similar note, US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 34 "*the present reliance on centralized VASPs to comply with AML/CFT and sanctions obligations is not likely to sufficiently mitigate illicit finance risks associated with DeFi services*".

[192] On the role of DeFi in facilitating and enabling criminal activity see Chainalysis, *The 2022 Cryptocrime Report*, cit., 5.

[193] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 7.

[194] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 3, "*Regulating intermediaries is, indeed, the most common and simple approach to regulate financial activities.4*

regulator to take a "where's wally" approach which rely on the supposition that somewhere in the DeFi infrastructure there is probably (recognizing that it will not always be the case) an identifiable person, whether legal or natural, providing a service that would render them subject to compliance with Anti-money Laundering requirements.

This dilemma is a cross-cutting theme of blockchain regulation and one we will encounter further on in our analysis.[195] Suffice it to say for now, that, at this first stage of blockchain regulation, this was still a limited problem. Ethereum – and with it general use programmable contracts – was introduced in 2014 and it would still take a couple of years for DeFi and DAOs to catch on. We will, then, return to this problem in chapter five where we will delve into the relationship between Decentralized organizations and compliance duties.

Shifting now to a more nitty-gritty analysis of the strategy applied, the main fallacy of the fencing approach was underestimating the criminogenic potential of the crypto-market. This is from two main perspectives.

First, solely monitoring the entry and exit points to the crypto-market means intra-market transactions are left to the wild west. Without any control, criminals are free to layer their proceeds and blur the money trail so that the intermediary at the exit point may find it very difficult to ascertain the illicit source of the proceeds. This problem is magnified by the exclusion of crypto-to-crypto exchangers. Criminals can move their proceeds across different coins and, hence, ledgers, to reduce the relevance of blockchain transparency. This behaviour, known as "chain hopping" [196] has been proven to be used by money launderers and to be effective in hiding the source of ill-gotten funds.[197]

*Form a regulatory perspective, this means that fostering market efficiency, protecting investors, safeguarding financial stability and any other regulatory goal became much more complicated when confronted with crypto finance*".

[195] For an in-depth analysis see chapter 5 entirely devoted to the regulation of Decentralized Autonomous Organizations.

[196] A. Moiseienko – O. Kraft, *From money mules to chain hopping. Targeting the finances of cybercrime,* Royal United Services Institute for Defence and Security Studies, London, 2018, 40 – 41; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26, defines chain hopping as "T*he act of switching from one infrastructure to another, or from one digital asset to another, often in quick succession, in order to evade tracking attempts*"; TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023*, cit., 16.

[197] European Banking Authority, *Report with advice to the Commission on crypto-assets*, cit., 21; G. Forgang, *Money Laundering through Cryptocurrencies* in *Economic Crime Forensics Capstones*, 2019, 4, 12; Chainalysis, *The 2022 Cryptocrime Report*, cit., 20; Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,*

The risk is that, even when the individual does use an intermediary and all money laundering controls are carried out, the criminal source of the money will be so far away to be imperceptible. As the criminal activity happened too far down the chain of transactions.

Second, solely regulating the point of contact underestimates the potential for crypto-native activities to be used for money laundering. If, in the beginning, crypto was solely a coin, with time many other activities have flourished. Criminals can use such different implementations – as ICOs,[198] NFTs, DeFi – to invest their proceeds and launder money inside the market. Detecting money laundering then becomes exceedingly complex as the funds exchanged are the proceeds of such underlying legitimate activity with limited possibility of going back to the roots of the investment.

Finally, as merchants are excluded under the anti-money laundering legislation any purchase in crypto-assets falls out of the purview of the controls.[199]

In this sense, the strategy of the policymaker seems partial as it tries to create checkpoints in a market that has no fixed entry-exit points and underestimates the anti-money laundering risk connected to the crypto-market *per se*.

The last criticality of this first regulatory wave is that both wallet providers and exchangers offer a parallel non-regulated business model.

As mentioned above, custodian wallet providers are not the only option available. Non-custodian wallet providers can also be used to store tokens.[200] The peer-to-peer nature of crypto-assets makes their custody more similar to cash rather than traditional digital currencies. The individual has a choice on whether they prefer to store their cash in a safe – or under their mattress – or in a bank. Non-custodian wallet providers are explicitly excluded from the purview of the Directive. This is

London, 2020, 41; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 62 – 63.

[198] G. Forgang, *Money Laundering through Cryptocurrencies,* cit., 17.

[199] This risk is currently limited as the use of crypto-assets as a means of payment is reduced, however, were crypto to gain a more widespread adoption, it would constitute a fundamental blind spot, as underlined by US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 34, "*the ability to use virtual assets to pay for goods and services is increasing. While some merchants may use third-party services that have AML/CFT obligations, the growing use of virtual assets as payment for goods and services could decrease the role of centralized VASPs*".

[200] Out of the sample analysed by G. Hileman – M. Rauchs, *Global cryptocurrency benchmarking study*, cit., only 27 percent of wallet providers managed their users' private keys.

a sensible choice as the provider has, in this case, no control over the funds and simply provides a means to store them. However, it leaves opens the possibility for criminals to simply migrate from custodian to non-custodian options.[201] In response to this possibility, the legislator has, further down the road, suggested that self-hosted solutions – as peer-to-peer transactions or self-hosted wallets – could be deemed as automatically high risk.[202] We will return to this in the next chapter as this is a regulatory strand characteristic of the latest regulations and, in particular, of what we referred above as the Phase three legislations.

In a similar fashion as wallet providers, Virtual Currency Exchangers have a disintermediated twin: decentralized exchangers. With the term decentralized we do not necessarily refer to an exchanger that functions through smart contracts as a Decentralized Autonomous Organization. Rather, these exchangers are decentralized in the sense that they simply match supply and demand.[203] Most of them are similar to a Craigslist where people willing to sell crypto-assets post their offer and can be contacted by the buyer. The sale is, then, usually executed peer-to-peer outside of the website; even though some of these websites do charge a commission this is not the rule. Some commentators believe decentralized exchangers can be included within the scope of the Directive through an extensive interpretation.[204] However, this extension is not automatic, especially when such platforms perform this bulletin board activity not only for crypto-assets but for a wide array of goods. It is also questionable whether it is correct to burden such basilar services with demanding duties as those provided by the anti-money laundering legislation.

The Directive does not provide for a definition of exchanger, however, under the FATF definition it is uncertain whether decentralized exchangers would fall under the purview of the regulation.

[201] L. Haffke – M. Fromberger – P. Zimmermann, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, cit., 11.
[202] See in this sense the amending guideline by European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* Paris, 2023, 4 - 5 *"acknowledges that transactions with self-hosted addresses (…) may expose them to increased ML/TF risk"*
[203] European Banking Authority, *Opinion on "Virtual Currencies",* cit., 14. The topic of decentralized exchangers functioning as a DAO - or DEX – will be covered in chapter 5 of the thesis where the regulation of decentralized arrangements will be assessed.
[204] L. Haffke – M. Fromberger – P. Zimmermann, *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, cit., 10.

Namely, one of the three requisites to be qualified as an exchanger, under the Guidance, is to charge a fee for their activity.

The meaning of fee is key in identifying the regulatory perimeter. Eminently, even if the platform were to mandate a subscription fee for posting, this would not necessarily be enough. Eminently, the letter of the law requires a commission. Depending on the interpretation of the term commission the solution would significantly change. If for commission is meant a fee to be paid when the exchange is carried out and proportional to the exchange a subscription fee would, hence, not be enough.[205] However, if for commission is meant an economic gain connected with the users' activity, then a user fee may be sufficient.

Going back to the roots of the distinction we may propend for an interpretation rooted in the transaction model. Eminently, the possibility for control is rooted in the intermediation of the transaction. In this sense, exchangers that simply facilitate the encounter of two parties shall be excluded as they miss the concrete ability to control the transaction – and even the ability to tell if the transaction was ever carried out. However, if the transaction is carried out through the exchanger's system or is facilitated by them then the fee requisite becomes relevant. If the *ratio* of only regulating intermediaries that charge a fee is to impose costly compliance burdens based on economic gain, then any economic gain connected with the service should justify the imposition of controls. It seems hence reasonable in such cases to assimilate decentralized exchangers to the same regime as centralized exchangers.

## 2. The second phase. The Regulation of the Market

[205] In this sense see the EtherDelta case where the presence of a fee was considered a key characteristic in the evaluation regarding the qualification of the decentralized exchanger as a CASP as described by The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 87 – 88.

The year 2018 – with the amendment by the Financial Action Task Force of its Glossary[206] to introduce a new definition of virtual asset[207] and virtual asset service provider[208] – marks the end of what we have labelled "first phase" and the beginning of a new strategy for the anti-money laundering regulation of crypto-asset. The Glossary's amendment was followed by the publication in 2019 of a new Guidance by the FATF on virtual assets and virtual asset service providers.[209] The revised standards encompass five new categories of covered entities (so-called, Virtual Asset Service Providers) and mark the beginning of the era of intra-market regulation in the field of crypto-assets.[210]

The FATF provides two main explanations for its change in approach and the connected expansion in the number of covered entities.[211]

First, the introduction and continuous expansion of new services and technologies – as Anonymity-enhanced Crypto-assets (so-called privacy coins or AECs),[212] mixers,[213] etc. – that facilitate the obfuscation of the blockchain transaction trail and increase the anti-money laundering risk of intra-market transactions.[214] Second, the advent of new business models, in particular Initial

[206] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 6.

[207] For an analysis of this definition see the previous section.

[208] See the definition at the Financial Action Task Force's glossary, https://www.fatf-gafi.org/en/pages/fatf-glossary.html

[209] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*, cit.

[210] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 18 "*Countries should address the ML/TF risks associated with VA activities, both where those activities intersect with the regulated fiat currency financial system, as appropriate under their national legal frameworks, which may offer various options for regulating such activity, as well as where such activities may not involve the fiat currency financial system but consist only of "virtual-to-virtual" interactions (e.g., as in the case of exchanges between one or more forms of VA)*"

[211] See Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 6, "*the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows, as well as the emergence of other virtual asset business models or activities such as initial coin offerings (ICOs) that present ML/TF risks, including fraud and market manipulation risks. Further, new illicit financing typologies continue to emerge, including the increasing use of virtual-to-virtual layering schemes that attempt to obfuscate transactions in a comparatively easy, cheap and secure manner*"; Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* cit., 34.

[212] World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 8.

[213] B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 7.

[214] US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 17; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 298; I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 14.

Coin Offerings (ICOs),[215] that generate new criminal risks completely internal to the market. Through these newly introduced business models, financial crime (as fraud or market manipulation) can be perpetrated without any connection with the outer world – i.e., the traditional financial system. These two factors combined enhance, according to the FATF, the risk profile of intra-market transactions calling for a more active role of financial integrity within the market. The strategy of mere containment is not enough anymore as the market cannot (if ever) be controlled through the sole policing of its entry and exit points.

As mentioned, the Guidance of 2019 introduces five categories of Virtual Assets Service Providers (VASP), adding, hence, four new categories of covered entities.

A VASP is, under the new Guidance:

> "*any natural or legal person who is not covered elsewhere under the Recommendation and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) Exchange between virtual assets and fiat currencies; ii) Exchange between one or more forms of virtual assets; iii) Transfer of virtual assets; iv) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; v) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset*".

In line with the new approach, the Guidance expressly specifies that, in contrast to the restriction in scope imposed in 2015, the FATF standards include both providers that offer crypto-to-crypto and crypto-to-fiat services.[216]

To better clarify the scope and meaning of these newly introduced categories, the FATF published a third Guidance in 2021.[217] This Guidance is a key element in better understanding the concrete scope of the FATF's rules. Let's delve, then, into these new categories to assess their concrete features.

[215] A. Delivorias, *Understanding initial coin offerings. A new means of raising funds based on blockchain*, cit.; D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 665.

[216] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 14, due to the FATF's lexicon the Guidance uses the term virtual-to-virtual and virtual-to-fiat, however, to ease the understanding we use consistently throughout the text the term crypto.

[217] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit.

In general terms, the Guidance clarifies that the five categories of VASPs should be interpreted broadly with a functional, activity-based approach. The supervisor should, then, always undertake an independent analysis of the intermediaries' business model to autonomously evaluate whether the intermediary falls within one of the five covered activities.[218] This is of particular importance in the crypto-assets market considering the propensity of developers – mainly in order to intercept the hype of decentralization – of branding their products as DAOs, DeFi, etc. even in the absence of a truly decentralized model. It is, hence, crucial for supervisors to autonomously assess the business model so to understand the service provided and the level of concrete decentralization.[219]

In this sense, the FATF clarifies that, in contrast with the previous Guideline, the new one aims at covering nearly all intermediaries that act in the crypto-market. If the previous Guideline carefully circumscribed its purview, here the aim is to encompass any business that provides services to third parties, apart from a carefully demarcated list of excluded entities. This is clarified by the Guidance itself which states:

> *"Despite the many and frequently changing marketing terms and innovative business models developed in this sector, the FATF envisions very few VA arrangements without VASPs involved at some stage if countries apply the definition correctly".*[220]

Notwithstanding this ample approach, there are still certain services explicitly excluded from the purview of the anti-money laundering regulation: the providers of ancillary services that do not engage in the delivery or facilitation of any covered activity and the services that solely facilitate the functioning of the crypto-assets network.[221]

[218] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 24-25.

[219] In this sense also US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 3; European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 95, "*in case a person or a managing body can be identified, despite its qualification, the DeFi application shall be treated as a crypto-assets services provider and fall under the same AML/CFT obligations (…) DEFIs may be subjected to the application of the relevant rules covering crypto- assets on a case-by-case basis*".to

[220] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 30

[221] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 32.

The expression ancillary services identifies all those services that facilitate the functioning of the market without direct involvement in the management of the individuals' funds – examples being hardware wallet manufacturers, providers of unhosted wallets, cloud services, etc.[222] In the absence of any direct involvement in the underlying activity and in the management of the funds, the exclusion aims at not imposing an unreasonable burden on entities that simply provide the means for the market to function smoothly. The distinction between ancillary and covered activities becomes, however, increasingly blurred when it comes to entities that function in a decentralized fashion. A classic example being decentralized exchangers. In these cases, tracing the line between facilitation without management and direct involvement is a complex exercise. When the service is functionally very similar to that provided by a covered entity, defining ancillary activity is crucial to avoid surreptitious circumventions of the compliance duties. For this reason, as described in the following sections, the FATF has provided specific guidance on how to distinguish between covered and excluded services.

Services that facilitate the functioning of the network means those that are purposeful to the overall functioning of the network and not to the activity of one specific user. Decentralized networks, due to the absence of a central management body, rely for their functioning on the cooperative activity of the community. In contrast to centralized networks, where the ledger is owned by an entity that both provides the service and maintains/updates it, decentralized networks are not owned by anyone. This makes their update/maintenance a qualitatively different activity compared with the provision of services to individual users. Several autonomous entities – natural and legal persons – participate in the maintenance, update, and day-to-day functioning of the network. Within this category, we can include miners, core developers, and blockchain nodes. Some of these may pursue this activity for profit in a corporate form – as is the case for most miners nowadays – others may do it as a form of public service – as is usually the case for nodes. The main discriminating factor between these entities and the covered ones is that the service provided by facilitators is not directly connected with a single user. Rather it is directed to the functioning of the network as a whole and, hence, is only indirectly functional to the provision of services to single users. For instance, while it is true that miners provide a vital service to individual users, as they bundle their transactions in a new block and compute the hash permitting the confirmation of individual transactions, the service is only indirectly provided to the users. Namely,

[222] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 25.

mining is primarily functional to the operation of the network as a whole and is only indirectly beneficial to single users.

Having analysed the exclusions, let's now shift to the analysis of what is included. The starting point is the textual definition of VASP. Following the Guidance any covered entity must share three general characteristics, irrespective of the concrete activity pursued:[223] i) it has to be a natural or legal person; ii) it has to conduct the activity as a business, excluding, hence, entities that act occasionally or for non-commercial reasons. The activity has, hence, to be provided on a sufficiently regular basis and for business purposes; iii) the service has to be provided for, or on behalf of a third party, excluding, hence, all merely internal activities – as intra-group transfers or services.

Finally, the definition excludes from its purview any entity covered elsewhere under the Recommendations, making Virtual Assets Service Providers, as Virtual Assets, a residual category.[224]

If these are the general coordinates of the Guidance, let's now shift our focus toward the analysis of each of the five categories that make up the definition of Virtual Asset Service Provider.

### 2.1 Exchangers

The first activity enumerated by the Guidance is the provision of exchange services. Under the renewed approach these include both crypto-to-*fiat* (limb one) and crypto-to-crypto transactions (limb two), significantly expanding the scope of covered activities. To be qualified as an exchanger, the entity does not have to necessarily manage every element of the exchange but can play several

[223] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 25.

[224] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 25.

roles. As clarified by the Guidance, it can act either as *"a principal, as a central counterparty for clearing or settling transactions, as an executing facility or as another intermediary facilitating the transaction"*.[225]

This expansion is certainly welcome as it adjusts the regulation to the concrete risk factors of the market, addressing one of the main loopholes identified in the previous section: the absence of intra-blockchain controls which facilitated chain-hopping and intra-market frauds. Further, it rationalizes the policy approach by equating, in terms of compliance duties, activities that are qualitatively similar, as exchanges of *fiat* and crypto. Finally, compared with the previous definition, the one provided by this Guidance is less detailed and more activity-oriented. If the previous definition identified exchangers through a description of their business model, the current one solely focuses on the result of the activity – the exchange of crypto with crypto or *fiat* – irrespective of the means used. In a multifaced market like the crypto-one, where new business models emerge daily, this approach makes the definition better equipped to stand the test of time. Also, it permits to avoid that small twitches in the business model can allow to circumvent compliance duties.

Notwithstanding the clarification, the definition still leaves open several interpretative doubts. Two areas that are of particular relevance.

The first, and arguably most controversial, category is that of decentralized exchangers. With the term decentralized we do not refer, in this case, to services that function autonomously through smart contracts (so-called DEXes, which impact will be analysed in chapter five devoted to decentralized services). Rather we refer to exchangers that solely match the supply and demand of crypto-assets to, then, enable peer-to-peer exchanges.[226] In this sense, the exchanger is decentralized as it does not directly manage the trade of value but simply connects the two parties that then transact in a decentralized fashion. As abovementioned, the exclusion of such exchangers was already a matter of concern in 2015. The exclusion of these providers created a significant break in the fence the regulator was trying to build around the crypto market. At the same time, imposing compliance duties on a service that basically acts as a bulletin board for sales of crypto-assets without any direct involvement in the management of funds seemed excessive as well as a potential breach of the proportionality principle and risk-based approach. The solution adopted

[225] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 26.

[226] Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* cit., 14.

by the FATF in 2019 is to exclude all services that only act as a match-makers between buyers and sellers without any involvement in the custody or transfer of the assets.

Eminently, the Guidance states:

> "*Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and the provision of financial services associated with issuance will generally not be a VASP. For example, this may include websites which offer only a forum for buyers and sellers to identify and communicate with each other without offering, even in part, those services which are included in the definition of VASP".*[227]

The crux is, hence, the management of the funds. Only if the service manages, through custody or transfer, the customer's funds can it be qualified as a VASP. This choice seems to be proportionate considering the purposes of the regulation and the associated risk factor. Eminently, it is only through the concrete management of the funds that the provider can assess the risk factor of its customer and evaluate the associated anti-money laundering compliance duties.

A second contentious element, concerning the scope of the term exchanger, is connected with so-called crypto-kiosks or ATMs. Kiosks are machines, visually very similar to an ATM, that allow individuals to convert cash into cryptos and vice versa.[228] With classic ATMs the problem of compliance is virtually non-existent. The withdrawal or deposit of *fiat* is always connected with a bank account or other intermediary that will, in turn, be responsible for the controls. However, due to the structure of blockchain accounts, a crypto ATM can be used to send tokens to a self-hosted wallet. In such a case, the absence of an intermediary on either side of the transaction means that no one oversees it and applies the relevant controls. This begs the question of whether the owner of the ATM should be qualified as a covered entity *per se*. The risk is of particular relevance as ATMs allow for cash-to-crypto and crypto-to-cash transactions. This means that, if

[227] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 35; a similar approach is taken by the US FinCEN, see FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, cit., 24, "*if a CVC trading platform only provides a forum where buyers and sellers of CVC post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform), the trading platform does not qualify as a money transmitter under FinCEN regulations*".

[228] Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* cit., 19.

the crypto-asset is sent to a self-hosted wallet, not only there is no control on the crypto side, but that also the *fiat* side of the transaction is virtually unmonitored.[229]

At the same time, the occasional nature of such transactions and the same architecture of ATMs (based on human-to-machine rapid interactions) make it hard to implement controls. A blanket implementation of compliance duties could simply push kiosks out of business. The Guidance of 2019 does not take a clear stance on the point. ATMs are left in a grey area as they "may" fall within the definition of exchanger.[230] The choice is fundamentally left to National authorities as the Guidance states:

> "*Some jurisdictions may consider the use of VA kiosks (…) as an occasional transaction, whereby the provider or owner/operator of the kiosk and the customer using the kiosk transact on a one-off basis. Other jurisdictions may not consider such transactions to be occasional, with resulting consequences for CDD obligations".*[231]

Mind you, this does not mean that ATM transactions are completely out of the purview of anti-money laundering controls. Rather, if a jurisdiction decides to qualify exchanges through kiosks as occasional transactions, then – following Recommendation 10 - the related compliance duties are only triggered above a designated threshold. The threshold for crypto-assets is currently set at one thousand euros/dollars.[232] Hence, even when exempted under national law as occasional transactions, such exemption only applies to exchanges under the threshold.

To sum up, the Guidance expands the scope of the category of exchanger by adding crypto-to-crypto transfers and introducing a general, activity-based definition that focuses on the concrete management of the customer's funds by the covered entity.

[229] Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* 19.

[230] In contrast the US FinCEN expressly includes kiosks operators among the covered entities, see FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, cit., 18, "*An owner-operator of a CVC kiosk who uses an electronic terminal to accept currency from a customer and transmit the equivalent value in CVC (or vice versa) qualifies as a money transmitter both for transactions receiving and dispensing real currency or CVC*".

[231] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 49.

[232] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 40 – 41.

## 2.2 Transfer

The second category of services covered by the Guidance (third limb) are those that facilitate the transfer of crypto-assets. Transfer services, together with wallet providers (limb four), serve as an all-compassing category for any entity that provides funds management services within a certain coin. If exchangers cover most (if not any) intermediated transaction between markets (whether crypto or *fiat*), limbs three and four cover most (if not any) intermediated transaction within a certain blockchain. In conjunct, these two categories cover any service that provides static (wallet providers) and dynamic (transfer) intermediation with a certain coin market.

Transfer services are defined as:

> *"any service allowing users to transfer ownership, or control of a VA to another user or to transfer VAs between VA addresses or accounts held by the same user".*[233]

The Guidance further clarifies that covered transfers are not only the ones carried out on-chain (meaning between two blockchain accounts) but also the ones happening off-chain. This clarification is connected with a business model that has been adopted by a growing number of intermediaries[234] – especially wallet providers. As analysed in chapter two, the decentralization of blockchain means the transaction system is quite cumbersome. Transfers of crypto-assets take time and money, with costs growing in parallel with the price of crypto. To avoid such costs, certain intermediaries have started to pool all their customers' tokens in proprietary accounts and then manage individual accounts through a private ledger – as a traditional bank would do. When two customers of the same intermediary exchange crypto-assets, these transactions are registered off-chain – meaning there is no modification in the ownership on the blockchain ledger but only in the intermediaries' ledger. Such transactions may have been technically not considered as crypto transfers (as nothing is registered in the blockchain ledger). For this reason, the FATF clarified the

[233] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 26.

[234] A. Blandin et *al., 3rd Global Cryptoasset Benchmarking Study*, cit., 39-40; on the use of off chain transaction also by disintermediated arrangements see O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 14.

extension of compliance duties to any transfer irrespective of whether these happen on-chain or off-chain.[235]

Apart from this clarification, the definition of transfer services is quite straightforward covering any entity facilitating transfer of values between crypto-assets accounts or customers (in the case of off-chain transactions).

The inclusion of transfer services is also relevant as it addresses an important risk factor of the crypto-market: Mixers or Tumblers.[236]

These services are so-called privacy-enhancing services as they provide blockchain's users with the possibility of blurring the transaction trail associated with their coins.[237] As analysed, while pseudonymous, the blockchain is extremely transparent in terms of transaction trail.[238] All transactions are registered in a single, public ledger. This means that anyone can follow the money connected with a certain account. To address this privacy loophole, Mixers provide a means to blur the transaction trail and hamper traceability. To this end, these software filter and randomly reallocate a group of incoming transactions to target accounts, making it extremely difficult to match the sending account to the receiving one.[239] This way they break the link between sender

[235] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 26.

[236] G. Forgang,, *Money Laundering Through Cryptocurrencies*, cit., 16; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 17; Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* cit., 30; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, cit., 63.

[237] C. Berggren – J. Asplund, *Identifying and Analyzing Digital Payment Flows Regarding Illegal Purposes on the Internet: I Samarbete Med Cgi Och Finanskoalitionen*, Independent thesis advanced level, Linköping University, 2016, 26; M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 1.

[238] World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 8; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 298.

[239] See the definition of A. Jakubenko, et. al., *Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument,* in *KnE Social Sciences*, 3, 2, 2018, 48, "*A Mixer sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "commingles" this transaction with other user transactions, so that it becomes unclear to whom the user intended the funds to be directed*". See also, M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, cit., 2; for an example of mixer functioning see M. Möser – R. Böhme – D. Breuker, *An inquiry into money laundering tools in the Bitcoin ecosystem*, in *2013 APWG eCrime Researchers Summit*, 2013, 3.

and receiver address, hence, reducing the usefulness (in anti-money laundering terms) of blockchain's transparency.[240]

Privacy-enhancing technologies are not criminal *per se*, as account holders may use them to address legitimate privacy concerns. Nevertheless, these services have been heavily used by criminals.[241] Under the first policy wave, Mixers were excluded from the purview of the regulation as they did not provide exchange or asset management services. However, with the introduction of transfer services as covered entities, Mixers now, arguably, fall under the purview of the regulation as they technically intermediate the transfer of crypto-assets from one account to the other.[242] This is certainly a welcome addition as it closes a relevant loophole in the previous framework.

### 2.3 Safekeeping

The fourth limb of the Guidance extends the regulation to a category already familiar to the European anti-money laundering legislation: wallet providers. Like the Fifth Directive, the Guidance only encompasses custodian wallet providers excluding those providers merely offering software or hardware non custodian services – which are framed within the above-analysed category of ancillary services.[243]

[240] M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 3; Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* cit., 30; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 72-73.

[241] M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 4. For a very recent case we can refer to Tornado Cash, a decentralized mixer that was sanctioned by the US Department of Treasury (OFAC) for having laundered more than 7 billion dollars since its creation including 455 million dollars connected with the North Korean hacker collective Lazarus Group. For more information regarding the case and connected allegations see the press release by OFAC https://home.treasury.gov/news/press-releases/jy0916

[242] The Same approach taken was taken by the US FinCEN in 2019, see FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* cit., 19, "*An anonymizing services provider is a money transmitter under FinCEN regulations. The added feature of concealing the source of the transaction does not change that person's status under the BSA*".

[243] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 29, "*Firms which merely provide ancillary infrastructure to allow another entity to offer this service (…) will not normally satisfy this definition. Nor does this limb typically cover software developers or providers of unhosted*

At the same time, the Guidance sensibly widens the scope of the term custodian wallet provider compared to the preceding Union's approach. This expansion is carried out through a more expansive definition of safekeeping and also adding a second category of activities that fall under this limb: the administration of crypto-assets.

The first activity, safekeeping, is defined as the "*service of holding a VA or the private keys to the VA on behalf of another person*".[244] The FATF closes the textual loophole identified above, eliminating the distinction between providers that store the private key and those that directly store the tokens. Under this limb, any form of safekeeping, as long as it implies direct control of the tokens on behalf of a third party, is qualified as a covered activity. The second activity, administration, includes "*the concept of managing VAs for or on behalf of another person*". The main difference being, fundamentally, the aim of the service provided. With the former aimed at safekeeping and the latter at management.[245]

More in general, the FATF identifies one element as key in ascertaining whether an entity falls within or outside the regulatory corral: control. Covered entities under limb four are all those:

> "*that have the ability to exercise control over VAs (…) The term "control" should be understood as the ability to hold, trade, transfer or spend the VA. Parties that can use a VA or change its disposition have control of it*"[246]

The Guidance further clarifies that the control does not even have to be exclusive to qualify as a covered activity. The activity qualifies as covered even when the customer retains a certain level of control over their account – as in multi-signatory arrangements.[247]

*wallets whose functions are only developing and/or selling the software//hardware However, countries must look at individual facts and circumstances in applying the definition for specific cases*".

[244] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 29

[245] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 16.

[246] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 29.

[247] The Guidance clarifies that the control does not even have to be exclusive to qualify as covered activity, Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 30, "*As in the definition of "transfer", this does not mean the control must be unilateral. "Control" can include circumstances where keys or credentials held by others are required in order to change the assets disposition, such as multi-signature processes. The existence of a multi-signature model or models in which multiple parties must use keys for a transaction to happen does not mean a particular entity does not maintain control, depending on the extent of the influence it may have over the VAs*". For multi-signatory it is meant a type of custodian arrangement that only allows to transfer the coin with the use of two passwords. Usually, one of these passwords is held by the

The new definition, taking into account the multiple and continuously evolving business models existing in the market, moves away, in a similar fashion as the exchanger definition, from a business-model centred definition. The European definition of custodians as solely the entities holding the private keys is substituted by an expansive, activity-based definition centred on the concept of control. Under this definition, any business that exercises, even partial or non-exclusive, control over crypto-assets for or on behalf of a third party is qualified as a covered entity.

### 2.4 Participation in and provision of financial services related to an issuer's offer and/or sale

The last limb of the FATF's definition of VASP is aimed at addressing an emerging business model that wreaked havoc in the crypto-market since 2016: Initial Coin Offerings.

With prices of crypto through the roof, more and more individuals started to crave a piece of the crypto-cake. This demand has been met by an increasing number of crypto-projects. New tokens are marketed on a nearly monthly basis raising stellar amounts of money. One of the most common strategies to carry out such a crypto-offering is through so-called Initial Coin Offerings (ICO). An ICO consists in the issuance of a token in connection with a certain project (usually detailed by a white paper) as a means to raise early funding for the venture.[248] The buyer of the token gains specific predetermined rights (the coins may be similar to bonds or stocks or a mix of the two concepts) and the issuer accrues funds to finance its venture.[249] In the, at least initial, absence of any clear regulation, these offerings flourished, raising millions of euros for projects that many times didn't even have a line of code written, resulting in widespread fraud.[250] The

administrator/safekeeper and one by the owner, meaning that, to transact or dispose of the coins, both parties need to agree.

[248] P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, cit., 646.

[249] D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 666; P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, cit., 646

[250] See O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 16 example of a rug pull fraud.

Guidance of 2019 is the first attempt to regulate this practice through the imposition of anti-money laundering compliance duties.

Notwithstanding the focus of the limb is on ICOs, the definition does not directly cover the token's issuers. As clarified by the Guidance "*the sole act of issuing a VA, entirely on its own, is not a covered service under limb (v) of the VASP definition*".[251] The covered activity is, hence, the provision of financial services in the context of "*issuance, offer, sale, distribution, ongoing market circulation and trading of a VA*".[252] To be covered by anti-money laundering duties is, hence, not the entity issuing the token but the one that intermediates its sale and transfer.

The reason of this exclusion, which, as we will see, recurs also in the Union's discipline, is connected with the treatment of software developers. Software developers have been, up to now, considered excluded from the purview of compliance duties. The entity or person that simply creates an instrument, whether a crypto-asset or a Decentralized service, is not classified as a VASP.[253] This exclusion is in line with the technology neutral approach of the sectorial regulation that aims at policing intermediaries engaging in a certain activity and not the technology *per se* or its creators. Imposing compliance duties on a software developer would entail demanding them to design the technology in a certain fashion, this way directly regulating the technology. As further analysed, this hands-off approach seems to be partially changing in the last years. We will further delve into this topic in chapter five devoted to the regulation of decentralized entities and software developers.

[251] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 30.

[252] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 30.

[253] In this sense also European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 95 "*Another key concern also arise from crypto-assets exchange, lending or transfer services, activities normally offered by regulated crypto-assets services providers but made through decentralized or distributed application, often run on a decentralized ledger, with no legal or natural person with control or influence over it, often referred to as 'decentralised finance' (DeFi). There seems to be a broadly shared consensus among jurisdictions that DeFi applications should not be considered crypto-assets services providers if there is no identified body that can be held liable for their use*". For more on the regulation of decentralized arrangements and their developers see chapter 5.

To sum up, as long as the issuer is solely designing and launching the token, as Nakamoto did, no compliance duty will be imposed. In contrast, if the issuer is also involved in the sale and/or transfer of the issued tokens then it would qualify as a covered entity.

## 3. The Market in Crypto-assets Regulation

As with our previous analysis concerning the definition of crypto-assets, the last piece of legislation we will examine is the Market in Crypto-assets Regulation (MiCaR). From a policy strategy perspective, the MiCaR follows the approach of the 2019 FATF Guidance in significantly expanding the number of covered entities compared with the Fifth Anti-Money Laundering Directive.[254]

Specifically, the MiCaR introduces ten categories of covered entities – labelled Crypto-assets Service Providers or CASPs. The MiCaR not only enlarges the scope to all the activities defined as covered – exchangers, wallet providers, transfer services, and offerors – under the FATF's renewed definition,[255] but further expands the concept of CASP to include new types of business models. The result is a list of covered entities encompassing nearly any intermediary operating within the crypto-market.

Starting from the definition of Crypto-assets Service Providers, the MiCaR follows the FATF's model defining a CASP as any entity with three characteristics: i) is a legal person or any other undertaking; ii) conducts the activity as a business, hence, providing its services on a professional basis; iii) provides services to third parties.[256] To these three elements, the MiCaR adds a fourth

[254] As underlined by European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU*, Paris, 2020, 36, the definition of CASP provided by the Fifth Anti-money Laundering Directive was no longer in line with the FATF's Regulation; see also European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 100

[255] European Central Bank, *Opinion of the European Central Bank on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing,* cit., 14.

[256] See article 3, para 8, "*crypto-asset service provider' means legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis, and are allowed to provide crypto-asset services in accordance with Article 53".*

one that is directly connected with its substantive discipline: to qualify as a CASP the entity has to be allowed to provide crypto-asset services in accordance with the Regulation. Namely, the Regulation introduces an authorization process for any CASP that wishes to provide its services within the Union. We will further delve into this process in the following section.

In addition to these overarching characteristics, to qualify as a CASP, the entity must provide one of the covered services as enumerated by article 3, para 9, MiCaR. These services are:

> "*(a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for funds; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) placing of crypto-assets; (fa) providing transfer services for crypto-assets on behalf of third parties; (g) the reception and transmission of orders for crypto-assets on behalf of third parties; (h) providing advice on crypto-assets; (hb) providing portfolio management on crypto-assets*".

Crypto-asset Service Providers are not, however, the only regulated entities under MiCaR. In addition to CASPs, the Regulation provides for two additional categories of covered entities: the issuer and the offeror of crypto-assets. Both these entities are not classified as CASPs but are the object of a partially separate and customized discipline.

Let's then delve into these two additional categories. An issuer is defined as "*the natural or legal person or other undertaking who issues the crypto-assets*". An offeror is defined as a natural or legal person, or other undertaking, including the issuer, that offers crypto-assets to the public. An offer to the public is then defined as:

> "*a communication to persons in any form and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered, so as to enable potential holders to decide whether to purchase those crypto-assets*".

The Regulation, hence, breaks the issuance of a new crypto-asset in two fundamental moments, to which correspond two different entities: i) the technical design and issuance of the token – operated and managed by the issuer; ii) the offering of the token to the public – operated and managed by the offeror.

The first moment is loosely defined as the Regulation does not provide for a definition of issuance. We can, hence, infer that any activity consisting in the creation of a new type of token can be classified as issuance.

The second moment is more clearly demarcated as a specific definition of crypto-assets offering is introduced. The definition is an exact copy of the one already provided for the offer of securities to the public by article 2, letter d), of the Prospectus Regulation.[257] The similarity places crypto-assets offerings squarely within the purview of the larger European financial market regulation and underlines that the purpose of the legislator with MiCaR is to increasingly assimilate crypto-assets with any other classic financial instrument.

The indexes laid out by the definition for an entity to be identified as offeror are fundamentally three: i) there needs to be a communication (which can be carried out with any means); ii) the communication needs to be addressed towards more than one person, although not necessarily to the general public (as underlined by the use of the plural persons); iii) the communication needs to be complete enough to enable the recipient to make an informed choice regarding whether to buy the asset.

These two phases of the token issuance can be managed by the same entity (as the offeror can also be the issuer) or by two different entities. This depends on whether the issuer solely designs the token and launches its protocol or if they are also involved in its, *lato sensu,* commercialization.

While *prima facie* clear, tracing the line between mere issuance and offer will certainly be a complex exercise. Eminently, any activity of issuance does entail some form of communication as the developer has to, at the very least, gather enough contributors to initiate and maintain the network. Even a fully decentralized network as Bitcoin, required a certain organization for its launch. Nakamoto had to reach out to find core developers and early adopters eager to become nodes and

[257] Regulation of the European Union, 14th June 2017, n. 1129; the same goes, even though the similarity is less relevant considering the conciseness of the definitions, with the definition of issuer and offeror respectively defined by art. 3, lett. h and i; a part of the literature, as well as certain jurisdictions, had already argued in favour of the applicability of the Prospectus Regulation to Initial Coin Offerings, see D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 670, in favour of the introduction of an *ad hoc* regime P. Hacker – C. Thomale, *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, cit., 649.

mine the early blocks. When this outreach activity shall be deemed to have reached a level of sophistication sufficient to qualify as an offer will be a challenging interpretative exercise.[258]

Even though it is still early to conclude for any interpretative solutions, this problem is very similar to the (relatively) long-standing one concerning the regulation of software developers in decentralized arrangements. Eminently, the reason why issuers are differentiated in terms of regulation from offerors is that, in a decentralized arrangement an issuer can design a token without retaining any control of the latter. In cases as such, the issuer is a software developer rather than a business providing a service. The service is provided by the token – and/or the decentralized arrangement[259] – and not by the individual/s designing it.

Since the introduction of crypto-assets, the legislator has been struggling with the if and how of the regulation of such arrangements. To differentiate between true software developers – not covered by the anti-money laundering legislation – and service providers, the FATF developed a series of indexes. These indexes will most probably apply also to the issuer/offeror distinction. For a more detailed analysis of the topic, we refer to chapter five which delves into the regulation of decentralized autonomous organizations.

To sum up, the MiCaR introduces three categories of covered entities: the CASPs (formed by ten sub-categories), the issuer, and the offeror. For each category, the MiCaR provides for a registration duty as well as several other obligations aimed at safeguarding investors and guaranteeing the solidity of the providers operating within the common market.

The present analysis will be divided as follows. In the next section, we will analyse the ten categories of CASP introduced by the Regulation. We will then examine the authorization system introduced by MiCaR for CASPs, issuers and offerors. Finally, we will delve into the upcoming Anti-money Laundering Package to assess up to what extent it adopts the definitions introduced by the Regulation and how the (typically financial) regulation of MiCaR will translate into the Union's anti-money laundering framework.

[258] As underlined by H. Axelsen - J. Rude Jensen – R. Omri, *When is a DAO Decentralized?,* cit., 69, "*no DAO can start decentralized, as any project must be initiated by a small core team, bootstrapping development until the project matures and attracts open-source contributors*".

[259] It is important to keep in mind that the creation of a DAOs many times coincides with the issuance of a new token (usually on top of a pre-existing token) that is used to fund, vote, and administer the organization.

## 3.1 The definition of CASP

The definition of CASP adopted by MiCaR is largely rooted in the FATF's definition of VASP adopted with the 2019 Guidance. The similitude applies to the overall definition of covered service provider as well as to its single subcategories. A large part of our analysis developed for the Guidance can, thus, be applied to MiCaR's Crypto-assets Service Providers. However, the MiCaR also introduces new categories of regulated intermediaries hence further widening the policy reach.

Let's, then, analyse the definition of each category of covered entities as provided by the Regulation.

### 3.1.1 The custodian wallet provider

The first covered activity is a familiar one for the European anti-money laundering regulation: custodian wallet providers. Their activity is defined as:

> "*safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys*".

This definition adapts the previous one laid down by the Fifth Directive – that focused on the management of the private key – to the one adopted by the FATF.

First, the management of the private key is now not a core factor for the qualification as covered entity but only one of the possible business models. Second, safekeeping is placed side by side with a second activity: controlling. This addition underlines that the key factor to qualify as a covered entity is the notion of control. A covered entity will, hence, be any service provider that has control over crypto-assets belonging to a third party, either directly or through the management of their private key.

### 3.1.2 The platform operators and the exchangers

The second category is the trading platform operator. This is a very interesting one as it is directly relevant to our earlier discussion on decentralized exchangers. Eminently, the category of platform operator seems to be significantly broader than the pre-existing one of exchangers. The former being defined by MiCaR as:

> *"the management of one or more multilateral systems, which brings together or facilitates the bringing together of multiple third-party buying and selling interests for crypto-assets – in the system and in accordance with its rules - in a way that results in a contract, either by exchanging one crypto-asset for another, or a crypto-asset for funds".*

This definition makes no direct reference to the management or transfer of funds nor the collection of a fee by the intermediary. The only requirement laid down is that the interactions the platform facilitates should result (or be aimed at) the conclusion of a contract for the exchange of crypto or of crypto-to-*fiat* between third parties. This is precisely the business model we have described for decentralized exchangers: meaning platforms that do not directly manage the exchange of funds but rather facilitate the match of demand and supply. Up to now, these entities, as long as they did not manage the exchange of funds, were excluded from the purview of the regulation. However, MiCaR seems to, quite explicitly, expand its scope to platforms that simply facilitate the conclusions of contracts without any direct management funds.

This expansion is further confirmed if the third and fourth limb of the definition are considered. These limbs encompass the exchange of crypto-assets for funds and for other crypto-assets, defined as:

> *"concluding purchase or sale contracts concerning crypto-assets with third parties against funds (or other crypto-assets) by using proprietary capital"*

These two limbs precisely cover the business model of centralized exchangers that use own funds to exchange their customers' funds. The addition of these two separate categories for centralized arrangements, further points in the direction of an expansion of the regulatory scope towards decentralized exchangers. The width of this expansion will depend on how supervisors will interpret the expression "*in a way that results in a contract*". With the widest interpretation including platforms that simply facilitate the meeting of the will and the strictest requiring the facilitation of the conclusion and execution of the exchange contract.

At the same time, it is important to underline that MiCaR is not an anti-money laundering legislation. Hence, this extension and the interpretation of the aforementioned expression may be different when the category is applied to anti-money laundering. Eminently, as we have explained, the main reason why decentralized exchangers were excluded was that they had no overview of the transaction flows. Eminently, they simply act as bulletin boards for sellers and buyers. Precisely for this reason, the FATF, in its 2021 Guidance, drew the line between covered and excluded entities focusing on the management of funds. As long as the entity is not managing funds it is excluded from the purview of the Guidance. Now, while MiCaR pushes for a further expansion, these factors will still need to be taken into account when defining a covered entity to ensure compliance duties match the concrete risk factor. Namely, the mere creation of a marketplace is certainly relevant in terms of consumer and investor protection. However, the same activity is not necessarily pertinent to financial flows control. In the first sense, the marketplace does facilitate the encounter of supply and demand and, hence, has an understanding of the products offered. In the second sense, in the absence of direct management of the funds, the ability of the marketplace to assess anti-money laundering risk.

### 3.1.3 The provision of transfer services

The fifth category is the provision of transfer services, defined as:

> *"transfer, on behalf of a natural or legal person, crypto-assets from one distributed ledger address or account to another".*

This category is specular to the FATF's transfer services one although partially more restrictive. If the Guidance expressly extended its purview also to off-chain transactions, here the definition seems to restrict its applicability only to on-chain ones. Eminently, the Regulation clearly states that the transfer has to happen between two DLT addresses or accounts. This would cut out off-chain transactions that are carried out by the intermediary and recorded in its private, centralized ledger.

### 3.1.4 The provision of advisory services and portfolio management

The sixth category under MiCaR is the provision of advisory services. This activity is defined as:

> *"offering, giving or agreeing to give personalised recommendations to a third party, either at the third party's request or on the initiative of the crypto-asset service provider providing the advice, in respect of one or more transactions relating to crypto-assets, or the use of crypto-asset services".*

The analysis of the rest of the Regulation points to a definition of advice as mainly connected with financial advice provided in connection with investments in crypto-assets. Eminently, if the expression used by the definition is quite broad and could potentially cover other types of professional advice – as, for example, legal - the rest of the regulation consistently refers to the activity of facilitating the investment in crypto-assets and choosing an investment strategy.

This is further underlined by the association of advisors with portfolio managers as the two categories are regulated by the same article – article 73 MiCaR. Indeed, portfolio managers can be framed as a custodian version of financial advisors. These are defined as the entities that:

> *"manage portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more crypto-assets".*

If the advisor also holds control of their clients' funds can, hence, be classified as a portfolio manager.

The exclusion does not imply that legal advice concerning crypto-assets will be out of the purview of the anti-money laundering regulation. Rather, the latter will be covered under the pre-existing anti-money laundering duties for the legal sector.

### 3.1.5 The middlemen

The last macro-category covered by the Regulation includes all those businesses that act as bridges between the offeror of crypto-assets and the potential buyers.

These include: the execution of orders for crypto-assets, meaning:

> *"concluding agreements to buy or to sell one or more crypto-assets or to subscribe for one or more crypto-assets on behalf of third parties and includes the conclusion of agreements to sell crypto-assets at the moment of their issuance".*

Placing crypto-assets, defined as the:

> *"marketing, on behalf of or for the account of the offeror or of a party related to the offeror, of crypto-assets to purchasers".*

The reception and transmission of orders, meaning:

> *"the reception from a person of an order to buy or to sell one or more crypto- assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution".*

All mentioned activities can be assimilated to the FATF's one of: "*participation in and provision of financial services related to an issuer's offer and/or sale".*

## 3.2 The authorization system

Although not of direct relevance for anti-money laundering purposes, it is appropriate to sketch the content of MiCaR's regulation beyond the definition of crypto-assets and CASP. Eminently, due to its relevance for the market's regulation, the regulation will undoubtedly cross paths and influence the anti-money laundering regime. Specifically, one field where it will have a direct relevance is the registration of CASP. Eminently, Crypto-assets Service Providers are following the Fifth Directive under a registration duty. This regime will be partially substituted by the one provided by MiCaR.[260]

The core of MiCaR is the discipline of crypto-assets' issuance and offer to the public. To protect investors and reduce information asymmetries, a set of detailed rules are laid down regarding the who, when, and how of crypto-assets' issuance. To the issuance of crypto-assets are devoted Title II, III, and IV divided following the tripartition among utility, asset-referenced, and e-money tokens detailed in the previous chapter. A second strand of regulation lays down registration requirements for CASP aimed at guaranteeing *ex ante* compliance with relevant regulations as well, once the registration is granted, Union-wide operativity – through so-called passporting.

### 3.2.1 The offer of crypto-assets, other than asset-referenced tokens or e-money tokens

The first category to be regulated by MiCaR is a residual one comprising all crypto-assets that are not asset-referenced or e-money tokens. The issuance of such tokens is under a looser discipline compared with the other two categories.

To issue this first type of token or apply for admission to a trading platform the Regulation mandates three fundamental requirements: 1) be a legal person; 2) draft, publish, and notify to the competent authority a white paper; 3) comply with a set of minimum standards (act honestly, treat token holders fairly and equally, avoid conflicts of interest, etc.).

Key to this discipline is the regulation of the white paper.[261] The concept of a white paper is not new to the crypto-world. It is quite common for initial coin offerings, or any other token issuance,

[260] For a more detailed analysis on this intersection see chapter 4, section 4.

[261] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 17

to be accompanied by a white paper detailing the token's characteristics, the goal of the project, etc.[262] The problem that has arisen is that such white papers were frequently incomplete or inaccurate. This has caused an explosion of crypto-projects raising stellar amounts of money and then failing (due to fraud or incompetence). Attracted by the, seemingly magical, earnings of early adopters, investors flocked to crypto-projects and invested millions in tokens that were rooted in dreamy white papers without, in some cases, even a line of code written.

MiCAR addresses the problem by introducing a detailed regulation of the white paper. First of all, the white paper is explicitly mandatory for any issuance.[263] The white paper has to include a list of compulsory information - information about the offeror or the person seeking admission to trading, information about the crypto-asset project, information regarding the underlying technology – and warnings – including that the crypto-assets may lose their value in part or in full. The aim is to ensure the white paper provides investors with a complete picture of what they are buying (the white paper should be published on the issuers' website) and to force the issuer to only proceed to a public offering when the project is advanced enough to be able to draft a complete paper. It is for this same purpose that MiCAR regulates marketing communications.

The white paper also plays a role in facilitating the activity of supervisory authorities. Eminently, the white paper must be notified to the competent authority at least twenty working days before its publication together with a statement detailing where the token will be offered and the starting date of the public offer.

While the white paper has a function of protection for the investor, MiCAR also makes its notification a means to streamline crypto-assets offerings in Europe. The Regulation states that National law cannot require any *ex-ante* authorization, with the notification as the only requirement needed to proceed to an offering. Furthermore, it prohibits Member States from imposing "*any further information requirements, with regard to the offer of those crypto-assets or the admission of such crypto-assets to a trading platform for crypto-assets*".

These prescriptions are reinforced through the introduction of civil liability in case of non-compliance. When a white paper is not drafted in accordance with MiCAR, a "*a holder of crypto-*

[262] D. Boreiko – G. Ferrarini – P. Giudici, *Blockchain startups and prospectus regulation*, cit., 669.
[263] Exclusions under art. 4, para. 2.

*assets may claim damages from those persons or bodies for damage caused to her or him due to that infringement*", adding that "*any contractual exclusion thereof shall be deprived of any legal effect*".

### 3.2.2 The offer of asset-referenced tokens

The offer or admission to trading of asset-referenced tokens is under a more stringent discipline compared to the one detailed so far.

First of all, to offer an asset-referenced token the entity should be a legal person (with very limited exceptions) established in the Union and have received an *ex-ante* authorization by the home Member State – excluding smaller offers or offers only directed to qualified investors. This authorization is rooted in an evaluation of both the entity and the white paper. An exception to this double evaluation is introduced for credit institutions which only need to submit their paper for approval.[264]

Before proceeding to an offer, the issuer should submit an application comprising the white paper (which content largely overlaps with the one mentioned above) and a series of information regarding the issuer. With asset-referenced tokens, the evaluation of the National authority is not only *ex-ante* but also entails the entity *per se* (considering elements as the management body's repute, the cybersecurity framework, etc.).

After having received the application, the competent authority has twenty-five working days to communicate if the application is complete, sixty working days to adopt a fully reasoned draft decision (also based on additional information that can be requested during this time frame), the draft decision should be communicated to EBA, ESMA and the ECB (or the National Central Bank where outside the euro-zone) that have twenty working days to send a non-binding opinion, within twenty-five working days from the reception of such opinion the Authority should issue a final decision.

[264] Certain requirements are dictated also for credit institutions, see art. 15a.

Once granted, the authorization is valid for the entire Union.

To underline how crypto-assets regulation – especially when it comes to stablecoins – mixes technical and political considerations, among the grounds of refusal, and authorization's withdrawal, MiCAR explicitly includes (apart from the classic ones of individual and corporate non-compliance) a negative opinion by the ECB or the National Central Bank "*on grounds of (…) monetary sovereignty*".

The issuance of a parallel currency by the private sector, if diffused enough, may exclude the public authority from the management of the currency. While the Digital Euro[265], and other Central Bank Digital Currencies' projects worldwide constitute a "market answer" to this menace providing for a State-backed competitor to stablecoins, MiCAR delivers to the State a regulatory bulwark[266]. The demarcation of what a serious threat to monetary sovereignty is will then be up to Central Banks, and Courts to decide.

Asset-referenced tokens are under more stringent requirements also in terms of governance and organization. Of particular relevance are those concerning the reserve of assets, due to the specificity of stablecoin's business model. As mentioned, one of the methods a stablecoin can employ to maintain its value stable is by referring to another asset, currency, or basket thereof.[267] When the investor buys such tokens, the issuer buys an equivalent value (or a percentage) of the referenced asset. This guarantees the holder against fluctuation as they can always redeem their tokens against the value of the underlying referenced asset.

One of the main problems underlined in practice is a significant risk that issuers don't buy the reserves promised or overvalue them[268]. When a crisis hits (or any other event that triggers something comparable to a bank-run), the issuer is unable to honour its debts and millions, if not billions are lost.

[265] https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html

[266] on a similar note, art. 19b restricts asset-backed token too widely used as means-of-exchange.

[267] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 19, Financial Stability Board, *Regulation, Supervision and Oversight of" Global Stablecoin" Arrangements: Final Report and High-Level Recommendations,* 2020, 5.

[268] See the controversy regarding Tether's backing, New York Times, *The Coin that could wreck crypto*, 17th June 2022, https://www.nytimes.com/2022/06/17/technology/tether-stablecoin-cryptocurrency.html

To avoid this scenario MiCAR prescribes a series of rules to guarantee the formation and preservation of the reserves. Such measures entail prescriptions on the insulation of funds, the management of the liquidity risk, the reserves' custody, the connection between issuance/redemption and reserves, and mandatory independent audits (every six months). To further guarantee investors, MiCAR mandates issuers to draft a "recovery plan" to restore reserves and a "redemption plan" to guarantee orderly redemption of assets by holders (to be drafted within six months from the authorization and notified to the Supervisors).

### 3.2.3 The issuance of e-money tokens

For the issuance of e-money tokens MiCAR largely refers to the e-money Directive.[269] This reference encompasses the issuer (that can only be a credit or an e-money institution), the token (that qualifies as e-money under the meaning of the Directive) and in general the regulation of the token. Article 43, paragraph 1-b, explicitly makes Title IV MiCAR *lex specialis* with respect to the Directive stating: "*Title II and III of Directive 2009/110/EC shall apply with respect to e-money tokens unless otherwise stated in this Title of this Regulation*".

The main additions to the Directive's discipline are the key elements of MiCAR we have already underlined. First, the white paper for which a notification procedure and not an approval one is prescribed. In this sense, e-money tokens follow the same discipline as the first category of token we have analysed, with a notification twenty days prior to the publication and a prohibition to impose an *ex-ante* approval procedure. Second, reserve and redeemability. E-money tokens can only be issued at par with the reserves and must guarantee immediate and free redeemability. MiCAR also extends to e-money tokens the duty to draft a recovery and redemption plan.

### 3.2.4 Significant asset and e-money tokens

[269] Directive of the European Union, 16th September 2009, n. 110.

For both asset-backed and e-money tokens, MiCAR introduces a separate category: the significant token. The discipline is mostly similar for the two tokens. The classification is done by the EBA, after a consultation procedure, based on a series of criteria (number of holders, number, and value of transactions, international usage, etc.). The classification can also be requested by the issuer. In this case, they need to prove they are likely to meet the abovementioned criteria shortly after the issuance.

The classification as significant shifts the supervisory responsibilities from National authorities to the EBA. Due to the width of the services provided, issuers of significant tokens are also under additional requirements, in terms of risk management, competition, stress tests, etc.

### 3.2.5 Crypto-assets service providers

The last piece of MiCAR's infrastructure is the regulation of CASPs.

MiCAR introduces an authorization procedure mandatory for any CASP that provides services, even if remotely, in the Union's market (safe for a series of categories of providers that are under a notification regime).[270]

To lawfully operate CASPs must be legal persons or other undertakings and must have received authorization in the host Member State. The related application must contain a list of information detailing the CASPs governance structure, activity, management, and so on. Within forty days from the reception of the application, the National Authority, after having completed a number of controls, must adopt a reasoned decision.

The authorization is not general, rather it only applies to one or more specific services that must be detailed in the application. Once obtained the authorization, the CASP is allowed to provide its

[270] See art. 53a MiCaR.

services throughout the Union without the possibility for other Member States to require additional authorizations.

Apart from the authorization procedure, CASPs are under very similar behavioural and organizational duties as issuers (honesty, transparency, prudential, and governance requirements). Furthermore, MiCAR introduces additional provisions for specific services – such as safekeeping, trading, and exchange.

Also, concerning these entities, MiCAR introduces the concept of significant CASPs. Meaning those services that have more than 15 million active users *per annum*. This denomination does not shift the supervisory duties at the Union level, as with issuers, but rather introduces a monitoring duty by the European Securities and Market Authority (ESMA) regarding the activity of National Supervisors.

### 3.3 The AML Package

As anticipated in the previous section, the relevance of the MiCaR for our analysis is essentially indirect. The Regulation is not, *per se,* an anti-money laundering legislation. However, the definitions introduced by MiCaR are deemed to become the gold standard for the European regulation of crypto-assets irrespective of the field.

It is to this end that the upcoming Anti-Money Laundering Package refers to both MiCaR's definition of crypto-asset and Crypto-asset Service Provider when defining its scope. Therefore, MiCaR's definition of CASP will, as the definition of crypto-assets, become one of the pillars of the future sectorial regulation.[271] However, unlike the definition of crypto-assets, which has been translated into the Package without any modification, for the regulated entities the transposition has only been partial. It is, hence, necessary to briefly delve into the text of the Anti-Money

[271] European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities,* cit.

Laundering Package, and most importantly of its Regulation, to delineate up to what extent the MiCaR will be relevant for money laundering purposes.

But first, let's cursorily introduce the Anti-Money Laundering Package.

The "Anti-Money laundering and countering the financing of terrorism legislative package"[272] is an ambitious proposal presented by the European Commission in July 2021. The package is the outcome of a reflection started in 2019 as a result of a series of high-level money laundering cases that rocked the European financial system.[273] Following these scandals, the Commission published a Report[274] analysing the cases and a Communication laying down the key weaknesses of the system that had led to the associated failures.[275] This analytical work resulted in an Action Plan, published in May 2020, for the modernization of the Union's Anti-Money Laundering Framework.[276] The Action Plan identified six pillars for the amelioration of the present system: *"1) Ensuring the effective implementation of the existing EU AML/CFT framework; 2) Establishing an EU single rule book on AML/CFT; 3)Bringing about EU level AML/CFT supervision; 4)Establishing a support and cooperation mechanism for FIUs; 5) Enforcing Union-level criminal law provisions and information exchange; 6) Strengthening the international dimension of the EU AML/CFT framework*"

In line with the action plan and with a view at implementing the abovementioned pillars, the Commission presented, one year later, the Anti-Money Laundering Package. The Package is composed of four legislative instruments: the First Anti-Money Laundering Regulation, the Sixth Anti-Money Laundering Directive, the Regulation for the institution of a European Anti-Money

[272] For further information see https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en

[273] H. Koster, *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework* in *Journal of Money Laundering Control,* 2, 2020, 383; for an analysis of such scandals and the connected possible regulatory responses see A. Minto – N. Skovmand Rasmussen, *Approaching the Danske Bank Scandal in a "Tragedy of the Commons" Perspective: Implications for Anti-Money Laundering Institutional Design and Regulatory Reforms in Europe,* in *European Company and Financial Law Review,* 19/2, 2022.

[274] European Commission, *Report from the Commission on the assessment of recent alleged money laundering cases involving EU credit institutions, (COM/2019/373 final*), 2019; H. Koster, *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework*, cit., 380.

[275] European Commission, *Communication from the Commission - Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework (COM/2019/360 final)*, cit.; for a detailed analysis of such fallacies see also European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU*, cit.

[276] European Commission, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (C/2020/2800), OJ C 164*, 2020.

Laundering Authority, and the Regulation on the implementation of the travel rule in the field of crypto-assets (analysed in the following chapter).

The main purpose of this Package is the acceleration of the harmonization, in the area of money laundering prevention, both in terms of legislation and enforcement.[277]

From the former perspective, the Package provides for the substitution of the current Fifth Anti-Money Laundering Directive with the First Anti-money Laundering Regulation. The crux of the sectorial regulation will, hence, shift to a directly applicable, uniform legislation that will guarantee homogeneity across the bloc.[278] While the Package still provides for a Directive – the Sixth Anti-money Laundering Directive – [279] this solely covers ancillary fields as risk calculation, cooperation among FIUs, etc. The core areas – as the identification of the regulated entities, reporting obligations, compliance duties – will all be covered by the upcoming First Regulation. This will constitute a seismic shift as it will deprive Member States of the leeway they have been granted so far and provide for a single rule book across the entire bloc.

From the latter perspective, the Package introduces a new European authority tasked with centralized supervision: the European Anti-money Laundering Authority (AMLA). Eminently, one of the main shortcomings identified as the root cause of the financial scandals analysed by the Commission' report was precisely the lack of proper supervision, especially in cross-border

[277] See European Commission, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, cit., 2, "*there is growing consensus that the framework needs to be significantly improved. Major divergences in the way it is applied and serious weaknesses in the enforcement of the rules need to be addressed*"; see also, Proposal for a Regulation of the European Union, 20th July 2021, n. 0239, "*The need for harmonised rules across the internal market is corroborated by the evidence provided in the 2019 reports issued by the Commission. These reports identified that whereas the requirements of Directive (EU) 2015/849 are far-reaching, their lack of direct applicability and granularity led to a fragmentation in their application along national lines and divergent interpretations. This situation does not allow dealing effectively with cross-border situations and are therefore ill-suited to adequately protect the internal market. It also generates additional costs and burdens for operators providing cross-border services and causes regulatory arbitrage*"; European Banking Authority, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, cit., 14.

[278] See European Commission, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, cit., 4, "*EU AML/CFT legislation needs to become more granular, more precise and less subject to diverging implementations. Certain additional requirements imposed by Member States when transposing AML Directives might however contribute to a stronger AML/CFT framework and could be integrated into the future EU rulebook. To limit divergences in the interpretation and application of the rules, certain parts of the AMLD should be turned into directly applicable provisions set out in a Regulation*".

[279] Proposal for a Directive of the European Union, 20th July 2021, n. 0250.

operations.[280] To this end, the introduction of a European Supervisor constitutes a fundamental step for the correct enforcement of the anti-money laundering compliance duties.

As stated by the Commission:

> *"EU's AML/CFT framework is only as strong as its weakest link, and failings in one national competent authority create risks for the whole of the Single Market. The EU as a whole suffers financial, economic and reputational damage as a consequence".*[281]

The European supervisor will not substitute but rather supplement and integrate National ones so to guarantee a common minimum level of enforcement across the bloc.

To sum up, the Anti-money Laundering Package is a bundle of legislations presented by the Commission in 2021 and deemed to be introduced in 2024. The main purpose of the Package is to further harmonize the rules and their enforcement at the Union's level.

### 3.3.1 The Anti-money Laundering Package and Crypto-assets

If the overarching goals pursued by the Package are those mentioned above, the latter also aims at adjourning the European legislation to the latest Guidance coming from the FATF. Specifically, one of the areas where such an update is urgently needed is the regulation of crypto-assets. The restrictive approach taken by the Fifth Directive is no longer in line with the FATF's standards post-2018 and, more in general, with the risk perception associated with the crypto-market.

As stated by recital 11 of the Anti-money Laundering Regulation:

> *"Directive (EU) 2018/843 was the first legal instrument to address the risks of money laundering and terrorist financing posed by crypto-assets in the Union (…) Due to rapid technological developments and the advancement*

[280] European Commission, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, cit., 6.

[281] See European Commission, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*, cit., 6.

*in FATF standards, it is necessary to review this approach. A first step to complete and update the Union legal framework has been achieved with Regulation (MiCaR), which set requirements for crypto-asset service providers wishing to apply for an authorisation to provide their services in the single market. It also introduced a definition of crypto-assets and crypto-assets services providers encompassing a broader range of activities. Crypto- asset service providers covered by Regulation (MiCaR) should also be covered by this Regulation, to mitigate any risk of misuse of crypto-assets for money laundering or terrorist financing purposes".*

When it comes to crypto-assets regulation, the key piece of legislation is the Regulation. Eminently, it is the Regulation that identifies the list of covered entities and, hence, is the main *locus* of the present analysis regarding covered entities.

Specifically, the Regulation, at article 3, paragraph 3, letter g), includes Crypto-assets Service Providers among the regulated entities, eliminating the previous references to the two distinct categories of exchangers and wallet providers. Article 2, paragraph 14, then, defines Crypto-asset Service Provider as "*a crypto-assets service provider as defined in Article 3(1), point (8) of Regulation (MiCaR) where performing one or more crypto-asset services as defined in Article 3(1) point (9) of that Regulation*". The definition is, hence, completely symmetrical to the one provided by MiCaR.

There is, however, a key difference in terms of regulated entities between MiCaR and the Regulation. The latter, nor any other legislations of the Anti-money Laundering Package, does not refer to two categories of covered entities under MiCaR: offerors and issuers. As mentioned above, these two categories do not fall under the umbrella of Crypto-assets Service Providers. Rather, they are separate regulated entities. The lack of any reference to them means their exclusion from the anti-money laundering regulatory purview.

This does not mean that any and all activities connected with the issuance of crypto-assets are outside the anti-money laundering purview. As underlined in section three-one-five, there are several activities connected with token offerings – marketing, reception and, placing of orders – that do qualify as Crypto-assets Services under MiCaR. However, the mere act of issuing a token will not fall under the umbrella of the Bloc's compliance duties. The choice of excluding issuers is, after all, in line with the FATF's Guidance of 2021. As we saw, also following that Guidance, solely the activities facilitating an issuance fall under the umbrella of the Regulation and not the issuance *per se.*

If issuers are certainly excluded from the anti-money laundering purview, the same does not apply to offerors. Eminently, the category of offerors is introduced by MiCaR as an overarching one that supersedes the micro-categories of CASPs. However, even if offerors are excluded from the Anti-money Laundering Regulation, most of the actions they will have to execute to carry out an offer will qualify as covered activities. Eminently, in line with the FATF's take on the matter, the Regulation excludes only the mere issuance not accompanied by any subsequent commercial activity. In contrast, an issuance that resolves in commercial activities – as marketing, placing, and taking of orders – will qualify as a covered activity.

Between regulated and unregulated entities there is, hence, a fine line. To fall outside the regulatory corral the issuer needs to abstain from any form of subsequent commercial activity.[282] Such an exclusion seems reasonable if an intermediary-centred approach is taken: mere issuers do not intermediate exchanges of value, hence, are not intermediaries. Rather, issuers are software developers who create and launch a network/token without retaining control over the latter. However, if we look beyond the traditional approach, the role of issuers could be valorised in a different light. As designers of autonomous systems which generate relevant financial risks, pre-launch, design duties could be customized to them. Hence, while with issuers a mere extension of the pre-existing duties may be inappropriate, new and customized duties may be devised to guarantee *ex-post* compliance. In sum, the regulator correctly excludes issuers from applying controls envisioned for intermediaries. However, such an exclusion should not be complete. Different and customized duties should be provided for issuers taking into account their role as designers of autonomous software. The structure of such duties is the object of chapter five which reflects on how such an *ex-ante* regulation could be devised.[283]

The Anti-money Laundering Package is the last piece in our legislative journey. Throughout this Part, we have outlined how the legislator has identified new intermediaries in the, seemingly disintermediated, crypto-asset market. Now that the object and subjects of the sectorial regulation have been identified, it is time to critically evaluate its content. After a brief conclusion in the next

[282] For further reflections concerning this distinction between issuer and offeror see section 3 of the present chapter.

[283] See section 2.4 of the present chapter and section 3 of chapter 5. A much stricter exemption is applied in the US by the FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, cit.

Part, the following chapter will do exactly that by delving into the content of the anti-money laundering duties and how these adapted to crypto-assets.

# Part Three

## Final Remarks

The present chapter has analysed how the legislature has framed the object and the subjects of the anti-money laundering regulation in the crypto-assets arena. We have seen how the strategy, the definitions, and the underlying principles have changed during the last decade.

The path has started, back in 2014, with a currency-centric, general definition of crypto-asset and a single regulated entity – i.e., exchangers; we now have a technology-specific definition and a multitude of covered entities encompassing nearly any centralized activity carried out in the crypto-space. Having abandoned the idea of simply containing, fencing the market, the regulator has adopted an increasingly hands-on approach. New categories have been introduced, and crypto-assets have been gradually assimilated to traditional financial instruments.[284]

The *fil rouge* of this legislative path is the quest for customization. As the market evolved, the legislator has been faced with the need to provide for increasingly detailed duties customized to the market. At the same time, such customization seems to have lacked a true capacity of going beyond the traditional regulatory strategy.

In terms of definition, the legislator seems to have missed the key differentiating characteristics of crypto-assets and blockchain technology: the disintermediation of digital interactions. It is in disintermediation that the crux of the crypto-risk dwells. The provision of an all-encompassing definition that equates centralized and decentralized tokens constitutes a missed opportunity for

[284] E. Martino, *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* cit., 13.

concrete customization. The MiCaR's abandonment of a purist vision of technological neutrality is certainly a welcomed innovation. However, if the intentions were good, the execution fell short.

There is, nonetheless, still time to steady the boat. The upcoming introduction of the Anti-money Laundering Package provides an opportunity to adjust the overarching definition and customize it to the concrete risk generated by crypto-assets. Through the introduction of the two proposed sub-definitions of centralized and decentralized token, the Package can safeguard the overarching definition while laying the foundations for a tailored, risk-based approach.[285]

In terms of covered entities' identification, the legislator has also maintained a traditional approach. An approach that focuses on centralized intermediaries and traditional compliance duties. This strategy is only partially valid: the crypto-assets market has known a certain degree of centralization, and it is only fair such intermediaries are under similar anti-money laundering duties as other traditional centralized intermediaries.[286] At the same time, intermediary-centred regulations ignore the hard questions. The regulation of decentralized organizations and networks, the role of software developers, and compliance-by-design, the treatment of blockchain information are all themes that have been dodged by the current policy framework.

These themes have not, however, been overlooked because of ignorance. As demonstrated by the discussion during MiCaR's legislative process regarding the qualification and regulation of decentralized autonomous organizations, the regulator is acutely aware of these issues. However, it has so far preferred not to address them directly.

The overarching critique that can be moved is, hence, that the legislator has lacked the political will and creativity to overcome its previous approach and devise innovative solutions. The intermediary-centred strategy has simply been extended from traditional finance to crypto-assets. If this approach is partially correct when it comes to the centralized-side of crypto-assets, it does not hold for its most innovative elements: decentralized and disintermediated organizations and transactions.

[285] See Chapter 3 Part 1 Section 3.

[286] See the comparison between the business model of crypto-lenders, stablecoins issuers and traditional banks of G. Gorton – J. Zhang, *Bank Runs During Crypto Winter*, cit., which advocate for a same activity same regulation approach.

Blockchain modifies the architectural postulates underlying digital transactions on which the anti-money laundering strategy has been built upon. The legislator cannot just ignore such a paradigm shift. As detailed in the following two chapters, there are initial signs that this approach is slowly changing as the criminal risk connected with decentralized arrangements and disintermediated transactions is forcing the hand of supervisory and enforcement authorities.[287] However, an overarching regulatory framework is needed to guarantee that enforcement does not thwart individual freedoms and foster legal uncertainty. Such a regulatory framework cannot but start from the delineation of clear definitions that create distinct legal categories and distinguish between classes that present different risks.

[287] See chapter 4 concerning the use of blockchain analytics tools and chapter 5, in particular, the discussion concerning the Tornado Cash case.

# Chapter Four

## The Anti-money laundering compliance duties

### Same old, same old?

## 1. Introduction

The previous chapter has analysed the object and the subjects of the regulation. The present chapter will delve into its content. To this end, it will analyse the anti-money laundering compliance duties with a special focus on crypto-assets' regulation.

So far we have outlined how the legislator, at the FATF and Union level, has framed the categories of crypto-assets and crypto-asset service provider (CASP). The present chapter will delve into how, and up to what extent, the concrete anti-money laundering compliance duties have been applied and adapted to the two above-outlined categories. It will also delve into how blockchain has partially modified the way supervised and supervisors approach compliance. It will examine how the transparency of the blockchain ledger has prompted the development of analytics tools that allow a much deeper analysis of the customer and the transaction patterns compared to traditional monitoring infrastructures.

The chapter is structured as follows. The second section will delve into the fundamentals of the anti-money laundering legislation. It will offer an overview of what money laundering compliance duties consist of. The third section will analyse how such duties have been extended to the crypto-assets market from a legislative and regulatory perspective. The fifth section will analyse the registration duty imposed on crypto-assets service providers and its coordination with the upcoming regime introduced by the MiCa Regulation. The sixth section will delve into the upcoming European Travel Rule Regulation.[1] The seventh section will focus on blockchain analytics tools to explore their impact on the implementation of compliance duties and on the overall infrastructure of financial supervision.

## 2. The Anti-money Laundering Compliance Duties. A recap

The first source for the analysis of anti-money laundering compliance duties are the Forty Recommendations[2] published by the Financial Action Task Force. The Recommendations (also known as FATF Standard) are the backbone of the sectorial regulation as they lay down the minimum common standards to be applied in any industry and by any type of covered entity.[3] The Recommendations are, then, integrated by a set of Guidances published for specific industries or type of regulated entity to customize the overarching policy strategy (as the above-analysed Guidance on virtual assets and virtual asset service providers).

The Standard was first approved by the FATF in 1990. After a series of modifications, the last comprehensive version has been published in 2012 and has since been regularly updated. The Standard is composed of forty high level Recommendations divided in seven areas: 1) AML/CFT Policies and coordination; 2) Money laundering and confiscation; 3) Terrorist financing and financing of proliferation; 4) Preventive measures; 5) Transparency and beneficial ownership of legal persons and arrangements; 6) Powers and responsibilities of competent authorities and other institutional measures; 7) International cooperation. Due to the international scope of the FATF's

[1] Proposal for a Regulation of the European Union, 20th July 2021, n. 0241.
[2] Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., for further information and related publications see https://www.fatf-gafi.org/en/topics/fatf-recommendations.html; on their relevance P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 125 – 126.
[3] V. Mitsilegas – N. Vavoula, *The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law,* cit., 264; M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 293.

mandate, the Recommendations are thought as a flexible instrument to be adapted by each jurisdiction depending on the characteristics of their legal system.[4]

At the Union level, the backbone of the compliance regulation is constituted by the Money Laundering Directives. These Directives have been in force since 1990, in parallel with the FATF's Standard, and have been progressively enriched during the last three decades. The latest Directive is the Fifth, approved in 2018, which also constitutes the first anti-money laundering Directive encompassing crypto-assets.[5] The core of the policy strategy as laid out by the Directives is then complemented at the Union and National level. At the Union level, by specific Regulations and executive acts of the Commission and the European Supervisory Authorities, specifically the European Banking Authority. An example being the Travel Rule Regulation, implementing FATF's Recommendation 16, analysed in section five of the present chapter. At the National level, by legislations implementing the Directives and guidelines published by each Financial Intelligence Unit.

As detailed in the previous chapter, the sectorial regulation is currently undergoing a major upheaval at the Union Level through the introduction, envisioned for the late 2024, of the Anti-money Laundering Package. The Package will partially replace the current Directive with a Regulation. For the purpose of our present analysis, we can take the Directive and the Standard as our point of reference. Eminently, the aim here is to highlight the key elements of anti-money laundering compliance to facilitate the readers' understanding of the customized regulation provided for crypto-assets. These core concepts are not fundamentally affected by the aforementioned legislative project.

[4] See among the fundamental principle of FATF's policies, the Functional equivalence and objectives-based approach which means "*the FATF requirements, including as they apply in the VA space, are compatible with a variety of different legal and administrative systems. They broadly explain what must be done but not in an overly-specific manner about how implementation should occur in order to allow for different options, where appropriate. Any clarifications to the requirements should not require jurisdictions that have already adopted adequate measures to achieve the objectives of the FATF Recommendations to change the form of their laws and regulations. The Guidance seeks to support ends-based or objectives-based implementation of the relevant FATF Recommendations rather than impose a rigid prescriptive one-size-fits-all regulatory regime across all jurisdictions*", in Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 9.

[5] For an analysis see the previous Chapter.

## 2.1 The Risk-based Approach

The overarching principle governing the anti-money laundering field, provided by Recommendation 1 of the FATF Standard, is the risk-based approach.[6] The risk-based approach applies equally to legislators, supervisors, and covered entities.[7] This principle aims at avoiding that compliance duties are applied in a mechanical fashion (causing the, so-called, tick boxing fallacy).[8] Due to the multifaceted and adaptive nature of money laundering, both supervisors and supervised should tailor compliance duties to the specific nature of the risk identified for each specific case.[9] In this sense, the anti-money laundering legislation is envisioned as a flexible instrument to be customized to each single situation depending on the risks identified. Covered entities are, hence, required to put an extra effort and assess the risk at hand and then decide how to apply the regulation.[10]

[6] The risk-based approach constitutes the second iteration of the anti-money laundering regulation, eminently, in the beginning the regulation was focused on a rule-based approach. However, following critics that such an approach was costly and created rules easy to circumvent for money launderers, the rule-based approach was substituted, starting from 2003, with the current risk-based approach. Eminently, money launderers have proven adaptive and reactive to regulatory standard, thus, making a stable, rule-based approach too predictable. For an analysis see A. Bello – J. Harvey, *From a risk-based to an uncertainty-based approach to anti-money laundering compliance,* in *Security Journal,* 30, 2017, 25-27.

[7] E. Savona - M. Riccardi, *Assessing the risk of money laundering: research challenges and implications for practitioners*, in *European Journal on Criminal Policy and Research*, 25, 2019, 1; P. Van Duyne – J. H. Harvey – L. Y. Gelemerova, *The critical handbook of money laundering: Policy, analysis and myths*, cit., 127.

[8] For tick boxing fallacy it is meant the implementation of anti-money laundering controls in an automatic, mindless function. From this perspective, anti-money laundering duties are simply another box to tick to open an account which in turn significantly decreases the concrete effectiveness of the controls. See, A. Bello – J. Harvey, *From a risk-based to an uncertainty-based approach to anti-money laundering compliance,* cit., 26; S. Ross – M. Hannan, *Money laundering regulation and risk-based decision-making*, cit., 107.

[9] See Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., 30, "*By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way*"; for the application of the risk based approach in supervision see Directive of the European Union, 20th May 2015, n. 849 (consolidated version updated to the 30th June 2021) article 48, paragraph 6, and for covered entities article 8. See also L. Dalla Pellegrina – D. Masciandaro, *The risk-based approach in the new European anti-money laundering legislation: a law and economics view*, cit., 936, "*Since money launderers can have a complete knowledge of an AML regulation with such an approach, they therefore can adjust their money laundering techniques in order to comply with the codified rules, consequently making illegal operations indistinguishable from legal ones. At the end of the day, FIs will identify all transactions as regular ones*".

[10] See Directive of the European Union, 20th May 2015, n. 849, recital 22, "*The risk of money laundering and terrorist financing is not the same in every case. Accordingly, a holistic, risk-based approach should be used. The risk-based approach is not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based*

There are three main dimensions of the anti-money laundering risk.

First, the overarching risk, to be identified at a policy/supervisory level. At this level, the object of the analysis concerns industries and categories of transactions.[11] Second, the risk, to be identified by the single covered entities, regarding the different areas (industry and geographical) where the entities operate and each macro-process. Third, the individual risk, to be identified by the covered entity and its compliance team. At this level, the focus is on the single customer and/or transaction depending on its specific characteristics.

The first and second risk factors should guide both supervisors and supervised in the allocation of resources[12] and in drafting tailored policies.[13] The second and third risk factors should guide the covered entity in customizing the level of controls to be applied in each specific case.[14] Eminently, the regulation requires covered entities to draft a risk profile for each customer on which basis all further compliance decisions should be made.[15] For instance, a customer operating in a high-risk industry (as diamonds, gold trading, weapons, or crypto-assets) or high risk country[16] as well as a high-risk individual (as a Politically Exposed Persons)[17] should warrant for increased controls –

*decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively*".

[11] At the Union's level the National risk assessment is complemented by a Union level risk assessment that is published on a biannual basis jointly by the European Supervisory Authorities (EBA and ESMA) as provided by article 6, paragraph five, of Directive of the European Union, 20th May 2015, n. 849, cit.; E. Savona - M. Riccardi, *Assessing the risk of money laundering: research challenges and implications for practitioner,* cit., 2.

[12] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 34.

[13] S. Ross – M. Hannan, *Money laundering regulation and risk-based decision-making*, in *Journal of Money Laundering Control*, 1, 2007, 106; A. Simonova, *The risk-based approach to anti-money laundering: problems and solutions* in *Journal of Money Laundering Control*, 4, 2011, 347; for an example of such policies see European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactio ns ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* Paris, 2021.

[14] European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849),* cit., 20; O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 28.

[15] These decisions include whether to pursue Enhanced Due Diligence controls, the frequency of ongoing due diligence, the threshold and frequency of transaction monitoring.

[16] High risk countries are identified, following art. 9 of the Anti-money Laundering Directive, by the Commission annually such an exercise and its effects are regulated by European Commission Delegated Regulation, 14th July 2016, n. 1675.

[17] The category of Politically Exposed Person is one of particular relevance for anti-money laundering purposes. Eminently, due to their position these individuals are considered of higher risks as they could be involved in corruption or other instances of public funds' mismanagement. For this reason, Politically

so-called Enhanced Due Diligence.[18] At the same time, if risks are low, simplified controls can be applied.[19]

The risk-based approach, hence, introduces a preliminary duty on both supervisor and supervised to pursue a risk assessment at each of the three levels identified.[20] This exercise is thought as a collaborative effort between supervisors and supervised. Eminently, it is up to the supervisors to provide covered entities with information and guidance to shape their risk assessment.[21] In this sense, covered entities have a bounded discretion when evaluating risk. The supervisor sets the boundaries and identifies the key risks, tracing a common minimum standard. It is, then, up to the supervised to evaluate, within these boundaries, the risk a single customer, process, or transaction poses.

Exposed Persons are under tighter controls for anti-money laundering purposes and are considered as high risk customer. A Politically Exposed Persons are defined by article 3, para. 9, of the Directive of the European Union, 20th May 2015, n. 849 as "*a natural person who is or who has been entrusted with prominent public functions and includes the following: (a) heads of State, heads of government, ministers and deputy or assistant ministers; (b) members of parliament or of similar legislative bodies; (c) members of the governing bodies of political parties; (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; (g) members of the administrative, management or supervisory bodies of State-owned enterprises; (h) directors, deputy directors and members of the board or equivalent function of an international organization*". For a critique A. Bello – J. Harvey, *From a risk-based to an uncertainty-based approach to anti-money laundering compliance,* cit., 30, that argue such automatic risk factors constitute a surreptitious reintroduction of the box-ticking approach.

[18] O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 13.

[19]For some examples of elements that covered entities should take into account when evaluating a customers' risk see Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., 68. Examples of risk factors are: business that are cash intensive; countries subject to sanctions, embargoes, or similar measures issued by, for example, the United Nations; on-face-to-face business relationships or transactions. Mitigating factors include: the customer being a public company listed on a stock exchange or a public administration; or the provision of services as life insurance policies where the premium is low (e.g., an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).

[20] M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 293.

[21] As provided by article 7, para 4, letter e, of the Directive Member States shall "*make appropriate information available promptly to obliged entities to facilitate the carrying out of their own money laundering and terrorist financing risk assessments*". For a list of such sources see Guidelines 1.30, European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849),* cit., 25.

This exercise is a fundamental part of compliance in the field and one that is also key in the *ex-post* evaluation regarding the effectiveness of an anti-money laundering framework.[22] The risk assessment should, hence, be duly documented and updated.

Furthermore, the risk assessment is conceived as a dynamic rather than static exercise. This means that, both supervisors and supervised, should reassess their risk periodically and ensure is kept up to date. Regarding what periodically means, European law only identifies a clear deadline for the risk assessment pursued by the Commission – i.e., every two years.[23] National Authorities have a leeway in deciding when the risk assessment should be updated.[24]

One element that has to be kept in mind when analysing risk assessments and risk indicators is their connection with costs. Eminently, the risk-based approach has a direct impact on compliance costs. As compliance duties change depending on the nature of the customer, certain customers (due to their employment status, industry, or geographical location) are significantly more costly for covered entities than others. This is because such customers require more incisive controls and, hence, a larger allocation of resources. For instance, to open an account to a customer operating or located in a high-risk jurisdiction, the covered entity has to apply enhanced due diligence controls which are more resource and time intensive compared to normal controls.

Such a cost variance has caused a phenomenon known as de-risking.[25] With de-risking is meant the business choice made by covered entities not to provide services to certain customers or

[22] S. Ross – M. Hannan, *Money laundering regulation and risk-based decision-making,* cit., 107. In favour of this approach, L. dalla Pellegrina – G. Di Maio – D. Masciandaro – M. Saraceno, *Are Bankers "Crying Wolf"? Type I, Type II Errors and Deterrence in Anti-Money Laundering: The Italian Case* in *Italian Economic Journal,* 2022, 22, critical, A. Bello – J. Harvey, *From a risk-based to an uncertainty-based approach to anti-money laundering compliance,* cit.

[23] Article 6, paragraph 1, of the Anti-money Laundering Directive. For the latest risk assessment see European Commission, *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities,* COM(2022), 27th October 2022.

[24] Regarding the company wide risk assessment, the EBA Guidelines 1.7 states that the company-wide risk assessment should set a date for each year when the risk assessment is updated, see European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactio ns ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849),* cit., 21. In general see Guideline 1.6 – 1.10.

[25] T. Durner – L. Shetret, *Understanding bank de-risking and its effects on financial inclusion: an exploratory study*, Global Center on Cooperative Security Oxfam International, 2015. For the European response to the phenomenon, European Banking Authority, *EBA issues Guidelines to challenge unwarranted de-risking and safeguard access to financial services to vulnerable customers,* Paris, 31 March 2023, https://www.eba.europa.eu/eba-issues-guidelines-challenge-unwarranted-de-risking-and-safeguard-access-financial-services.

industries based on the connected compliance costs (and risks). This is a pathology of the system as it restricts access to fundamental services (as banks) to law-abiding customers simply due to their characteristics.[26]

Compliance costs and de-risking are topics of particular relevance for our field of study. Eminently, the crypto-assets industry has been consistently identified, at least at the European level, as high-risk.[27] Which means the concrete implementation of duties is significantly enhanced compared to the overall framework.[28] In this sense, when assessing anti-money laundering regulation, it is important to see the imposition of increased compliance duties, even if simply in the form of a higher risk status, also from the perspective of compliance costs.[29]

## 2.2 Profiling and Monitoring. The Customer Due Diligence

[26] As underlined by the EBA "*The EBA found that de-risking occurs across the EU and affects different types of customers or potential customers of institutions, including specific segments of the financial sector such as respondent banks, payment institutions (PIs) and electronic money institutions (EMIs), as well as certain categories of individuals or entities that can be associated with higher ML/TF risks, for example asylum seekers from high ML/TF risk jurisdictions or not-for-profit organisations (NPOs). While the impact and scale of de-risking within different categories of customers vary, de-risking can lead to adverse economic outcomes or amount to financial exclusion. Financial exclusion is of concern, as access to at least basic financial products and services is a prerequisite for participation in modern economic and social life*", see European Banking Authority, *Opinion of the European Banking Authority on 'de-risking',* Paris, 2022, 2; for an example of the real world effects of such a phenomenon see the reported impossibility for African diplomats to open bank accounts in Brussels as reported by Politico, see B. Moens – E. Wax, *African diplomats can't open bank accounts in Brussels — and Qatar scandal could make things tougher,* Politico, 22nd December 2022, https://www.politico.eu/article/african-diplomats-cant-open-bank-accounts-in-brussels-and-qatar-scandal-could-make-things-tougher/

[27] European Banking Authority, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, cit., 94.

[28] See European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849)*, cit., 73-74, that prohibits to covered entities, when dealing with customers that operate in the crypto-assets' space, to apply simplified due diligence measures and provides for a detailed list of controls that should be pursued in cases as such, the guideline is complemented, at page 195, where the Authority clearly states that "*Guidelines 9.20 to 9.24 reasonably reflect the increased ML/TF risk (of virtual currencies)*"; European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, SWD(2022), cit., 101, that identifies the crypto-market as posing a very significant very high risk (the highest level) of money laundering.

[29] On the economic impact of such a perception see M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 289; for an example see the Section Four of the present Chapter on the implementation of the travel rule in the crypto-sphere.

The performance of Customer Due Diligence (CDD) constitutes the main duty for covered entities under the anti-money laundering regulation.

Following article 11 of the Directive, Customer Due Diligence should be carried out by covered entities in four situations.[30]

First, when establishing a business relationship. Second, when carrying out an occasional transaction that: (i) amounts to euro fifteen thousand or more, whether that transaction is carried out in a single operation or in several operations that appear to be linked; or (ii) a wire transfer exceeding euros one thousand.[31] Third, when there is a suspicion of money laundering or terrorist financing. Fourth, when there are doubts about the veracity or adequacy of previously obtained customer identification data.[32]

When one of these four conditions is met, the covered institution will have to perform a number of checks – which fall under the umbrella of Customer Due Diligence. These are provided by article 13 of the Directive.

These measures comprise four fundamental steps. The first three steps fall under the umbrella of the so-called Know Your Customer (KYC). Know Your Customer refers to the activity covered entities have to perform in order to gain a complete understanding of who their customer is and the purpose of their business relationship. Following the risk-based approach, the level of detail

[30] The FATF Recommendations set a lower bar compared with the Directive: following Recommendation 10, CDD shall be triggered only "*If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing*", see Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., 64. In this sense, the Union's legislation requires covered institutions to acquire all relevant information irrespective of any suspicion, whereas for the FATF it is the suspicion that triggers CDD. This discrepancy does not constitute a violation of the FATF's Standards which are to be interpreted as the minimum any legislation should require with always the possibility for individual jurisdictions to impose higher standards.

[31] A wire transfer is defined by Regulation of the European Union, 20th May 2015, n. 847, article 3, paragraph 9, "*any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same*". For more details regarding this Regulation and connected definitions refer to paragraph 5 of this chapter delving into the travel rule.

[32] Specific thresholds are provided by letter c and d of the same article for "persons trading goods" (ten thousand euros) and gambling service providers (two thousand euros).

of this profiling exercise is dependent on the risk profile as assessed based on the customer's characteristics (location of the customer, complexity of its legal structure, etc.) and the purpose of the relation. As abovementioned, if the customer is deemed as high-risk, Enhanced Due Diligence controls should be applied, to obtain a more in-depth understanding of the customer.[33]

The Know Your Customer process entails, at a minimum three steps directly mandated by the Directive.

First, identifying the customer and verifying the customer's identity. The extent of such a verification duty changes if the customer is a natural or legal person.[34]

In order to understand these two steps, there is a distinction we need to draw between identification and verification. These two terms have a specific meaning in the anti-money laundering domain, one that applies to all sectorial compliance checks. It is, hence, important to keep this distinction in mind when interpreting any anti-money laundering regulation. To 'identify' means to obtain certain information (identity, source of income, address, etc.) from the customer themselves. In contrast, 'verifying' means to check the former information on "*the basis of documents, data or information obtained from a reliable and independent source*".[35] The verification constitutes, thus, a step further compared with the identification; one that sizably increases the compliance effort, and costs, required.[36]

Under the first step, the covered entity has, hence, to both identify and verify the customer's identity. This entails, if the customer is a natural person, ascertaining the customer's name, physical

[33] See Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., 74, which includes among such additional information: "*Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial own er; Obtaining additional information on the intended nature of the business relationship; Obtaining information on the source of funds or source of wealth of the customer; Obtaining information on the reasons for intended or performed transactions*", see, on a similar note, Directive of the European Union, 20th May 2015, n. 849, article 18a.; H. Koster, *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework,* cit., 381.

[34] For further information on the different controls to be applied see Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., 64 – 65.

[35] See article 13, Directive of the European Union, 20th May 2015, n. 849.

[36] On acceptable proof of identity see European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* cit., 43.

address, date of birth, and unique national identifier[37] and then verifying it through documents provided by reliable third parties (e.g., in person verification by an employee of the covered entity; verification through a certified identification software,[38] etc.). If the customer is a legal person, the identification covers the incorporation, registered name, and place of business. The verification can be carried out through the comparison between information provided by the client and third-party repositories, such as company houses.

The second step of Know Your Customer is mainly addressed to customers that are legal arrangements or legal persons.[39] Eminently, article 13 requires covered entities to:

> *"identify the beneficial owner and take reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer".*

The concept of beneficial ownership is a fundamental one for anti-money laundering purposes and deserves a brief digression.

The ultimate purpose of money laundering is to disguise the origin of the proceeds of a crime in a way that gives the impression of lawfulness.[40] This is a crucial step of money laundering. The phase identified in the introduction under the label "layering". Through layering criminals introduce a series of layers between the proceeds and the original criminal activity. The final purpose of money laundering is to introduce so many layers between the asset and its origin that

[37] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 41; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 79.

[38] Certified identification software are software that allow the verification of the identity usually based on a three step process where a photo of the ID is taken, then a photo of the customer which are then compared (usually through face recognition processes) to guarantee consistency, for an example see Jumio https://www.jumio.com/. For guidelines on their use see Guidelines 4.32 – 4.37, European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactio ns ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849),* cit., 21.

[39] Even though the concept of Beneficial Owner can also apply in case a natural person is acting on behalf of a third party.

[40] O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 13; for more on money laundering and its different phases see the introduction.

tracing back the asset to its initial source is impossible or, at least, very complex.[41] In order to introduce these hiding layers in an effective way, criminals have to disguise the identity of the people operating with the assets. To do so, money launderers use complex legal structures that distance the identities of the real beneficiaries from the assets, so that the covered entity does not perceive who the real owner is – and who it is they are actually in business with. Classic examples of such stratagems being the use of dummy corporations, shell companies,[42] front men, and trusts.[43]

In order to hamper such a phenomenon, the anti-money laundering regulation has introduced the concept of Ultimate Beneficial Owner (UBO).[44] By mandating the identification of the natural person who ultimately benefits from their services, the regulation aims at piercing the corporate veil and understanding *in concreto* who is behind a certain legal arrangement.

Beneficial owners are defined by article 3, paragraph 6, of the Directive as:

> *"any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted"*.[45]

Covered entities are, hence, required to unpack the corporate structure of their customers – even where multiple companies and jurisdictions may be involved – to then identify and verify who is the individual that ultimately benefits from the legal arrangement and the covered entities' services. In order to facilitate the identification of the Beneficial Owner, article 30, paragraph 3, of the Directive now provides for a Beneficial Ownership Registry. Particularly, the Directive requires each Member State to establish such a registry and "*mandate corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held*". Non-compliance with such a duty has to be

[41] P. Gilmour, *Reexamining the anti-money-laundering framework: a legal critique and new approach to combating money laundering* in *Journal of Financial Crime,* 2022, 1 – 2; O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 14.

[42] O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 33.

[43] For an analysis of how money launderers can obfuscate beneficial ownership see Financial Action Task Force, *Concealment of Beneficial Ownership,* cit.

[44] O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 40; for a detailed analysis see the FATF's sectorial guidance, Financial Action Task Force, *FATF Guidance on transparency and beneficial ownership*, Paris, 2014.

[45] The criteria to identify a beneficial owner or owners are further detailed by the same article, letter a, for corporate entities, letter b, for trusts, and, letter c, for foundation and other legal arrangements similar to trusts.

punished with proportional and dissuasive sanctions.[46] However, as clarified by paragraph 8 of the same article, covered entities cannot simply base themselves on the information in the registry. Rather they shall confirm such information through a risk-based approach. Examples of third-party providers where such information can be found for verification purposes are companies' houses.

The third and final step of Know Your Customer is the identification of the purpose and intended nature of the business relationship. To this end, the customer has to declare the reason why they are using the covered entities' services. For instance, they may declare that the account will be used to pay suppliers or to save money to buy a house. This last step simply consists of a unilateral declaration of the customer.

It is rooted in the information gathered through Know Your Customer that the fourth step of Compliance Due Diligence has to be pursued. Eminently, covered entities are required to monitor the activity of the customer and the ongoing business relationship in light of the information gathered. Particularly, they have to ensure that transactions:

> *"are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date".*[47]

This last step, also known as transaction monitoring, is directed at identifying suspicious transactions, meaning transactions (both incoming and outgoing) not in line with the profile of the customer or that signal a risk of criminal activity.[48] The reporting of such suspicious transactions is the ultimate goal of the anti-money laundering compliance duties and is the topic of the next section.

[46] Para 5 of the article established that not only competent authorities and FIUs could access such a registry but also any member of the general public. However, the Court of Justice found such an extensive access to be disproportionate, see European Court of Justice, C 53/20 – 601/20 WM and Sovim SA v Luxembourg Business Registers, 2022.

[47] Anti-Money Laundering Directive, article 3, paragraph 13.

[48] European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849),* cit., 55, Guidelines 4.72 – 4.75.; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 81, "*Monitoring transactions is an essential component in identifying transactions that are potentially suspicious, including in the context of VA transactions. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious*".

## 2.3 The endgame of anti-money laundering compliance: the Suspicious Activity Reports

The main end result of Customer Due Diligence is the identification and reporting of suspicious activities. Compliance's aim, when it comes to anti-money laundering, is to create a system of decentralized policing. Each of the covered entities is a nexus, a chokepoint, of the economic system. Due to their role, such entities have access to a wealth of data regarding their customers and connected economic activity. Through their policing, the anti-money laundering regulation creates a system of capillary intelligence for the prevention and identification of illicit financial flows. To achieve this goal, each of the covered entities has to profile their customer, monitor their activity, and report them when suspicious.[49]

The duty to report suspicious transactions falls not only on the covered entities as a whole but also on their directors and employees. The obligation to report suspicious transactions is, hence, both individual – as it falls on each employee of the covered entity to report suspicious activities – and collective – as the covered entity as a whole has to create systems that enable such reporting and ensure it is correctly performed.[50]

The duty to file a Suspicious Activity Report (SAR) is triggered when there is knowledge, suspicion, or reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing.[51] All suspicious activities should be reported to the Financial Intelligence Unit including attempted transactions. The bar for reporting is overtly low as a mere suspicion is sufficient to trigger the duty. This all-encompassing definition of suspicious transactions has been criticized by part of the literature as some have argued it has created an overly cautious approach by covered entities that may choose to report as a risk

[49] L. dalla Pellegrina – G. Di Maio – D. Masciandaro – M. Saraceno, *Are Bankers "Crying Wolf"? Type I, Type II Errors and Deterrence in Anti-Money Laundering: The Italian Case,* cit., 2.

[50] As provided by article 33, paragraph 1; for more on this topic see section 2.4 on the sanctions provided by the Directive.

[51] See article 33, paragraph one, letter, a, the covered entity has a duty of "*informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing*".

mitigation measure.[52] This has flooded financial supervisors with the consequence of increasing the noise in the information on suspicious activity and of making the identification of actually risky transactions significantly harder.[53]

Together with the duty to report a suspicious transaction, two ancillary obligations are provided for. First, the covered entity should refrain from carrying out the transactions of which they know or suspect the illicit nature.[54] Second, they must refrain from informing the customer or any third party that a suspicious activity report has been, or will be, filed (so-called prohibition of tipping off).[55]

The recipient of the suspicious activity reports is an *ad hoc* entity that should be instituted within each jurisdiction: the Financial Intelligence Unit (FIU).[56] The Financial Intelligence Unit is provided by Recommendation 21 of the FATF's Standard[57] as transposed by article 32 of the Directive.

Once a suspicious activity report is received, the Unit has to analyse it and, when deemed necessary, contact the competent National authority to trigger further investigations. The Unit can also request further information to the reporting institution, hence, creating a dialogue concerning the (suspicious) customer and/or transaction.

[52] This phenomenon is labelled by L. dalla Pellegrina – G. Di Maio – D. Masciandaro – M. Saraceno, *Are Bankers "Crying Wolf"? Type I, Type II Errors and Deterrence in Anti-Money Laundering: The Italian Case*, cit., 2, as the "Crying Wolf Effect"; B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 11.

[53] Just to give an idea of the magnitude of this problem, in the United States only two point three million SARs are filed annually, meaning over six thousand reports are filed on a daily basis. Numbers of this magnitude generate a pressure on the financial supervisors that, rather than being provided with a small number of sure leads, are flooded with thousands of reports which they are mostly unable to correctly process and analyse. A. Bello – J. Harvey, *From a risk-based to an uncertainty-based approach to anti-money laundering compliance,* cit., 26, "*Clearly, if banks report everything as suspicious, they effectively report nothing*"; S. Ross – M. Hannan, *Money laundering regulation and risk-based decision-making,* cit., 107.

[54] See article 35, Directive of the European Union, 20th May 2015, n. 849, an exception to such a duty to freeze the transaction is provided by the second paragraph of the same article "*where refraining from carrying out transactions referred to in paragraph 1 is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation*".

[55] See article 39, Directive of the European Union, 20th May 2015, n. 849.

[56] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 68.

[57] Financial Action Task Force, *International Standards on Combating Money Laundering and the Finance of Terrorism and Proliferation. The FATF Recommendations,* cit., 104 – 106.

## 2.4 The sanctioning infrastructure

The effectiveness of the anti-money laundering infrastructure is reinforced through a sanctioning regime provided by Section 4 (article 58 – 62) of the Directive.

The sanctioning regime stipulated by the Directive is administrative in nature, as the law does not directly provide for any criminal sanction. However, the Directive leaves Member States a certain leeway, stipulating the latter can substitute administrative sanctions with criminal ones.[58] The Directive, thus, gives a baseline that is up to individual States to implement or aggravate.

The sanctioning system follows a two-pronged approach as it targets, at the same time, legal and natural persons – i.e., the covered entities and their employees.

From a natural person's perspective, article 58, paragraph 3, states:

> "*Member States shall ensure that where obligations apply to legal persons in the event of a breach of national provisions transposing this Directive, sanctions and measures can be applied to the members of the management body and to other natural persons who under national law are responsible for the breach*".

Hence, when a breach of anti-money laundering compliance duties is ascertained, the liability should also extend to the individuals. Such individuals pertain to two categories. First, the members of the management body, which, under article 46, are responsible for the set-up, implementation, and supervision of the compliance model. Second, other natural persons who under, national law, are responsible for the breach. This is an ample category that can include any employee that plays a role in the anti-money laundering cycle, from the Know Your Customer Officer to the salesperson – e.g., a salesperson who has tipped of the client concerning a Suspicious Activity Report being filed.[59]

[58] See article 58, para 2, "*Member States may decide not to lay down rules for administrative sanctions or measures for breaches which are subject to criminal sanctions in their national law. In that case, Member States shall communicate to the Commission the relevant criminal law provisions*".

[59] See in this sense the crime provided in the Italian system by art. 55, para. 4, of the anti-money laundering law (D.lgs. 231/2007) for breach of the prohibition to tip off.

From the legal person's perspective, article 60, paragraphs 5 and 6, provide for a series of mandatory criteria based on which individual actions by employees should also be ascribed to the covered entity. The criteria are different if the person responsible holds a "leading position" or not. To ascertain if the employee has a leading position the Directive gives three alternative criteria: the person has "*(a) power to represent the legal person; (b) authority to take decisions on behalf of the legal person; or (c) authority to exercise control within the legal person*". If the employee has a leading position, the legal person should be held liable if the breach was committed in its interest. In contrast, if the employee responsible for the breach is not in a leading position, the legal person is only responsible where the lack of supervision or control by a leading person has made it possible to commit the breach for the benefit of that legal person by a person under its authority. Hence, in this second case to the positive element of the benefit for the legal person a second parameter is added, the lack of supervision of control which has to be causally connected with the breach.

Concerning the breaches which shall give rise to sanctions, the Directive again provides for a baseline. Article 59 states that, at a minimum, Member States shall sanction breaches that are serious, repeated, systematic, or a combination thereof, affecting four areas: 1) customer due diligence; 2) suspicious transaction reporting; 3) record-keeping; 4) internal controls.

Finally, regarding the type of sanctions and their determination, the Directive only gives a baseline for those applied to legal persons. The sanctions applied to individuals are, hence, left to the discretion of Member States. The sanctions listed by the Directive for legal persons are:

> "*(a) a public statement which identifies the natural or legal person and the nature of the breach*[60] *(b) an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct; (c) where an obliged entity is subject to an authorisation, withdrawal or suspension of the authorisation; (d) a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities; (e) maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least* EUR *1 000 000*".[61]

Regarding their determination, article 60, paragraph 4, provides for the following criteria:

[60] The publication of the sanction can be avoided or postponed in specific cases provided by article 60.

[61] A specific sanctioning system is provided by art. 59, para 3, when the covered entity concerned is a financial or credit institution.

"*(a) the gravity and the duration of the breach; (b) the degree of responsibility of the natural or legal person held responsible; (c) the financial strength of the natural or legal person held responsible, as indicated for example by the total turnover of the legal person held responsible or the annual income of the natural person held responsible; (d) the benefit derived from the breach by the natural or legal person held responsible, insofar as it can be determined; (e) the losses to third parties caused by the breach, insofar as they can be determined; (f) the level of cooperation of the natural or legal person held responsible with the competent authority; (g) previous breaches by the natural or legal person held responsible*".

To sum up, the Directive gives a baseline in terms of sanctioning to then be transposed or aggravated by Member States. The sanctioning regime follows a double binary approach punishing both the entity as a whole and the individuals responsible for the breach.

## 3. The application of the anti-money laundering regulation to crypto-assets

The overarching framework we have just sketched has been fully extended to the crypto-assets market. Eminently, so far, the core of the crypto-assets' policing strategy has focused on the extension of the full spectrum of classic anti-money laundering compliance duties to a series of intermediaries identified in this emerging market (as clarified in chapter three, section two). To this end, the Fifth Anti-money Laundering Directive[62] added wallet providers and exchangers among the list of covered entities enumerated by article 2.[63] Covered entities in the crypto-market are, therefore, under the same above-detailed compliance duties as any other intermediary. The MiCaR and the Anti-money Laundering Package take a similar approach. Apart from an extension in the

[62] Directive of the European Union, 30th May 2018, n. 843.

[63] As detailed in the previous chapter this list of covered entities will be complemented, in the same fashion as the Fifth Directive, by the Anti-money Laundering Regulation to match the Financial Action Task Force's latest Guidance.

number of covered entities, no new or customized anti-money laundering duty is provided for crypto-asset service providers.[64]

As explained in the previous chapters, this approach is controversial.[65] Eminently, the core of crypto-assets' innovation lies in the introduction of a new architecture for financial transactions. One that can be summarized with the two terms decentralization and disintermediation.[66] In turn, these two elements create distinct challenges for the implementation of traditional compliance duties.[67]

Let's start with decentralization. In a decentralized environment, the application of controls envisioned for vertical, human operated arrangements is complex. Compliance Due Diligence and Suspicious Activity Reports are thought to be applied by centralized arrangements that function in a hierarchical fashion. The same goes for the connected sanctioning system where allocation of responsibility is connected with the internal organizational structure of the arrangement. In decentralized autonomous organizations and decentralized networks, the kingpin is the code – meaning the smart contract the DAO is rooted in – rather than the humans. In this sense, the identification of individual responsibilities is complex as many of the actions are performed by the code in an automatic fashion.[68] In such environments, humans may, hence, miss the concrete ability to execute the mandated actions.

The second critical point is disintermediation: in a disintermediated environment the implementation of an intermediary-centred approach misses a whole chunk of the market – i.e.,

[64] For an analysis see section two of the previous chapter; for an overview of specific red flags provided for VASPs see Financial Action Task Force, *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, Paris, 2020.

[65] See, in this sense, the critique raised by the French Autorité de Contrôle Prudentiel et Résolution in O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 2, "*the regulation of disintermediated finance cannot simply replicate the systems that currently govern traditional finance. On the contrary, regulations must take into account the specific features of DeFi*"; World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 7, "*crypto-assets and their ecosystem do not always fit squarely into the existing activity-based, intermediary-focused approach of regulation, even where crypto-asset activities mirror those of the traditional financial sector. Some of the reasons for this include an inability to classify either various tokens under the existing definitions or the intermediary in providing services to users".*

[66] On the connection between decentralization and disintermediation see O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 2.

[67] World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 6, "*Crypto-assets, and the technologies on which they are based, present unique technical and structural challenges to regulation due to the decentralized, transparent and open-source nature of the ecosystem*"; C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 4.

[68] World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 9.

all those transactions that are not processed by an intermediary.[69] Moreover, it creates the problem of how should covered entities act when their customer transacts with a self-hosted wallet.[70] If individuals can simply avoid the anti-money laundering checkpoints, the whole control infrastructure loses its effectiveness.

This fallacy is clearly identified by the French *Autorité de contrôle prudentiel et de résolution* in a recently published paper focused on Decentralized Finance. The authority clearly states:

> *"DeFi,[71] based on blockchain infrastructures, has characteristics that make it difficult to assimilate with "traditional" finance. More specifically, traditional finance is critically reliant on a number of intermediaries (banks, insurance companies, clearing houses, etc.), which carry out key operations and manage the associated risks, and on which the bulk of the regulatory burden logically falls. However, the very concept of DeFi consists essentially in building an area of finance without intermediaries or trusted third parties (…) The first pitfall lies in trying to replicate the existing regulatory framework only and exhaustively, without taking into account the specific characteristics (and therefore the potential benefits) of DeFi. This tempting approach leads to restricting the focus of analysis to the identification of intermediaries to whom requirements should be applied".*[72]

In addition, even when such intermediaries are used, the illicit source of the proceeds could be hidden behind so many layers of unchecked transactions to nullify the effectiveness of compliance controls.[73] If the covered entity only focuses on the current customer and its business relationship it will miss the whole chain of self-hosted transactions leading to that specific account.

[69] In this sense see US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, cit., 35, "*the present reliance on centralized VASPs to comply with AML/CFT and sanctions obligations is not likely to sufficiently mitigate illicit finance risks associated with DeFi services*".

[70] See *ex multis* Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., "*P2P transactions are not explicitly subject to AML/CFT controls under the FATF Standards. This is because the Standards generally place obligations on intermediaries, rather than on individuals themselves (with some exceptions, such as requirements related to implementing targeted financial sanctions). The FATF recognises that P2P transactions could pose specific ML/TF risks, as they can potentially be used to avoid AML/CFT controls in the FATF Standards. Where VA transfers occur on a P2P basis, there are no obliged entities involved in preventing or mitigating ML/TF risks";* M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 286 – 287.

[71] DeFi is an abbreviation for Decentralized Finance. For a definition of DeFi see footnote 138.

[72] See O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 27.

[73] The same problem is qualitatively different when it comes to traditional financial transactions. Eminently, as all transactions in such a market are intermediated, the main problem there is connected with the lack of effective controls by one or more of the intermediaries involved in the chain of transactions. Conversely, in a disintermediated environment the chain of self-hosted transactions is under no control making the problem not one of effective implementation of the legislation rather one of architectural impossibility.

Furthermore, the classic anti-money laundering strategy was envisioned for a world where the storage of financial data was entirely rooted in private, fragmented ledgers. In contrast, blockchain introduces a new concept of financial transparency, one where transactions are stored in public, logically unified ledgers.[74] The transition warrants the question of whether customer-based profiling is still the best strategy available for financial monitoring. Eminently, if wallet holders' identities and profiles are much harder to access, blockchain transaction information is comparatively more transparent. Any covered entity can directly analyse a single transaction taking into account any connected (past or contemporary) transaction irrespective if it has been carried out with their systems, by another intermediary, or in a disintermediated fashion. This warrants the question of whether, with crypto-assets, the system should shift from a customer-based one (revolving around the concept of Know Your Customer and customer's profile) to a transaction-based one (revolving around the concept of Know Your Transaction and transaction patterns).[75]

Finally, the way financial data is stored also affects the relation between the supervisor and the supervised. In the traditional system, supervisors only had mediated access to financial data as the latter was held in private ledgers owned by the intermediaries. Blockchain disintermediates the relation between supervisors and financial data granting them direct access to the ledger. This means that, at least from the perspective of financial transactions, the supervisor has immediate access to the underlying data. This opens new possibilities in terms of supervision and calls for a more active role by public authorities, contemporarily attenuating the architectural necessity to delegate financial policing to private institutions. Embracing a more proactive approach, rooted in direct access to financial data, supervisors could directly identify suspicious transactions and only then trigger an information request to the relevant covered entity. This would relieve covered entities from part of the compliance costs, thus fostering competition in the market. We will further discuss how such an approach could work in section six-four.

As detailed in the following sections, all these new instances are emerging as a parallel strategy to classic intermediary-based regulation. The increasing use of blockchain analytics, the reflections

[74] J. Hirshman – Y. Huang – S. Macke, *Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network,* Technical report, Stanford University, 2013, 1.

[75] As clearly stated by M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 287, "*CCs reverse the traditional problem confronting AML efforts, from "parties known-transactions unknown" to "transactions known-parties unknown*".

concerning the regulation of software developers and compliance-by-design, as well as the qualification and policing of peer-to-peer transactions all constitute examples of such a trend.

Notwithstanding these problems, the above does not mean the intermediary-centred approach lacks any merit.[76] As detailed in the first and second chapter, the crypto-market has significantly evolved from its beginnings and has partially moved on from its initial fully decentralized structure: centralized, or partially centralized networks (as permissioned blockchains) and blockchain-based applications have emerged. Likewise, centralized crypto-assets service providers are widely used for ease or lack of specialized knowledge.[77] In this sense, the regulation of intermediaries is still a valid resource.[78] When the activity pursued is qualitatively similar to that of a traditional intermediary it is only fair to impose similar safeguards.

However, the previous approach should be adapted in two senses. First, compliance duties applied to centralized entities (as Crypto-asset Service Providers) should take into account the disintermediation factor and exploit its advantages while mitigating risks. As detailed throughout this text, the blockchain provides for a different architecture for digital exchanges of value and financial data storage. Such a different model should inform the way compliance checks are carried out by covered entities. For instance, the transparency and accessibility of blockchain data can be used as a means to better evaluate the risk factor of a customer by including in the risk assessment an analysis of its previous, publicly available, transactions.[79] Second, a customized strategy should be devised for that part of the market and those actors that do not fit within the framework of classic centralized arrangements. Otherwise, the risk being the uncontrolled growth of a parallel unregulated market performing the same activities as the centralized one.[80]

[76] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, 27.

[77] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 2 – 3.

[78] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 3.

[79] For how such systems have been integrated in compliance practices see the EBA guidelines detailed in section 3.1.

[80] European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 95, "*DeFi applications can be used to avoid existing AML/CFT legislation and the "travel rule" obligations as set out by the FATF*"; World Economic Forum, *Decentralized Finance (DeFi) Policymaker Toolkit*, cit., 18; as underlined by European Central Bank Crypto-assets Task Force, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, cit., 30, the increasing regulation of centralized service providers coupled with a lack of

Given the multi-layered nature of the topic, we will proceed as follows. The rest of the present chapter will delve into how the regulator has addressed the first identified problem: the customization of pre-existing compliance duties to intermediaries in the crypto-market. Section four will analyse how the overarching framework has been applied *in concreto* to the crypto-assets sector by the Union's supervisory authority. Particularly, we will analyse the upcoming European Banking Authorities' Guidelines on red flag indicators. Section five and six will analyse two pieces of legislation that extend specific compliance requirements to crypto-intermediaries: respectively the registration regime and the travel rule regulation. Section seven will then examine how the characteristics of the blockchain, particularly its transparency and accessibility, opened new avenues for financial monitoring and supervision. The next chapter will, then, delve into the second problem we have identified: the regulation of decentralized arrangements that do not fall within the scheme of covered entities. The chapter will analyse how regulators have, or have not, addressed the extension of compliance duties to such headless organizations.

## 3.1 The EBA's red flag indicators. The anti-money laundering regulation in motion

The preceding section has examined the application of the primary legislation to the field of crypto-assets. However, as detailed in section two-one, the anti-money laundering regulation is multi-layered in nature. Due to the risk-based approach, the overarching regulation is envisioned as a flexible instrument to be customized to the characteristics of the single industry and customer.[81]

As detailed in the section on the risk-based approach, this customization effort is fundamentally carried out by two entities: the supervisor and the covered entity. The supervisor – at the Union level the European Banking Authority – publishes guidelines that trace the boundaries and identify the fundamental risk factors. The covered entity, then, within these boundaries, drafts the internal guidelines that define its operating model depending on the risk appetite.

regulation of disintermediated ones may generate the unintended "*risk of an uneven playing field and a shift from centralised to decentralised services*".

[81] B. Villányi, *Money laundering: History, regulations, and techniques*, cit., 11.

For instance, the supervisor may identify a certain area as high risk. It will then be up to the covered entity to decide how to apply this guidance. It can do so by mandating enhanced due diligence controls on each customer operating in the area or it can make the business choice of not accepting such clients.

Guidelines are, hence, a key part of the concrete implementation of anti-money laundering duties as they impact the risk calculation and compliance measures applied by covered entities.

At the Union level, article 17 of the Anti-money Laundering Directive entrusts to the European Banking Authority the issuance of such guidelines. The currently in-force Guideline was published on the 1st of March 2021.[82] This Guideline does not directly address risk mitigation measures to be implemented by the crypto-asset industry. Rather, it introduces a specific guideline (9.20) on how covered entities should mitigate the risk posed by customers that offer services related to crypto-assets. The Guideline is very short and is mostly aimed at underlining the significant risk connected with this industry. For instance, guideline 9.23 expressly prohibits covered entities from applying Simplified Due Diligence controls when dealing with crypto-related services.

Of much greater relevance for our ends is the upcoming set of Guidelines, whose last draft version was published on the 31st of May 2023.[83] Particularly, the Draft introduces a Sectorial Guideline (Guideline 21) specifically addressed to crypto-asset service providers.

The Sectorial Guideline constitutes the first effort by the Union's supervisor to customize anti-money laundering controls to the characteristics of the crypto-market. Eminently, if the in-force Guideline simply provides a means for non-crypto covered entities to protect themselves from the risks posed by crypto-assets, the upcoming text is aimed at guiding CASPs in mitigating the risks posed by their business model. In a sense, the first Guideline takes an external perspective to crypto-risk, and the upcoming ones takes, for the first time, an internal perspective. It is the same Banking Authority to clearly express this objective:

[82] European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849*, EBA/GL/2021/02, cit.

[83] European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849*, cit.

*"The EBA performed a review of the revised ML/TF Risk Factors Guidelines and concluded that the elements set out in these guidelines could be extended to CASPs but also that CASPs had specific characteristics differentiating them from credit institutions and other financial institutions and thus these specificities together with crypto-assets' inherent ones would benefit from further guidance and clarification. For instance, as CASPs products and services offered differ from credit institutions and other financial institutions' products and services, adding guidance, specifically addressed to CASPs, on the risk factors related to these products and services could be of benefit for CASPs. An example is the product's increasing-risk factor when CASPs products entail privacy-enhancing features or offer a higher degree of pseudonymity such as mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and so-called privacy coins. Another example is that as the area of crypto assets is new, different of other assets' areas and in constant evolution, additional guidance on firms' staff's AML/CFT trainings regarding crypto assets unusual transactions or more advanced transaction monitoring analytical tools would be of benefit".*[84]

In line with the mentioned objective, the sectorial Guideline introduces a detailed list of risk factors (so-called red flags), and a set of mitigating measures. The red flags are divided in four risk categories depending on the source of the risk: 1) Product, services, and transaction; 2) Customer; 3) Country or geographical; 4) Distribution channel.[85]

The EBA identifies two overarching elements that characterize the general crypto-risk and one that enhances it. The two characteristics of the crypto-risk are the transnationality of the transaction model and customer base and the instantaneity of the value exchanges. The risk-enhancing factor is the provision of "*products or services which contain privacy-enhancing features or which offer a higher degree of anonymity"*.

Besides these general risk elements, the EBA provides for a detailed list of risk factors CASPs have to take into account when assessing their customers. These factors are both general and technology-specific.

[84] European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* cit., 36.

[85] These are recurring risk categories in the anti-money laundering field, see O. Tucker, *The flow of illicit funds. A case study approach to anti-money laundering compliance,* cit., 80.

General risk factor means a risk indicator recurring in the anti-money laundering regulation and not specific to crypto-assets. These are, for instance, the fact a customer is a shelf company[86] or a politically exposed person (PEP),[87] a transaction pattern unusual or of high frequency, volume, or value inconsistent with the KYC. These factors are not particularly interesting as they are in line with the pre-existing regulation. Hence, they do not signal a customization effort but rather a reiteration of the previous strategy.

Of particular interest are the crypto-specific risk factors as they indicate which elements of the crypto-market are viewed as particularly sensitive by the supervisor. The analysis of such factors reveals four fundamental areas of interest.

First, the use of privacy-enhancing services or anonymity-enhancing features "*such as, but not limited to, mixers or tumblers, obfuscated ledger technology, Internet Protocol (IP) anonymizers, ring signatures, stealth addresses, ring confidential transactions, atomic swaps, non-interactive zero-knowledge proofs and so-called privacy coins*" is perceived as particularly risky.

The transparent nature of blockchain transactions has led to the development of a series of technological solutions aimed at increasing privacy. This is mainly achieved by reducing the transparency of the blockchain ledger or the traceability of the transaction trail. For instance, privacy coins – such as Monero – employ a type of blockchain in which the ledger, while public, does not bear intelligible information concerning the transactions carried out. Such solutions can be developed and used for perfectly legitimate reasons as users may wish to add an additional layer of privacy in their financial transactions. As we will see in section seven-three of the present chapter, some argue that the implementation of such solutions may even be compulsory under the General Data Protection Regulation. However, as any instrument that allows individuals to move

[86] A shelf company is defined by the FATF as an "*incorporated company with inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has already been established*", see Financial Action Task Force, *Concealment of Beneficial Ownership,* Paris, 2018, 5.

[87] A Politically Exposed Person is defined by article 3, number 9 of the Anti Money Laundering Directive as "*a natural person who is or who has been entrusted with prominent public functions and includes the following: (a) heads of State, heads of government, ministers and deputy or assistant ministers; (b) members of parliament or of similar legislative bodies; (c) members of the governing bodies of political parties; (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; (g) members of the administrative, management or supervisory bodies of State-owned enterprises; (h) directors, deputy directors and members of the board or equivalent function of an international organization*". Due to their connection with the public apparatus these individuals are considered to be exposed at a higher risk of corruption and money laundering.

in the shadows, privacy-enhancing tools have a relevant criminogenic potential. This is particularly worrying considering that these tools obfuscate the only information covered entities and investigators sometimes have: the transaction trail. When dealing with self-hosted wallets or DAOs, blockchain transparency is all you have. Due to this element, the anti-money laundering supervisor has increasingly identified these tools as high risk.

Particularly, the Guidance identifies privacy-enhancing technologies as both an overarching risk and a specific one among the product, services, and transaction risk factors.

The second area of concern identified by the Guideline is the interaction or use of self-hosted addresses or unregulated DeFi services. The fact a customer has interacted with self-hosted addresses or DeFi, or is a DeFi service, is categorized as a risk-enhancing factor. In this sense, it seems that the legislature tries to solve the absence of a specific strategy for the policing of DeFi and self-hosted addresses (the disintermediated and decentralized part of the crypto-market) by identifying them as high-risk. Unable to reign on disintermediation it indicates to the intermediated side of the market to be wary of the disintermediated one. Such a designation makes, in turn, each interaction between these two parts of the market more burdensome and costly.

Third, technological literacy is considered a key risk-mitigating factor. The Guideline identifies as high-risk customers "*a vulnerable person or a person who displays very little knowledge and understanding of crypto assets or the related technology, which may increase the risk that the customer is being used as a money mule*".

Fourth, the interaction with services or products not compliant with the MiCa Regulation. This risk factor is aimed at reinforcing the effectiveness of the MiCaR regulation.

Concerning the mitigating measures a CASP can apply, the Guideline mostly refers to traditional measures such as obtaining evidence on the source of funds, source of wealth and increasing the frequency of monitoring of crypto-assets transactions.[88] However, of particular relevance for our ends is the frequent referral made to the use of blockchain analytics tools. These are identified by the EBA as a key mitigating factor to ensure the correct monitoring of the customer's transactions

[88] For the entirety of such measures see guideline 21.12 in European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* cit., 30.

and connected risk assessment. We will further delve into this topic in section seven of the present chapter.

## 4. The registration duties. A way in for *ex-ante* compliance

Recommendation 14 of the Financial Action Task Force's Standard stipulates that providers of Money or Value Transfer Services (MVTS) should be either licensed or registered. The aim of this requirement is twofold.

On the one hand, clearly identifying the providers of services that may generate a money laundering risk and are not otherwise licensed or registered (as financial institutions or insurance companies). MVTS can operate as small businesses or even as individual brokers and their identification can constitute a challenge *per se*.[89] Hence, hampering supervision and enforcement. Through mandatory registration, the supervisor is provided with a clear understanding of the market's conformation and can better assess the connected risk.

On the other hand, the registration of covered entities allows supervisors to operate a pre-emptive evaluation. This permits to verify that, before starting their operations, the covered entity has already in place the necessary compliance safeguards. This is of particular relevance for smaller businesses or new industries. Through registration requirements, the legislature guarantees that such entities are aware of their compliance duties before commencing operations. This as they have to guarantee their compliance with anti-money laundering duties before entering the market. Furthermore, the registration process (should) become a moment of dialogue and mutual learning

[89] For an example of such a risk see the regulation of Hawalas. Hawalas are a system traditional within the Muslim community to move money nationally and internationally. Hawalas are based on networks of individuals based in different countries or different parts of the same country usually connected by family and/or ethnic ties. To move money, the customer deposits the sum at the hawala intermediary based in its location, the money can then be withdrawn by the receiver at the hawala intermediary at the receiving end. The money never physically moves as the sending and receiving intermediary's keep an open account between themselves and settle it in batches. Hawalas were identified as particularly high risk due to their informal nature and absence of overview. For this reason, hawalas have been included among MTVS and are, hence, under a duty of licensing/registration to allow supervisor to have an overview of hawalas in their jurisdiction and apply risk mitigating measures. For an overview of the regulation see International Monetary Fund, *Regulatory Frameworks For Hawala and Other Remittance Systems,* Washington D.C., 2005.

between the covered entity and the supervisor. Especially, when it comes to new business models, the registration process is ideally a moment where the overarching framework is adapted to the single infrastructure and business model.

The FATF's Guidance on crypto-assets explicitly extends the requirement, provided by Recommendation 14, to crypto-asset service providers, mandating these should be either licensed or registered.[90]

Following the Guidance, from a geographical perspective, the registration/licensing should be applied, at a minimum, where the covered entity is created or, in case of an individual, resides.[91] However, the jurisdictions where services or products are offered, and the jurisdictions where the CASP conducts its operations can also require licensing or registration.[92] The Guidance specifies that such a broader coverage is not essential under the FATF Standard. Nonetheless, it constitutes the safer course and is, hence, recommended.[93] To identify the location where the CASP is operating, the Guidance then offers a series of criteria: the location of offices and servers, presence of promotional communications targeting specific countries/markets, the language on the CASP's website and/or mobile application, etc.[94]

When it comes to the concrete implementation of this duty, ample leeway is left to States.[95] Neither the Standard, nor the Guidance provide for a detailed clarification of how Recommendation 14 should be applied. Rather, the focus of the FATF is teleologic. The aim of the registration is to establish an *ex-ante* control regarding the concrete ability of the service provider to comply with the anti-money laundering requirements. To this end, the Guidance simply provides that, as part

[90] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 22; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 107.

[91] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 22.

[92] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 107; Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 23.

[93] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 44.

[94] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 45; these are recurring parameters when it comes to the identification of the location of a digital provider's activity and can, hence, be seen as a mere exemplification, for an example see the Yahoo v. Belgium case, Cour de Cassation, first of December 2015, P.13.2082.N.

[95] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 43; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 84, "*the standards for VASP registration or licensing are extremely wide and varied around the world*".

of the registration process, the supervisory authority should require the CASP to meet a series of criteria. Such criteria should include the verification that:

> *"prior to launch, their AML/CFT programs, including policies, procedures and organization taking into account the characteristics of the VASP's activity (i.e., types of VAs and transactions, targeted customers, distribution channels), are implemented or able to be implemented once launched. This could include judgement as to the competence and trustworthiness of compliance staff".*[96]

It will be, hence, up to the single jurisdiction to decide how to shape its registration regime.

Due to its *ex-ante* nature, the licensing/registration phase is one of the *loci* where the element of compliance-by-design emerges.[97] Eminently, in various parts of the Guidance, the FATF underlines how the implementation of compliance duties should be guaranteed also through built-in features.[98] These include:

> "*limiting the scope of users' ability to transact anonymously, controlling who can access the arrangement, controlling whether/how AML/CFT preventive measures are built into the arrangement and/or by ensuring that AML/CFT obligations of obliged entities within the arrangement are fulfilled, e.g. by using software to monitor transactions and detect suspicious activity*".

This *ex-ante* approach is particularly stressed when it comes to the regulation of Decentralized Autonomous Organizations. Eminently, as the registration/licensing is granted before the entity commences its operations, there is an increased opportunity for by-design requirements. Particularly, the FATF underlines, with regards to arrangements that claim to be fully automated, how the licensing/registration requirement could be the only way in for the regulation. The Guidance states "*the process of creating and developing an asset for launch is unlikely to be able to be*

[96] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 45.

[97] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 46, "*VASPs should put in place AML/CFT compliance prior to launch when designing or building a new product or service, as it is much more difficult to do so later*".

[98] See Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 46, "*VASPs should put in place AML/CFT compliance prior to launch when designing or building a new product or service, as it is much more difficult to do so later. Therefore, careful assessment of risks and thorough evaluation of mitigation measures at the licensing and registration stage is especially important. Once licensing and registration has taken". place, AML/CFT mitigations which are built into products and services should be maintained and be the subject of supervision*".

*automated*".[99] Software development may, through registration requirements, become the way in for by-design anti-money laundering duties to be applied pre-launch.[100]

In this sense, through registration/licensing supervisory authorities may compel developers to create built-in, pre-launch, compliance controls and, correspondingly, only authorize those autonomous arrangements that, by-design, comply with the minimum standards provided by the anti-money laundering legislation.[101] We will further delve into this element in the next chapter, in the section devoted to the qualification of the software developer as a crypto-asset service provider.

Together with the duty of registration, the Guidance provides for a duty of supervision. The jurisdiction not only has a duty to provide for a registration regime but it also has to invest sufficient resources to ensure its enforcement. Particularly, the Guidance requires States to devote sufficient resources to identify unregistered CASPs and provide for dissuasive sanctions.[102]

## 4.1 The European Approach. Between the Fifth Directive, MiCaR, and the Anti-money Laundering Package

[99] A similar notation, regarding the usual centralization of such projects in the development/launch phase is done by O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 7, "*The early stages of a project are usually highly centralised: in the software development phase, the core team of developers, which is often funded by venture capitalists (who get protocol governance tokens in return), holds the administrator keys of the protocol. It is this team that usually develops the main operating rules of the protocol (fees, voting rules, etc.), which are embedded in the program code. The protocol is then deployed on the market, and begins to operate on the basis of the encoded rules. In some cases, the developers keep administrator keys during the early stages of the roll-out (test phase), so that any malfunctions can be corrected as quickly as possible (with the possibility of shutting down the system). Often, the development team forms a foundation or an association*".

[100] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 138, "*The obvious point here is that a DAO does not spontaneously come into existence. The above components evidence a concerted effort by a group of people acting together to create the infrastructure through which a DAO can be created and operated. The number of participants in that group, and their geographic spread may vary, but they are very clearly not decentralised, by necessity. This same group of DAO founders will typically oversee the inception and initial development of a DAO and seek to steward it towards increased membership and participation, with a view to eventually fully vesting management and control into the community of token holders. In this way, many DAOs start of largely centralised but may aspire to significantly more decentralisation than when they began life*"; World Economic Forum, *Decentralized Finance (DeFi) Policymaker Toolkit*, cit., 24, "*Imposing regulatory obligations may be easier earlier in the life cycle, where there may be clearly identifiable access points and more room to influence the long-term trajectory*".

[101] For an example of how such a by-design compliance model could be shaped in a DAO see chapter 5, section 3.

[102] Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* cit., 23.

The registration requirement for crypto-asset service providers was implemented, at the European level, by the Fifth Anti-money Laundering Directive.

Article 47 of the Directive states that:

> *"Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered".*

The Directive, hence, provides for a general overarching duty to be applied by each Member State.[103] The duty left quite an ample leeway to the Member States which could decide how and up to what extent apply it. Additionally, the Directive did not provide for a mutual recognition regime for the registration.[104] This generated a risk for a multiplication of registration duties for an industry inherently transnational.

The decentralized approach was criticized by the European Banking Authority. In its report of 2019 on the European anti-money laundering framework,[105] the Authority underlined that the provision of a solely national regime was causing fragmentation, in turn hampering the orderly functioning of the common market.

In particular, the Report stated:

> *"The EBA has since observed that, in the absence of an EU-wide approach, there are indications that Member States, in anticipation of a forthcoming FATF Mutual Evaluation or to attract VASP business, have adopted their own VASP AML/CFT and wider regulatory regimes. As these regimes are not consistent, this creates confusion for consumers and market participants, undermines the level playing field and may lead to regulatory arbitrage. This exposes the EU's financial sector to ML/TF risk".*[106]

[103] European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 99.

[104] For mutual recognition regime is meant a rule that – as it happens with MiCaR's passporting regime – provides that, once registered in a Member State such registration is automatically recognized across the bloc.

[105] European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU,* cit.

[106] European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU,* cit., 36.

To solve such a fragmentation, the Authority advised for a unified authorization or registration regime for CASPs to be applied and monitored at the Union level.[107]

This recommendation has been implemented by the Market in Crypto-assets Regulation. As we have detailed in the previous chapter, MiCaR introduces a unified registration regime for all CASPs and offerors within the Union.[108] The Regulation also provides for a mutual recognition regime: the registration process needs to only be carried out in one jurisdiction (the home Country) and is then recognized across the Union (through so-called passporting). Other Member States must recognize such authorizations so as to guarantee the Union-wide operativity of service providers.

While passporting is certainly useful as a means to promote the crypto-market and facilitate intra-European provision of services it must be noticed it may also create a risk of a regulatory race to the bottom. The possibility to simply register in one Member State and then operate across the Union may push crypto-companies to forum shop. At the same time, States wishing to attract investments and become the European crypto-hub could use their regulatory leeway to lower the regulatory bar. This is especially so for a market as the crypto-one which frequently lacks a strong physical presence. Such a problem is not exclusive to crypto-companies' registration and characterizes the Union's market in various areas, as tax law. However, given the risk factors at play, a clear baseline – through sectorial Guidelines – should be established, at least at the anti-money laundering level, clearly detailing what the minimum requirements for registration are. Furthermore, the EBA and, in future, the AMLA, should closely monitor the registration requirements so to avoid such a race to the bottom.

From a European Union perspective, one of the arising questions with the introduction of MiCaR is how the registration duty provided by the Regulation coordinates with the anti-money laundering regime. Eminently, as we have mentioned, MiCaR is not an anti-money laundering regulation *per se*. However, especially when it comes to registration requirements, coordination is key. Eminently, a duplication of the registration duties would constitute an unnecessary burden

[107] European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU,* cit., 36, "*put in place a robust and consistent authorisation or registration regime for VASPs, bearing in mind also the wider need to ensure the consistency of approaches to addressing ML/TF risk; and b. establish a mandatory public register of VASPs that will be authorised or registered in the EU to support the identification of VASPs that are obliged entities under the AMLD*".
[108] See Chapter three section two.

for CASPs and contradict the aim of MiCaR of creating a clear, unified regime for the crypto-market.

Regarding the connection between such registration regime and the anti-money laundering legislation, the MiCaR explicitly refers to the latter at recital 16. There it states:

> "*entities offering services falling within the scope of this Regulation should also comply with applicable anti-money laundering and counter-terrorist financing rules of the Union, which integrate international standards*".

The coordination among the two fields is specified by article 62 which details the application process for CASPs. The article, at paragraph 2, letter i), includes among the information to be provided by the applicant:

> *"a description of the applicant crypto-asset service provider's internal control mechanisms, policies and procedures to identify, assess and manage risks, including money laundering and terrorist financing risks".*[109]

The duty at the registration level is then connected, through article 68, with the provisions detailing the governance requirements for CASPs. These governance requirements are among the criteria upon which the authorization, under article 59, has to be evaluated and granted. Article 68, paragraph 7, states:

> *"Crypto-asset service providers shall have in place (…) effective procedures and arrangements for risk assessment, to comply with the provisions of national law transposing Directive (EU) 2015/849. They shall monitor and, on a regular basis, evaluate the adequacy and effectiveness of those mechanisms, systems and procedures, taking into account the scale, the nature and range of crypto-asset services provided, and shall take appropriate measures to address any deficiencies in that respect".* To close the circle, article 64, paragraph 1, letter f), lists, among the grounds justifying the authorization's withdrawal, a CASP's failure to: "*have in place effective systems, procedures and arrangements to detect and prevent money laundering and terrorist financing in accordance with Directive (EU) 2015/849*".

The connection between the two fields is, then, further strengthened at the supervisory level. Article 94 states that supervision in the field of MiCaR shall be exercised "*in collaboration with other*

[109] The MiCaR also provides for a series of non-mandatory consultation processes (the supervisor may coordinate with the AML supervisor and FIU) in a series of cases as the withdrawal of authorization, the issuance of asset-referenced token, etc. see article 56, paragraph 5a; article 55, paragraph 4a, article 74, paragraph 4a.

*authorities, including authorities competent for the prevention and fight against money laundering and terrorist financing*".

The registration provided by the Fifth Directive will, hence, be superseded by the MiCaR's regime. This is clearly signalled by the absence of any reference to such a regime in any of the legislations composing the upcoming Anti-money Laundering Package (which will supersede the Fifth Directive).

At the same time, the Package provides for an additional regime customized for anti-money laundering compliance. Eminently, the solely national nature of MiCaR's registration may have the unintended effect of subtracting the covered entity from the control of each national Financial Intelligence Unit. Most importantly, it may hamper the cooperation between covered entities and National FIUs, as it would create a situation where the only reference point for anti-money laundering compliance would be the Unit of the home Country, irrespective of the location of the client and/or transaction. Such an arrangement could multiply the cooperation requests and flood the national FIUs – especially those located in crypto-hubs – with SARs connected with different Member States. At the same time, every follow-up question the FIU or investigative authorities would have regarding a SAR would have to be routed through the home Country's FIU.[110]

To avoid such a cooperation nightmare, the pending Proposal for an Anti-money Laundering Directive[111] provides for an *ad hoc* regime.

Article 5 of the Directive provides that:

> *"Member States may require (…) crypto-assets service providers operating through agents located in the host Member State and operating under either the right of establishment or the freedom to provide services, and whose head office is situated in another Member State, to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the entity operating on a cross-border basis, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request".*

[110] On the risks of passporting see European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU*, cit., 46-48

[111] Proposal for a Directive of the European Union, 20th of July 2021, n. 0250.

To avoid that the establishment of Contact Points recreates the abovementioned fragmentation, hence frustrating the same purpose of passporting, the Directive provides for a unified framework. Article 5, paragraph 2, of the Directive states that the (upcoming) European Anti-money Laundering Authority (AMLA) shall detail unified criteria in order to determine "*the circumstances in which the appointment of a central contact point (…) is appropriate, and the functions of the central contact points*".

In conclusion, the MiCa Regulation supersedes the national registration regime provided by the Fifth Directive. Registration is now only required in the home Member State and recognized across the Union.[112] The MiCa registration is complemented by the establishment of national contact points. Such contact points are not mandatory but can be established if required by the Member State's legislation. The establishment of a Contact Point is qualitatively different from to the registration regime. Eminently, the registration is an *ex-ante* requirement that implies an assessment of the CASPs governance structure. In contrast, contact points are aimed at facilitating *ex-post* supervision. In this sense, the national supervisor cannot impose additional controls to allow the CASP to operate. The contact point simply acts as a point of reference for the supervisor to guarantee compliance and facilitate dialogue concerning individual SARs. Contact points, hence, constitute a useful solution to avoid the multiplication of registration duties while maintaining national supervision.

### 4.2 The Registration regime and Decentralized Autonomous Organizations. A few thoughts

The Registration regime is quite a straightforward regulation when it comes to centralized arrangements: controls regarding the compliance infrastructure carried out by the supervisor before the entity commences its operations in a certain jurisdiction. The same cannot be said when

[112] This shift will require an adaptation period as currently both MiCaR and the Fifth Anti-money Laundering Directive are in force, hence, creating a duplication of the registration regimes. The unification, at a legislative level, will only be completed with the introduction of the AML Package envisioned for 2024. In the meanwhile, it will be up to national supervisors to decide how to coordinate the European registration regime (provided by MiCaR) with the National one (provided by the National legislation implementing the Fifth AML Directive).

analysing its implementation to decentralized arrangements. While the regulation of DAOs is the topic of the next chapter, a few points have to be addressed here as specifically connected with the registration regime. The points raised in this section will, then, be analysed in more detail in chapter five.

Particularly, two elements stand out as specifically contentious.

First, the interpretation of the CASP's "home jurisdiction" requirement under MiCaR. The Regulation identifies the home jurisdiction with the place where the entity is incorporated, or the individual resides. These criteria are already insufficiently clear for entities that operate in a digital world, with the risks of choosing the most complacent jurisdiction – generating the, above-mentioned, forum shopping phenomenon. However, when it comes to a DAO, the identification of the home jurisdiction is further complicated. Eminently, the legal qualification of such entities is currently at the fore of the debate. The European regulation has, so far, shied away from directly framing and regulating decentralized arrangements.[113] The MiCaR explicitly excludes decentralized organizations from its purview. This leaves DAOs in a legal vacuum and begs the question of whether such arrangements should be incorporated at all. In the end, a DAO is no more than a string of code (a bundle of smart contracts) users can interact with.[114] Software, in general, does not need to be incorporated. Hence, in the absence of *ad hoc* regulation, the question arises if DAOs should be either.

The requisite of the place of incorporation seems, accordingly, to not be appropriate when it comes to DAOs. An option could be to translate such a parameter as identifying the home jurisdiction with the place where the decentralized software is developed. This interpretation would be in line with the FATF's multiple references to pre-launch, engrained compliance. When it comes to pre-launch requirements, the object of engrained compliance duties is not the DAO per se, but its developer/s. If by-design compliance has to be pursued, the jurisdiction best placed to do so is where the developer/s is located. This would also be in line with the manner centralized software

[113] As detailed in Chapter 5 the initial text of MiCaR approved by the Parliament did bear a definition of Decentralized Autonomous Organization. However, in the final text such definition has been eliminated and DAOs have been excluded from the purview of the Regulation.

[114] For an example of a DAO's functioning see the description of "The DAO" project at Chapter 1, para. 3.2.

is currently regulated. Eminently, the location of the developer is usually identified as the jurisdiction where the software legally resides.

Nonetheless, the identification of such a place may be complex when it comes to decentralized autonomous organizations.

If the DAO is developed by an incorporated company or a single individual, we have an easy case. The registration requirement can be shifted from the CASP's place of incorporation to the developers'. This shift is not textually provided, as the law only refers to the regulated entities' place of incorporation whereas, under this interpretation, the registration would be imposed where the regulated entities' developer is incorporated. Nevertheless, such extensive interpretation is not far-fetched and in line with the criteria detailed by the FATF Guidance. The main pain point of this interpretation being the qualification of the software developer as a covered entity.[115] Eminently, the qualification of the software developer as a covered entity is a prerequisite to impose on the latter compliance duties.

However, if the DAO is developed by a loosely connected network of developers across the world, we have a harder case. In the absence of a clear regulation, the question arises of where the developer is located. The risk being either a legal vacuum or a multiplication of the duties for each jurisdiction where there is at least one active developer. In such cases, a mere extensive interpretation does not seem sufficient. A clear European framework to identify the duties of DAOs' developers – if any – should, hence, be provided to avoid regulatory arbitrage.

Such a clear framework for the registration of DAOs would be, in any case, advisable. Eminently, also considering the liability – administrative and possibly criminal[116] – connected with non-compliance, a developer should know the 'if', 'where', and 'how' of their legal duties. Differently, a violation of the principle of foreseeability of the criminal sanction could be argued.[117] The regulation seems, in contrast, to be, at best, confused. Eminently, notwithstanding the multiple

[115] For an in-depth reflection on the qualification of the software developer as CASP see the following Chapter.
[116] For more on the sanctioning system see chapter 3, section 2.4.
[117] For an example of how such a case-by-case approach may lead to the criminal indictment of software developers see chapter 5 section 5 on the Tornado Cash case. There, the software developer of Tornado Cash, a DAO acting as a mixer, has been arrested in connection with the actions pursued by its software. Such an indictment raises a problem of foreseeability when the compliance duties of software developers are not clearly identified.

references to engrained compliance, the FATF Guidance excludes mere development from its purview. Similarly, the MiCaR explicitly excludes DAOs and issuers from the overall regime. At the same time, completely excluding DAOs from any *ex-ante* controls will be complex, especially when these are extensively used for criminal purposes. The risk is, then, a case-by-case approach adopted by judiciary and supervisory authorities in the absence of a clear overarching legislation.[118]

The second moment of friction is when the registration is required by jurisdictions where the DAO operates, but not where it has been developed – from now on "secondary registration". As underlined by the Task Force, development may be the only window of opportunity for the regulator when it comes to decentralized arrangements. Once the DAO is launched, its rules of conduct are engrained in the smart contract and no longer modifiable, with non-modifiability being one of the main selling points of such arrangements. This begs the question of how post-launch compliance can be imposed on an autonomous software. Furthermore, if the DAO is indeed decentralized it means no human is in control of its actions. Who should the supervisor then talk to in order to enforce such a duty?

To address this second problem, a clearer registration regime for DAOs should be provided. One that, if registration is indeed mandatory, imposes on the home jurisdiction the establishment of by-design requirements that allow secondary registration. An example of such requirements being the establishment of a compliance governance body that retains at least partial control of the DAOs functioning – through kill switches and/or backdoors that allow the adjustment of the smart contracts to the requirements imposed by secondary jurisdictions. Furthermore, rules should be imposed to guarantee the DAO does not operate in jurisdictions where it has not been registered.[119]

## 5. The Travel Rule Regulation. A primer for architectural policy-making?

[118] For more on this topic see chapter 5.

[119] For an in-depth analysis of possible solutions to the regulation of Decentralized Autonomous Organizations see Chapter 5 where the two mentioned strand are further developed. Particularly, for an example of a possible governance framework see Chapter 5, Section 3.

## 5.1 An introduction to the Travel Rule

The extension of the travel rule to crypto-assets is fairly recent, however, this is a requirement that has long been applied by financial institutions. It is, hence, necessary to concisely detail its general discipline before delving into its extension to the crypto-assets market.

The travel rule is provided by Recommendation 16 of the FATF's Standard[120] which states:

> *"Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain".*

As detailed by its interpretative note, the crux of the Recommendation is the mitigation of the risk generated by wire transfers. The aim is to avoid that wire transfers can be used as a means to move and launder illicit funds. To this end, the travel rule has the purpose of guaranteeing that all the parties involved in a wire transfer (sending and receiving financial institution) have a complete understanding of the transaction and connected risk factors.

Eminently, in a wire transfer each intermediary involved only sees its side of the exchange. Each financial institution knows its customer and evaluates whether the transaction is in line with its profile. However, this creates a one-sided perspective on the risk. To have a complete picture, it is necessary that all involved intermediaries not only see their side of the transfer but also the counterparties'. This additionally allows to evaluate whether the transaction is part of a pattern and connect other related transactions.[121]

[120] These forty Recommendations were published, in their latest version, in 2012, and constitute the backbone of the sectorial regulation. See Financial Action Task Force, *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations,* cit.

[121] This is particularly relevant to hamper money laundering practices as smurfing or structuring. Smurfing consists in dividing a large transaction is several smaller transactions. The aim is avoiding triggering compliance controls or automatic SARs that may be activated above a certain threshold. Furthermore, smurfing may be used as a means to conceal the real consistence of a certain transaction, see Department of Finance Canada, *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada,* March 2023, 18.

To this end, Recommendation 16 states that each wire transfer should include "accurate" originator and beneficiary information. Accurate means the information is verified – in the sense detailed above – by the covered entity or by the counterparty.

Recommendation 16 has been implemented within the European Union by Regulation n. 847 of 2015.[122]

The Regulation applies – following article 3, number 9 – to any transfer of funds, at least partially executed electronically, where at least one of the two service providers involved in the transaction is established within the European Union.[123] Encompassed are not all value transfer, as a series of exception are provided by article 2 of the Regulation – i.e., cash withdrawals, payments for goods and services, transfers of value between two institutions in their own name, etc. In brief, the Regulation covers all exchanges of value carried out by two private customers with the intermediation of one or more payment service providers.

The Regulation then details the content of the identification and verification duties.

On the side of the originator, the service provider has to attach to each transfer of funds the following information: the customer's name, account number, ID number, number of identification of the customer, place, and date of birth; for the counterparty, name, and account number.[124] On the side of the beneficiary, the service provider has to only verify that the information required by the Regulation is attached to the wire transfer and verify the veracity of the data concerning its customer.

A key element for the concrete implementation of the travel rule is the allocation of the duty to verify the veracity of the information connected with the wire transfer. This is an element that will be crucial for the implementation of this rule to crypto-assets.

As mentioned, the verification duty is a resource-intensive activity in terms of compliance.[125] This because it entails additional activities by the regulated entities aimed at ascertaining the veracity of

[122] Regulation of the European Union, n. 847, 20th May 2015.

[123] For a definition of payment service provider see Directive of the European Union, 25th November of 2016, n. 2366.

[124] Such duties are partially reduced by the Regulation where the transfer is within the EU (article 5), or concerns sums under Euros one thousand (article 6 para. 2).

[125] See section 2.2 of the present chapter.

the information provided by the customer. To avoid overburdening covered entities, the travel rule breaks down the verification duty between the two intermediaries. Each intermediary only has to verify the information pertaining to its customer and simply identify the counterparts. This way the verification activity is pursued by the intermediary only concerning the individual with whom they have a direct contact – i.e., their customer.

## 5.2 The extension of the Travel Rule to the crypto-assets market

Trailblazer in the extension of the travel rule to crypto-assets has been the Financial Action Task Force. If the applicability of Recommendation 16 to crypto-assets service providers was already hinted in the first Guidance of 2015,[126] it is only in 2019 that the FATF detailed how such a duty should be extended.[127] Eminently, the original wording of Recommendation 16 clearly restricted its purview to wire transfers.

Wire transfers were defined as:

> *"any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to beneficiary person at a beneficiary financial institution".*[128]

Crypto-assets transactions were, hence, initially considered outside of the purview of Recommendation 16 for two main reasons. First, CASPs are not qualified as Financial Institutions but belong to a separate category. Second, crypto-assets are conventionally not qualified as a currency in the anti-money laundering field.[129] At the same time, crypto-assets' transfers were perceived as qualitatively similar to wire transfers in terms of risk. Eminently, transactions in

[126] Financial Action Task Force, *Virtual currencies,* cit., 10, "*Countries should ensure that when convertible virtual currency exchangers conduct convertible VC transfers that are wire transfers, they include required originator and beneficiary information specified by Recommendation 16*".

[127] Financial Action Task Force, *The FATF Recommendations,* cit., 77, for a chronology of the policy evolution see 138; World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach*, cit., 16.

[128] See Financial Action Task Force, *Guidance for a Risk-based approach for Money or value transfer services,* Paris, 2016, 9.

[129] For a reflection on the definition of crypto-assets see Chapter 3.

crypto-assets constitute an exchange of a valuable token executed through electronic means between two parties.

To close this perceived gap, the Guidance of 2019 clarified that Recommendation 16 does apply to any exchange of value executed by a CASP.[130] The Guidance explicates that, due to the functional and not formal nature of the FATF's norms, the travel rule has to be applied to any exchange of value that, *in concreto,* performs a function similar to a wire transfer, even if not formally qualifiable as a wire transfer. With special regard to crypto-assets, the Guidance explicitly extends the purview of the travel rule to two types of operations: 1) traditional wire transfer carried out by a CASP; 2) crypto-assets transfers between a CASP and another covered entity.[131]

Following our previous analysis, it should be easy to spot the weak point of such an extension: in contrast with traditional electronic transfer of funds, transfers of crypto-assets do not always involve a covered entity as they can also be carried out with or by a self-hosted wallet.[132] This is not to mean that the extension is per se incorrect. Rather than the extension of a rule envisioned for a fully intermediated market – the wire transfers one – to a disintermediated one opens a new front not previously envisioned by the policy maker: the policing of peer-to-peer transactions and peer-to-intermediated ones which did not previously exist.

It is the same Guidance to recognize this fallacy and the connected breach crypto-assets open in the effectiveness of the travel rule as it states:

> *"The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer (e.g., when an ordering VASP or other obliged entity sends VAs on behalf of its customer, the originator, to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer using his/her own distributed ledger technology (DLT) software, such as an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of* Recommendation 16 *with respect to their customer (the originator or*

[130] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 29.

[131] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 29.

[132] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 30; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 65.

> *the beneficiary, as the case may be). The FATF does not expect that VASPs and financial institutions, when originating a VA transfer, would submit the required information to individual users who are not obliged entities. VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user using his/her own DLT software, such as an unhosted wallet), should obtain the required originator information from their customer*".[133]

Such a weakness is, as detailed in the remainder of this thesis, cross-sectional to the whole anti-money laundering strategy in the field. As the market moves from a completely intermediated to an (at least partially) disintermediated electronic funds transfer system, an intermediary-centred strategy will necessarily miss a part of connected transactions. If traditional wire transfers are always carried out by an intermediary, the same does not apply to crypto-assets transfers.[134]

When it comes to the travel rule there is one specific type of disintermediated transfer that generates a legal puzzle: those transfers that are intermediated only on one side of the transaction – meaning a CASP-to-self-hosted transaction.

An exchange of value that is completely disintermediated generates a problem of efficacy of the legislation. In contrast, a transfer only unilaterally intermediated creates a problem of interpretation. In the former case, there is no doubt that the Regulation does not apply. The transaction is carried out by two private parties that are under no obligation to comply with the anti-money laundering legislation. In contrast, when the transaction is carried out between a covered entity and an individual this creates a new scenario compared to the pre-existing wire transfer market, insofar covered by the travel rule. This is a transaction where there is a possibility of control, as a covered entity is involved. However, this is a form of control that was not envisioned when the travel rule was first established.

The main question the legislature had to deal with is, hence, whether and up to what extent should travel rule requirements be applied in such on-sided transactions. Most importantly, should the verification duty of the CASP extend to the self-hosted counterparty?

[133] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 30.

[134] To underline such a difference is also, European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU*, cit., 40.

The answer to this question is the crux of the legislative dilemma created by the travel rule in the field.

The solution adopted by the FATF, in the above quoted Guidance of 2019, is a conservative one: when a transfer is addressed or received by an unhosted wallet, the CASP has to solely identify the self-hosted counterparty through a declaration released by its customer.[135] This means the CASP has no duty to corroborate the truthfulness of the information provided by its customer, but simply to ask and record the answer. This is a suboptimal solution in terms of financial flows monitoring as, in traditional transactions, data of both the originator and addressee are verified. In contrast, when it comes to crypto-assets, the information concerning the self-hosted wallet is solely based on a declaration by the CASP's customer.

The latest FATF Guidance, published in October 2021, which, for the first time devotes ample space to clarifying the application horizons of the travel rule, takes a substantially similar approach to its 2019 predecessor.[136] At the same time, the Recommendation opens the door to additional, more stringent requirements. The Guidance states that, while the general recommendation remains unaltered, individual jurisdictions or covered entities may go beyond it, particularly, by providing for additional obligations or cautions in the case of transactions with self-hosted wallets. Such measures can include: classifying each transaction with a self-hosted wallet as high-risk, and thus subject to more stringent compliance obligations, or even banning transactions with self-hosted wallets.[137]

## 5.3 The European take on the travel rule. A primer for architectural regulation?

[135] Financial Action Task Force, *Guidance for a risk based approach to virtual assets and virtual asset service providers*, cit., 30.

[136] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 65, "*The FATF does not expect that VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities. VASPs sending or receiving a VA transfer to/from an entity that is not a VASP or other obliged entity (e.g., from an individual VA user to an unhosted wallet), should obtain the required originator and beneficiary information from their customer*".

[137] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 87.

In July 2021, the European Commission presented a proposal for a regulation on the application of the travel rule to the crypto-assets market.[138] The proposal amends the general travel rule Regulation of 2015.[139]

The Commission's proposal did not mention self-hosted wallets, hence restricting its purview solely to CASP-to-CASP transactions. However, the European Parliament pushed, since the start, for an extension of the purview of the travel rule also to transactions with self-hosted wallets and, in particular, to unilaterally intermediated transactions (CASP-to-self-hosted).[140]

To this end, the proposal of the Parliament[141] provided for a CASP's duty of verification for any transaction involving a self-hosted wallet. Under the proposal, the CASP had to verify not only its customer's information but also the data concerning the owner of the self-hosted wallet. The first political agreement on the Regulation had mitigated such an obligation by providing, at article 14 and sixteen, a duty of verification only where the transaction exceeded one-thousand euros.[142] Under such a threshold the rule applied was the one provided by the FATF: simple identification based on the information provided by the customer.

[138] Proposal for a Regulation of the European Union, 20th July 2021, n. 0241.

[139] Regulation of the European Union, 20th May 2015, n. 847; A. Minto, *Riflessioni sull'applicabilità della disciplina antiriciclaggio ai Non-Fungible Tokens ("NFT")*, cit., 34.

[140] European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets*, 6th of April 2022, Rapporteurs: Ernest Urtasun, Assita Kanko.

[141] See European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets*, cit., art. 14 para. 5b, "*in the case of a transfer of crypto-assets made to an unhosted wallet, the provider of crypto-asset transfers of the originator shall collect and retain the information referred to paragraphs 1 and 2, including from its customer, verify the accuracy of that information in accordance with paragraph 5 of this Article and Article 16(2), make such information available to competent authorities upon request, and ensure that the transfer of crypto- assets can be individually identified*", ed art. 16 co. 4a, also see, recital 29a "*The provider of crypto-asset transfers should verify the accuracy of information with respect to the originator or beneficiary behind the unhosted wallet, and ensure that the transfer of crypto-assets can be individually identified*".

[142] European Parliament, *Provisional Agreement resulting from interinstitutional negotiations on Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets,* cit., see also recital 29b, "*In case of a transfer to or from a self-hosted address, the crypto-asset service provider should collect the information on both the originator and the beneficiary, usually from their customer. The crypto-asset service provider should in principle not be required to verify the information on the user of the self-hosted address. Nonetheless, in case of a transfer whose amount exceeds EUR 1 000 and is sent or received on behalf of a customer of a crypto-asset service provider to or from a self-hosted address, that crypto-asset service provider should verify whether such self-hosted address is effectively owned or controlled by that customer".*

The interesting aspect of this extension is that it changes the nature of Recommendation 16 in a way that directly affects the conformation of the market and the technology itself. Indeed, Recommendation 16, in the traditional market, is intended to require intermediaries to include in a wire transfer information they should already possess because of the Know Your Customer they performed during the onboarding phase. In contrast, in the crypto sphere, the travel rule creates a new profiling obligation extended to a party who has no prior relationship with the covered entity – i.e., the owner of the self-hosted wallet. A profiling obligation which would have to be pursued by carrying out a new Know Your Customer of the counterparty.

This regulatory approach generates a significant discrimination between intermediated and self-hosted wallets. Significantly, to transact with a self-hosted wallet, an intermediary will incur in higher compliance costs than when transacting with another intermediated wallet. This generates a risk of triggering a de-risking phenomenon by intermediaries.[143] At the same time, the holder of a self-hosted wallet, to transact with an intermediated wallet, will be forced to de-anonymize their account suffering a much greater compression of their confidentiality than when transacting with another self-hosted wallet.

The discrimination in question is of particular interest because it represents a (more or less conscious) attempt by the legislator to influence the conformation of the market so to favour its legislative goals. Significantly, through the legislation in question, the legislator makes transactions through self-hosted wallets more resource intensive (for intermediaries) and less private (for individuals). The change imparted by the legislation is all the more relevant when one considers that this goes against the fundamental innovation of blockchain: the possibility of exchanging value online without the need to use an intermediary.

The approach of the European legislature in this pending proposal poses two main problems.

The first problem is that the legislation risks fracturing the crypto market into two mutually segregated sectors, with interactions becoming burdensome and intrusive for the disintermediated side, and costly, for the intermediated side. On the other hand, while one understands the reasons why the legislator would want to push the crypto-market towards increasing intermediation, the

[143] For the meaning of de-risking and its impact see Section 2.1 of the present Chapter.

risk in doing so is to thwart the innovative core of crypto-assets,[144] which, in large part, lies precisely in the ability to exchange value digitally in a disintermediated fashion.

A second problem posed by this approach is the disproportionate impact of such an obligation on individual privacy. The entire privacy structure of crypto-assets is based on pseudonymity.[145] The pseudonymity is rooted in the fact that the user's account – its public key – provides no information about the identity of the individual behind it. If the veil of pseudonymity is torn, the individual user is exposed to a level of monitoring far more penetrating than in traditional financial transactions.[146] Significantly, in the traditional financial system, information is centrally stored by each intermediary in private ledgers. Such information is logically fragmented, as each intermediary only records the transactions and balances of their own customers nothing knowing about the customers of other intermediaries. In contrast, the blockchain ledger is public and accessible to anyone. Moreover, the connected information is logically centralized as each transaction carried out through a crypto-asset is recorded consequentially in a single ledger. This implies that, once the public key is de-anonymized, anyone can analyse and monitor the financial activity of a given individual, thus, accessing highly sensitive data. In this sense, forcing the owner of a self-hosted wallet to identify themselves poses a significant privacy problem, as it obliges them, for the sole purpose of performing a transaction, to disclose their entire financial history to the counterparty's CASP.[147]

These technical notations would have made the concrete implementations of such a legislative solution problematic. The European co-legislator, hence, ultimately reached a kind of middle ground solution. This solution is the topic of the next section.

[144] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 95, "*attempts to force the regulatory model on decentralised and peer-to-peer transactions will broadly sweep in innocent conduct and hamper innovation in this space*".

[145] For more on crypto-assets' privacy structure see chapter two section six.

[146] For a further reflection on the connection between privacy, blockchain transparency, and anti-money laundering monitoring see section 6.3.

[147] See the dissenting opinion to the proposal as approved by the Parliament of MEP Gunnar Beck according to whom "*By going beyond the FATF rules, crypto users with private, self-controlled wallets will be discriminated against and treated differently than people with cash. Every single transaction is potentially "travel rule eligible" and would have to be reported. This is a blatant violation of data protection law and is reminiscent of the behaviour of totalitarian surveillance states*", see European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets*, cit.; see also The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 95.

## 5.4 The final text. Postpone, postpone, postpone?

The final text of the Regulation, published in May 2023,[148] reached a somewhat confusing middle ground.

Eminently, article 3, paragraph 10, clarifies that the requirements of the Regulation apply to all transfers of funds including to or from self-hosted addresses. However, the extension is not complete. For transfers under one-thousand euros the FATF's rule applies: CASPs must solely identify the counterpart's information based on the customer's declaration. For transfers that exceed such a threshold, the Regulation requires CASPs to take adequate measures to assess whether the self-hosted address is owned or controlled by the originator.

This is a confusing solution from an interpretative perspective. Eminently, it remains unclear whether it should be read as a prohibition of all transactions to self-hosted addresses above the threshold not controlled by the customer or as a restriction of the verification duty only to such transactions. What is confusing is that, if the second interpretation is correct, it is unclear why increased compliance duties have been placed on transactions between the customer and their wallets and not on all transactions with self-hosted wallets. Truly, there is no reason to consider the first riskier compared to the second. Furthermore, the concept of "adequate measures" is not further specified. It is unclear whether this overlaps with verification procedures or it is a more flexible concept to be applied on a case-by-case basis by the covered entity.

It can be argued that the reason for such a choice is solving the problem by dodging it. Eminently, the problems analysed in the previous section are strongly reduced if the verification duty is restricted to transactions with self-hosted addresses owned by the customer. In terms of compliance costs, the increase for the covered entity is minimal: the CASP does not have to verify the information provided by a third party as the account is owned by its customer whose identity has already been verified. From the customer's perspective, the privacy restriction is present but

[148] Regulation of the European Union, 31sr May 2023, n. 1113.

less relevant as the customer is already using a centralized service provider and, hence, accepts a certain level of monitoring from the latter.

This explication seems to be confirmed by the rest of the Regulation. Eminently, the text partially delegates the overall problem connected with self-hosted addresses to supervisors and supervised and partially postpones it (as MiCaR with regards to DAOs and NFTs).

In the first sense, article 19b states that:

> *"Member States shall require crypto-asset service providers to identify and assess the risk of money laundering and terrorist financing associated with transfers of crypto-assets directed to or originating from a self-hosted address. To that end, crypto-asset service providers shall have in place internal policies, procedures and controls. Member States shall require crypto-asset service providers to apply mitigating measures commensurate with the risks identified".*

These include "*taking risk-based measures to identify, and verify the identity of, the originator or beneficiary of a transfer made to or from a self-hosted address or the beneficial owner of such originator or beneficiary*". This risk-based measure replicates the Parliament's proposal simply shifting it from overall regulation to concrete guidelines.

However, this guidance to National authorities seems to be at odds with the overarching policy goal of the sectorial Union's regulation: provide for a level playing field across the bloc. Eminently, certain Member States may implement such guidance as a mandatory verification requirement while others may not. This would fracture the common market as a covered entity would be mandated to verify the information depending on the Member State where the transaction is being carried out. Furthermore, such an uneven approach raises the question of how the covered entity should ascertain where the transaction is being carried out. Eminently, if the general rule is simple identification, how can the covered entity be sure what is the location of the self-hosted wallet's owner? The customer may simply lie and identify its counterparty as belonging to a Member State where mandatory verification is not required.

In the second sense, article 37, requires the Commission, by June 2027, to issue a report assessing the risks posed by transfers to or from self-hosted addresses as well as the need for specific measures to mitigate those risks, and propose, if appropriate, amendments to the Regulation. This way the legislature postpones addressing, at a regulatory level, the most concerning issues.[149]

It will, then, be up to the Commission and supervisory authorities to evaluate the impact of the exclusion spelled out by the co-legislators and decide on an extension of the travel rule beyond hosted wallets.

## 6. Blockchain analytics and compliance. A new tool for anti-money laundering?

The last section of the present chapter is devoted to a compliance trend rooted in the specific characteristics of blockchain's data structure: blockchain analysis. Before delving into the concrete functioning of such a technique, the present section details the overarching themes and regulatory trends such a technique has spurred. Section six-one will, then, detail the functioning and logic of blockchain analytics tools. Section six-two will reflect on the impact such a technique may have on the future regulatory strategy. Finally, section six-three will briefly examine the impact of such techniques on the privacy regulation.

As detailed throughout the thesis, blockchain modifies the way financial data is stored and managed. With blockchain, data transitions from private, fragmented ledgers to public, logically unified ones.[150] The shift entails a reduction in the role of financial institutions and, in general, intermediaries. Intermediaries lose control of the financial ledger of which they simply become a (possible) node. The entry and exit points to the ledger are no longer under the sole control of an intermediary as the same is decentralized both in terms of access and governance.

[149] This approach of dodging the most contentious issues and postponing them to a later date seems to characterize the whole sectorial regulation. Eminently, the MiCaR takes the same approach when it comes to the regulation of Decentralized Autonomous Organizations and Non-fungible Tokens, where the decision concerning their inclusion is deferred to a later date.

[150] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023,* cit., 5.

If this shift reduces the role of intermediaries as necessary checkpoints of the system, it also changes the accessibility and traceability of financial data.[151] Blockchain data is, by-design, public[152] as there is no more a gatekeeper that owns and stores the ledger. At the same time, the presence of a single ledger for the whole network means the information is logically unified. Private ledgers only store partial information – i.e., the transactions carried out with a certain intermediary. In contrast, blockchain ledgers store all transactions carried out with a crypto-asset in a consecutive fashion. Furthermore, such information is unmodifiable. Transactions can be analysed and traced irrespective of their date and any data retention policies.[153]

These characteristics of blockchain have spurred the development of a partially new compliance method: blockchain analysis. The public nature of the ledger means anyone can analyse it. Criminal activity carried out through crypto-assets is visible, even though not always apparent, to anyone. The unified nature of the ledger enhances the effectiveness of such an analysis. In traditional systems, a criminal could simply use different intermediaries to obfuscate its money trail. It would then be up to investigators to gain access to each ledger and piece together the money trail. With blockchain, the money trail can be followed *ad infinitum* as long as a certain crypto-asset is used.[154] Additionally, there is no need to request for access as the ledger is readily available.

This compliance technique is only partially new. Covered entities already employ and are mandated to carry out – as we have seen in the section on Customer Due Diligence[155] – transaction monitoring on their customer's activities. However, with blockchain, such monitoring is

[151] C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 3.

[152] A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 1; N. Tovanich – R. Cazabet, *Pattern Analysis of Money Flows in the Bitcoin Blockchain* in *Complex Networks and Their Applications* in *XI: Proceedings of The Eleventh International Conference on Complex Networks and Their Applications: COMPLEX NETWORKS 2022*, 1, 2023, 1; here we refer again to permissionless networks as permissioned one have a different data structure. World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 3

[153] A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 5; European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 14.

[154] A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 5; it has still to be underlined that such a characteristic of blockchain only applies to transaction that are carries out with one coin. If the individual changes its coin the transaction trail gets fragmented and loses its consequentiality. On the characteristics and effectiveness of this money laundering tactic, also known as "chain hopping", see A. Moiseienko – O. Kraft, *From money mules to chain hopping. Targeting the finances of cybercrime,* cit., 40 – 41; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26.

[155] See Section 2.2 of this Chapter.

significantly expanded in two senses. First, the covered entity can analyse all the transactions carried out by their customer, whereas in centralized ledgers they can only consider transactions executed with their systems. Second, anyone can conduct such an analysis. Whereas, in centralized systems, the analysis can only be performed by the owner of the ledger. With blockchain anyone – including Law Enforcement Authorities, supervisors, NGOs, and academics – can analyse blockchain transactions directly.[156]

As noted by Verduyn[157] "*The paradox of blockchain technology is therefore that while AML efforts must deal with imperfect knowledge of identities, they may exploit perfect knowledge of all transactions"*.[158] Based on these characteristics of blockchain, several companies have started offering blockchain analytics tools,[159] examples being Elliptic,[160] Chainalysis,[161] or TRM Labs.[162] Such tools allow to perform a wide range of analytics activities on blockchain ledgers, from simple tracing to more complex analysis aimed at identifying patterns or clusters of connected accounts/transactions.[163]

The use of blockchain analytics tools, hence, has a direct impact on how covered entities and States approach compliance. For companies, it extends their ability to assess customer risk by analysing transactions not carried out within their systems.[164] For States it changes the way they exert supervision. Blockchain accessibility opens a new regulatory avenue: direct monitoring of financial data by the supervisor. The public nature of the ledger disintermediates the relationship between supervisor and information bypassing the need to rely on intermediaries for monitoring.[165]

[156] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., viii.

[157] M. Campbell-Verduyn, *Bitcoin, crypto-coins, and global anti-money laundering governance,* cit., 298.

[158] On a similar note, A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 2, "*As cryptocurrencies rely on cryptographic protection and a decentralised peer-to-peer system, money ownership is implicitly pseudonymous, while its flow is publicly available and visible*".

[159] Together with private analytics tools there is also a wide range of free analytics tools that can be accessed and used.

[160] https://www.elliptic.co/.

[161] https://www.chainalysis.com/.

[162] https://www.trmlabs.com/.

[163] For more on the functioning and logic underlying these tools see the next section of the present chapter. A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 3; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 91, for more on these techniques see the next section; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial,* cit., 62.

[164] M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., 3505.

[165] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023,* cit., 5.

This architectural change, and its impact, have been underlined by regulators worldwide. The European Commission, the FATF, the US Department of Treasury, and the World Economic Forum have all directed covered entities and supervisors to employ analytics tools as a risk mitigation strategy.[166] Consequently, supervisors, police and intelligence agencies[167] as well as covered entities have started using such tools extensively.[168]

Particularly, blockchain analytics impacts both dimensions of anti-money laundering compliance: the supervisory and the compliance one. This duplicity is underlined by the Financial Action Task Force in its Guidance of 2021:

> "*A number of jurisdictions are using, or exploring using, blockchain analytics services to assist with their supervision. The services can be used in a number of ways, including to pinpoint areas that supervisors may wish to focus on during assessments of individual VASPs and helping to categorise the highest risk VASPs based on their activity. There is a cost consideration with these tools and not all VAs are covered by all vendors. Blockchain analytics are also widely used by VASPs and some FIs to monitor their own exposure to risk (e.g., VA transfers that have passed through mixer services or come from privacy wallets)".*[169]

The FATF, hence, identifies two main dimensions of blockchain analytics impact.

[166] European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 102, "*We note, however, that crypto-assets transactions conducted on public distributed ledgers leave immutable traces and are there for everyone to see. Persons engaging in ML/TF via such crypto asset transactions expose themselves to public scrutiny of their transactions. Europol should consider using blockchain analysis tools in order to analyse addresses and transactions for critical information such as geolocation data or the cryptocurrency exchange (used to purchase the coins)"*; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 3; World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 33; Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 36, "*A number of jurisdictions are using, or exploring using, blockchain analytics services to assist with their supervision. The services can be used in a number of ways, including to pinpoint areas that supervisors may wish to focus on during assessments of individual VASPs and helping to categorise the highest risk VASPs based on their activity. There is a cost consideration with these tools and not all VAs are covered by all vendors. Blockchain analytics are also widely used by VASPs and some FIs to monitor their own exposure to risk (e.g., VA transfers that have passed through mixer services or come from privacy wallets). It is important to consider any potential implications for privacy and data protection in the use of such tools, if they allow transparency that is not otherwise available (e.g., on public blockchains)";* The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 91.

[167] A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 1.

[168] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 3.

[169] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 71.

First, at a supervisory level, the analytics tools can be used to perform the risk-assessment function and the supervisory one.[170] In the first sense, through blockchain analytics, supervisors can assess the composition of the market, evaluate the level of penetration of crypto-assets in their economy, hence, decide how to allocate resources. They can also use it to identify parts of the market that are of particular concern – for instance, an extensive use of self-hosted addresses, privacy-enhancing tools, frequent contact with DeFi arrangements, or with CASPs located in high-risk jurisdictions – and intensify controls accordingly. In the second sense, they can use it to monitor the activity of a single CASP and supervise it in a manner non-intrusive for the covered entity. Furthermore, when conducting a review of the CASP's activity they can integrate the information provided by the latter with the open-source information bore by blockchain to verify it.[171]

Second, at a covered entity level, the tools can be used to better assess the customer risk and monitor its activity.[172] The covered entity can use the information provided by the blockchain to assess their customer's activity and enrich the Know Your Customer and transaction monitoring function. Explicitly mentioned elements of relevance in such an assessment are the interaction of the customer with mixers or other privacy-enhancing tools as well as self-hosted wallets.

At the Union level, this double dimension of blockchain analytics is equally reflected.

At a policy level, while the Fifth Directive did not mention such tools, references to it are made in the newly introduced legislations. Particularly, the Travel Rule Regulation, at article 37, paragraph 3, letter b), directs the Commission to draft:

> *"an assessment of the technological solutions for complying with the obligations imposed on crypto-asset service providers under this Regulation, including of the latest development of technologically sound and interoperable solutions for complying with this Regulation and of the use of DLT analytic tools for identifying the origin and destination of transfers of crypto-assets and for performing a 'know your transaction' (KYT) assessment".*

At the same time, recital 17 directs the EBA to

[170] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023,* cit., 5.

[171] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023,* cit., 5.

[172] US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 12, "*Blockchain analytics can also be a useful tool for the private sector to provide information on risk, support a risk-based approach to compliance, and review customer activity at onboarding and on a periodic or event-triggered basis*".

> *"issue guidelines specifying the enhanced due diligence measures that obliged entities should consider applying to mitigate such risks, including the adoption of appropriate procedures such as the use of distributed ledger technology (DLT) analytic tools, to detect the origin or destination of crypto-assets".*

Such references are not reiterated in the AML Package. However, their inclusion in the Travel Rule Regulation (the latest anti-money laundering policy to be approved) points in the direction of an inclusion in the final texts of the legislations composing the Package to be adopted in 2024, currently under the evaluation of the co-legislators.

The attention towards blockchain analytics tools is confirmed at the supervisory level by the, abovementioned, European Banking Authority's draft guideline.[173] The draft explicitly mentions these tools in several parts. At a general level, guideline 4 on transaction monitoring directs covered entities to evaluate:

> *"whether the use of advanced analytics tools, like the distributed ledger analytics tools, is necessary in light of the ML/TF risk associated with the firm's business, and with the firm's customers' individual transactions".*[174]

In a similar way the Sectorial Guidelines directs covered entities to apply:

> *"advanced analytics tools to assess the risk of transactions, particularly for transactions involving self-hosted addresses. Based on the nature of the CASP, it might be sufficient to apply advanced analytics tools to transactions on a risk-sensitive basis, as a supplement to the standard transaction monitoring tools. Such tools are crucial to trace the history of transactions, individual coins and to identify links with criminal activities, persons or entities".*[175]

[173] European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terro rist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* cit.

[174] European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terro rist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* cit., 17.

[175] European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terro rist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* cit., 32.

Furthermore, among the risk mitigation measures that can be implemented as part of the Enhanced Due Diligence the draft includes:

> *"assess more frequently or in more depth the activities performed through the crypto asset accounts used by the customer by using a crypto investigation tool (EDD risk mitigation Measure)"*.

This promotion of blockchain analytics techniques is also connected with the increasing wariness towards anonymity-enhancing technologies that stand in the way precisely of this type of analysis. The EBA classifies privacy-enhancing technologies – as privacy wallets, mixers, etc. – as factors that heighten the money laundering risk and warrant a closer examination by the covered entity. In a similar fashion, the FATF's Guidance of 2021 requires:

> "V*ASPs licensed by or operating in their jurisdiction can manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to AECs, mixers, tumblers, privacy wallets and other technologies that obfuscate the identity of the sender, recipient, holder, or beneficial owner of a VA. If the VASP cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities*".[176]

To sum up, the use of blockchain analytics tools constitutes one of the latest trends in the anti-money laundering regulation of crypto-assets. Both the FATF, in its Guidance of 2021, and the Union in its most recent regulation and guidance underline their value as a tool for both supervisors and covered entities. At the same time, the use of blockchain analytics is promoted through the identification of all services that blur the transaction trail as high-risk or, even, barred. We will return to this point in section seven-three on the clash between privacy and anti-money laundering regulation.

Notwithstanding its usefulness, blockchain analysis is certainly not a magic tool. The pseudonymity of crypto-assets entails that, while illicit or suspect transactions can be identified, it may still be exceedingly hard to identify the individuals behind such transactions – i.e., deanonymize accounts. This means that, in the absence of any instrument that allows to freeze a suspect's transaction, simple transaction monitoring may be a passive exercise.[177] Furthermore, criminals can use an array

[176] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 55.

[177] As underlined by A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 5, "*once information is published, it is nearly impossible to remove it*"; World Economic Forum,

of techniques to blur the transaction trail. Mixers, Privacy Coins,[178] chain hopping can all be employed to diminish the usefulness and transparency of blockchain data.[179] Finally, blockchain analytics techniques are still in a nascent stage. Their reliability – especially when complex transactions are involved, as in the case of mixers – is discussed.[180] Particularly, while their use for investigative purposes – including to establish probable cause for invasive investigative measures[181] – seems to be widely recognized, their admissibility as evidence is all but clear.

In this sense, the use of analytics tools should be carefully evaluated by covered entities especially when making business decisions affecting individual rights. The novelty of the techniques and the connected limitations should warrant special caution. Particularly, a special attention should be paid to the use of such techniques when deciphering transaction patterns involving privacy-enhancing services, as mixers. A good practice would be to always use corroborating information and evidence besides blockchain analytics results when taking decisions that impact individual rights, as account freeze or discontinuation of the business relation. In this sense, the result of blockchain analytics shall be seen as an element of suspicion to, then, be integrated through further external indexes.

Before we conclude, a final point has to be drawn. The development and diffusion of blockchain analytics as a compliance method, leads us back to the argument made in the previous chapter: decentralized governance warrants for a customized policy framework. Eminently, not all virtual assets or crypto-assets under the FATF and MiCaR definition share the outlined data management structure.

The mentioned fundamental innovation, and connected risks, in the data structure only apply to public, permissionless blockchains. This means blockchains whose governance structure is decentralized so that no central point of governance exists. It is only in this type of networks that

*Decentralized Finance (DeFi) Policymaker Toolkit*, cit., 7; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 12.

[178] D. Carlisle, *Virtual currencies and financial crime: Challenges and opportunities,* cit., 38.

[179] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26; as mentioned by I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 4, Monero a privacy coin has proven to be "*currently resistant to tracking and tracing methods that applied to other cryptocurrencies*"; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 12

[180] European Banking Authority, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, cit., 96.

[181] US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 12

the ledger is public. Private, permissioned DLTs, while replicating a ledger among various nodes, do not change the way ledgers are stored and updated. Furthermore, such ledgers do permit control of entry and exit points (hence identification) and centralized establishment of rules (e.g., the exclusion of mixing services).

To draft rules that police the use of blockchain analytics, centralized and decentralized crypto-assets cannot be put in the same basket. The fundamental innovations, and risks, connected with blockchain analytics need to be assessed with fully decentralized networks in mind.[182] Eminently, given the intrusive and pervasive use in crypto-compliance a clear legal basis should be provided. The use of such tools goes beyond the information usually processed and analysed by covered entities and supervisors, hence, a clear legal basis should be provided. However, to do so the abovementioned distinction has to be reinstated at the legislative level.

An example can easily clarify the distinction. As said, blockchain analytics paves the way for direct supervision by states' authorities of financial transactions. However, this only applies to ledgers that, due to their decentralized governance, are public. A permissioned blockchain, or any other type of private DLT, is not necessarily public. The publicity of the ledger – as we have detailed in chapter two – is a technological necessity connected with the decentralized governance of the network. In a centrally governed network, there is no architectural need for a public ledger. In contrast, such ledgers are usually private as the centralized governance body has no interest in sharing valuable data with its competitors. This means that, in terms of archiving infrastructure, centrally governed DLTs do not generate new opportunities for ledger analytics. The same goes for blacklisting. In a centrally governed network, there is no need for blacklisting. As the update of the ledger is centralized, the centre of governance can simply unilaterally block or reverse a tainted transaction.

In conclusion, the establishment and regulation of customized methods for compliance, as is the case with blockchain analytics, requires a clear distinction between centralized and decentralized tokens. This distinction should be kept in mind when analysing the remainder of this section, as the following arguments only apply to public, permissionless networks.

[182] See for a similar distinction, although from a data protection perspective, M. Finck, *Blockchains and data protection in the European Union,* cit., 18.

## 6.1 Blockchain analysis tools: tracing, clustering, and pattern analysis

Before delving into the larger policy implications of blockchain analytics, it is appropriate to briefly sketch its functioning. Blockchain analytics is an umbrella term that comprises a series of techniques. Such techniques differ widely in terms of complexity and potential.

The most basic technique that can be employed is tracing. Tracing simply entails following a certain account's activity across the ledger. This technique can be pursued through public, free blockchain explorers[183] or services provided by specialized companies.[184] The effectiveness of this method is, however, limited. Eminently, a minimally careful user can simply employ multiple addresses to avoid traceability.[185] The creation of new addresses is free and easy and does not require any identification.[186] Potentially a different address could be used for each single transaction without any relevant increase in costs.

To solve this weakness more advanced analytics techniques have been devised. Particularly, clustering allows bundling of addresses and/or transactions connected to a single user.[187] This allows to neutralize, or at least reduce, the effectiveness of employing multiple accounts. Furthermore, cluster analysis can be used to mitigate the effectiveness of anonymity-enhancing techniques, such as the use of mixers.

[183] These types of software are free and available online, they allow to search for a public key, transaction, and block to obtain basic information. See, for example, the service offered by blockchain.com at https://www.blockchain.com/explorer or Blockstream at https://blockstream.info/.

[184] For a review of such tools both private and open source see A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 3.

[185] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26; M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., 3499; I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 12.

[186] For address creation see chapter 2 section 5.

[187] M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., 3500.

The techniques used to cluster transactions are rooted in various heuristics. Let's analyse a couple of them to better understand their functioning.[188]

First, multi-input heuristic.[189] Multi-input clustering aims at connecting a group of addresses to a single entity. This is done by searching for multi-input transactions (meaning transactions where multiple addresses are used for a single transaction). The addresses can then be clustered as associated with one entity.[190] The basic idea being that, if two addresses are used for a single transaction, then both are controlled by the same entity. The investigator can then scan the blockchain to find other multi-input transactions where at least one of the clustered addresses is involved and enlarge the connected cluster.

Second, shadow heuristic. This heuristic is based on the concept of Unspent Transaction Output (UTXO). In short, a UTXO can be described as the change of a crypto-transaction.[191] As with a cash payment where a high-value banknote is used, in specific cases crypto-transactions result in change. In such cases, the transaction has two outputs. One output is the receiving address, and the other address is held by the sender.[192] If the investigator can understand which one of the two outputs is the UTXO, then they can cluster such address with the sending address.

The third macro-category of blockchain analytics techniques is pattern analysis.[193] Pattern analysis enables a different form of control compared to the previous two. Tracing and clustering always start from a certain address or transaction. In this sense, these techniques always require information to trigger the analysis: either a customer's or suspect's account or a transaction identified as connected to criminal activity. Pattern analysis inverts this process. Such types of

[188] For other examples see M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., 3500.

[189] M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., 3500, refers to it as co-spend clustering.

[190] J. Hirshman – Y. Huang – S. Macke, *Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network,* cit., 1, "*two public keys may be assumed to belong to the same entity if they both appear as inputs to a particular transaction, since this means that whoever authorized the transaction had access to both corresponding private keys*"; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial,* cit., 62 "*common protocol for cluster analysis is linking together all the input addresses for one transaction. That is, if two or more addresses are inputs of the same transaction with one output, then one can infer that those input addresses are controlled by the same user*". N. Tovanich – R. Cazabet, *Pattern Analysis of Money Flows in the Bitcoin Blockchain,* cit., 4.

[191] A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 2.

[192] N. Tovanich – R. Cazabet, *Pattern Analysis of Money Flows in the Bitcoin Blockchain,* cit., 2.

[193] See, among the others, the work by J. Hirshman – Y. Huang – S. Macke, *Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network,* cit.; M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit.; C. Berggren – J. Asplund, *Identifying and analyzing digital payment flows regarding illegal purposes on the Internet: I samarbete med CGI OCH Finanskoalitionen*, 2016.

software scan the blockchain and identify patterns of transactions that, according to their heuristic, are suspicious. Pattern analysis enables, hence, a more proactive form of supervision or monitoring. The supervisor and/or covered entity does not need a trigger to launch its investigation but can harvest the information directly from the ledger.

This software use pattern analysis heuristics, including through the use of artificial intelligence,[194] to identify red flags. When a certain number of red flags connected with a transaction or a chain of transactions are identified, the software reports it to a human analyst for assessment. Examples of such red flags being, for instance, the use of mixers, interaction with accounts connected with known criminal activity, and use of CASPs located in high-risk jurisdictions.

Pattern analysis can also be employed reactively. Meaning, the activity of a specific user or suspect can be monitored through pattern analysis to spot suspicious or risky transactions. Similarly, when evaluating the risk of a transaction, a covered entity can analyse the connected pattern of transactions to evaluate its risk.

The last of the macro-techniques is at the frontier between blockchain analytics and classic computer forensics: address deanonymization. The deanonymization of blockchain addresses is a key step for the prosecution and apprehension of cybercriminals.[195] Deanonymization techniques use external data – as IP addresses, and information posted online[196] – to connect an individual with a certain account/s.[197] Deanonymization is also linked with clustering techniques. The use of clustering can be used to enhance the probability of deanonymization. Eminently, through clustering, investigators and compliance officers can identify a group of addresses connected with a single entity. This, in turn, multiplies the possible point of failure: the attacker only needs to deanonymize one of the addresses in the cluster to identify the individual/s controlling them.

[194] See "Blockchain Inspector" as detailed by A. Balaskas - V. Franqueira, *Analytical tools for blockchain: Review, taxonomy and open challenges*, cit., 3; see also the work by M. Harlev, et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, cit., that use machine learning to label cluster of transactions as pertaining to certain type of service providers (mixers, exchangers, etc.) or activity (ransomware, dark markets, etc.).

[195] C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 4.

[196] The manager of the dark market Silk Road, Ross Ulbricht (aka Dread Pirate Roberts), was identified through an email address he had used to open an account on a specialized blog where he advertised the market.

[197] I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 3; C. Pelker Alden – C. Brown – R. Tucker, *Using Blockchain Analysis from Investigation to Trial,* cit., 62.

The present section has presented the fundamental tools and heuristics underlying blockchain analysis. The following sections will briefly reflect on the impact such techniques have on the future compliance infrastructure.

## 6.2 Blockchain analytics. Open questions and future regulatory avenues

Section six has analysed the current use of blockchain analytics, the present section will delve into a possible area of future development. Particularly, if the use of blockchain analytics to ameliorate current compliance systems is widely recognized, what seems to still be underexplored is how the use of analytics tools could change the overarching anti-money laundering strategy.

The present strategy was devised with private, intermediated ledgers in mind, a new strategy may emerge when public, disintermediated ledgers are introduced. The imposition of significant compliance burdens on intermediaries has, so far, been justified based on their exclusive access to financial data. The elimination of such a monopoly warrants a re-evaluation regarding the rationality and proportionality of such a choice. Compliance duties constitute a relevant burden on companies, especially small and medium enterprises. Compliance constitutes a significant limit to competition in the field due to substantial start-up costs and consequent barrier of entry to the market.[198] The limitation imposed on the right to free economic initiative has been currently justified rooted in its inevitability: covered entities are the sole guardians of customers' financial data, hence, the only one that can monitor it. In a changing architecture, the validity of such a statement should be reconsidered. In this sense, also the proportionality of compliance costs should be re-evaluated. Supervisors could take a more active role in detecting suspicious activity and cooperating with covered entities.

Let's see how this could work. The current system is rooted in profiling individual customers – through Know Your Customer rules. The covered entity profiles the individual to then identify

[198] R. Auer *Embedded Supervision: How to build regulation in decentralized finance*, cit., 3, "*Compliance expenditure weighs heavily on financial institutions, and even more so on smaller firms. Supervisors thus face a trade-off between getting the data they need and keeping the costs of compliance within reasonable limits*".

suspicious transactions. The information structure of blockchain may warrant an inversion of such a paradigm.[199] One that starts with identification and profiling of transactions and identifies suspect individuals in a second phase – so-called Know Your Transaction. In this sense, the idea of Suspicious Activity Report may be inverted. The analysis of the aggregated data, performed directly by the supervisor, would reveal anomalies in transaction patterns and address operativity. It would be this anomaly to trigger an (inverted) SAR that would then warrant an investigation by the covered entity into the connected customer. The literature has underlined how the use of SARs based on profiling has frequently proven inefficient. Pushed by the hefty sanctions imposed in case of non-compliance covered entities use SARs as a risk-mitigation strategy. This, in turn, results in FIUs being flooded by SARs, sometimes poorly motivated.[200]

A transaction-based system would reverse the logic underlying SARs and address this issue. It would be the FIU to trigger the investigation of the covered entity, which would then only investigate a handful of cases and could devote larger resources to such an activity. The FIU would signal to the covered entity a specific operativity that seems suspicious and ask the covered entity specific questions to corroborate its suspicions. This system would reduce the problem connected with overreporting as suspicious activities would only, or mostly, be the ones identified by FIUs and non-compliance would be limited to incorrect answers or lack of effective investigation.

This second policy strand is not necessarily alternative to the intermediary-centred one. It may also become a supplementary tool to better identify suspicious activities. Furthermore, certain profiling activities may still be required to the covered entity so to be prepared when suspicious activities were to be signalled by the FIUs.

If such a paradigm shift is here advocated for crypto-assets, the strategy could expand beyond the limits of the crypto-market. Eminently, the proposed introduction of Central Bank Digital Currencies (CBDCs)[201] – not classified as crypto-assets – would introduce certain elements of

[199] See C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 3, "*Due to technological features of cryptocurrencies, governments not only have to face obstacles but can also make use of opportuni- ties when regulating them: on the one hand, regulation scenarios have to find a solution for the lack of central administrative parties. Standard Know-Your-Customer (KYC) systems will not work if users do not have to identify themselves when opening an account. Furthermore, the pseudonymity of cryptocurrencies hinders any concept that is depended on the knowledge of the users' identity, for example, as it is required by law enforcement agencies' supervision of an individual. On the other hand, the public transaction record enables new regulatory approaches*".

[200] See the discussion at section 2.1 of the present chapter.

[201] A CBDC is a form of fiat currency which is issued by the Central Bank in a digital form instead of its legacy physical form. For further reflections see IMF Staff, *Casting Light on Central Bank Digital Currency,*

blockchain's data structure in the larger market. CBDCs are largely rooted in a permissioned blockchain controlled by the Central Bank on top of which the intermediaries would operate.[202] A CBDC would, hence, give full access to financial data to the supervisor. This would, in turn, mean, if and when such currencies were to be introduced,[203] that the shift from KYC to KYT advocated for crypto-assets could be applied to the larger financial market. While this topic is outside of the purview of the present dissertation, which focuses on crypto-assets, it certainly provides food for thought.

To conclude, the development and potential of blockchain analysis underlines the dual nature of this technology. Certainly, blockchain poses new challenges to crime prevention. As detailed, the absence of intermediaries, its transnational nature, and decentralized governance are all factors that call into question the pre-existing strategy to financial flows control. At the same time, blockchain's data structure, particularly its publicity (in permissionless networks) and logical centralization, provide unprecedented opportunities, in terms of data quality and access, to supervisors and covered entities. Initially emerged as a passepartout for digital privacy, blockchain, especially in its permissioned form, could truly become a tool for greater control of financial flows and crime prevention.[204]

International Monetary Fund, Washington, 2018; Norges Bank, *Central Bank Digital Currencies,* 1, 2021, 5; D. Legal – G. Ortiz Ibarrola – C. Blanco, *Moneda Digital del Banco Central: Implicancias para la estabilidad financiera y la politica monetaria en Paraguay,* Documentos de Trabajo n. 27 Banco Central del Paraguay, 2022, 4, S. Allen, et al. *Design choices for central bank digital currency: Policy and technical considerations*, No. w27634. National Bureau of Economic Research, 2020.

[202] See, The White House, *Technical evaluation for a U.S. Central Bank digital currency system,* cit., 11, "*a permissionless approach does not make sense for a system that has at least one trusted entity (i.e., the central bank). It is possible that the technology underpinning a permissionless approach will improve significantly over time, which might make it more suitable to be used in a CBDC system. However, given the state of the technology, most of the analysis that follows assumes that there is a central authority and a permissioned CBDC system*"; Norges Bank, *Central Bank Digital Currencies,* cit., 30.

[203] The introduction of CBDCs is still, at least in Western Countries at a study phase. However, the European Central Bank has signalled its interest in the introduction of such a token. See the Digital Euro Package presented by the Commission the 28th June 2023, at https://finance.ec.europa.eu/publications/digital-euro-package_en, as well as the multiple statements by the European bodies, European Central Bank, *Eurosystem launches digital euro project*, 14th July 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html, European Central Bank, *Digital Euro Project Timeline*, 2021, https://www.ecb.europa.eu/paym/digital_euro/shared/pdf/Digital_euro_project_timeline.en.pdf, Eurogroup, *statement on the digital euro project*, 16th January 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/01/16/eurogroup-statement-on-the-digital-euro-project-16-january-2023/

[204] A. Gullo, *Compliance*, cit., 14. These characteristics of blockchain is in line with other emerging technologies arisen during the last decades. Famously, President Clinton dismissed the Chinese efforts of

## 6.3 A brief excursus. Blockchain analytics and privacy

Before we close our analysis on blockchain analytics, a final point has to be made. The use of blockchain analytics generates a specific problem in terms of data protection and privacy. While data protection is outside the purview of the present analysis, as its focus is solely the anti-money laundering legislation, a brief mention has to be made as a factor that may impact the concrete use of these tools.

It is the same Financial Action Task Force to underline the trade-off underlying the use of such tools:

> *"It is important to consider any potential implications for privacy and data protection in the use of such tools, if they allow transparency that is not otherwise available (e.g., on public blockchains)".*[205]

The use of blockchain data is classifiable as an open-source intelligence (OSINT) analysis. OSINT is the macro-area that covers all data analysis performed on publicly available data (as social networks, newspapers, academic articles, etc.).[206] The relationship between such techniques and data protection has been extensively analysed by the literature.[207] Particularly, to be underlined is the relation existing between the reasonable expectation of privacy standard, spelled out by the

imposing larger control on the internet as "Nailing Jello to a Wall", see B. Allen-Ebrahimian, *The man who nailed the jello to the wall*, in *Foreign Policy,* 29th June 2016, https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/. However, the internet, initially envisioned as a space that would enable greater freedom and elude state control, has indeed largely become a tool for individual and collective monitoring. On the new approach to digital crime policing see G. Morgante, *Criminal Law and Risk Management: From Tradition to Innovation*, cit.

[205] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 71.

[206] B. Koops – H. Jaap-Henk – R. Leenes, *Open-source intelligence and privacy by design*, in *Computer Law & Security Review,* 6, 2013, 677.

[207] J. Rajamäki – S. Sarlio-Siintola – N. Alapuranen – M. Nevanperä, *Privacy and data protection in open source intelligence and big data analytics: Case 'MARISA'* in *Ethics as a resource. Examples of RDI projects and educational development*, 2020; A. Shere, *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis*, in *The New Collection,* 3, 2020; B. Koops – H. Jaap-Henk – R. Leenes, *Open-source intelligence and privacy by design*, cit.; A. Lyle, *Legal considerations for using open source intelligence in the context of cybercrime and cyberterrorism*, in *Open Source Intelligence Investigation: From Strategy to Implementation,* 2016.

General Data Protection Regulation[208] and the Police Directive,[209] and the use of publicly available information. The justification of such practices has mainly revolved around the concept of consent and legitimate interest in which the GDPR is rooted. On the one hand, the willing publication of data in an open platform is considered a form of implicit consent to third-party surveillance.[210] On the other hand, the use of data for anti-money laundering purposes is explicitly classified as a legitimate interest by the GDPR and the anti-money laundering Directive.

On this second point, a brief digression is necessary regarding the application of the privacy regulation to the anti-money laundering field.

Recital 19 of the GDPR, while clarifying that anti-money laundering compliance duties fall within its purview and not the Police Directive, explicitly allows Member States:

> "*under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities*".

This statement of principle is translated by article 43 of the Anti-money Laundering Directive which categorizes the processing of personal data for anti-money laundering purposes as a matter of public interest.[211] This, in turn, constitutes one of the legitimate bases for data processing.

If this is the general framework for the collection and analysis of anti-money laundering data, blockchain analytics tools partially change the terms of the discussion. Eminently, the data collected and processed through blockchain analysis is not data controlled by the covered entity, but rather is public, freely available data. In this sense, the analysis of blockchain data can be classified as an OSINT as the data subjects willingly publish their data in the blockchain ledger

[208] Regulation of the European Union, 27th of April 2016, n. 679.

[209] Directive of the European Union, 27th of April 2016 n. 680.

[210] A. Shere, *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis,* cit., 11.

[211] See article 43 "*The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Regulation (EU) 2016/679 of the European Parliament and of the Council*".

when executing a transaction.[212] The ledger is public and the connected information transparent. In this sense, the analysis of the data seems to be legitimate as both the consent and the legitimate interest recur.[213]

At the same time, a fundamental trade-off underlies the relation between privacy and anti-money laundering regulation when it comes to blockchain analytics.[214] If the GDPR requires and encourages the creation of privacy-enhancing technologies,[215] the anti-money laundering is precisely aimed at curbing such technologies, especially so with public, permissionless blockchain. Blockchain data is, many times, the only thing supervisors and covered entities have. This is particularly true when it comes to self-hosted addresses or decentralized autonomous organizations due to their pseudonymous nature and exclusion from the purview of compliance duties.

As detailed in sections four and seven of the present chapter, this has led the anti-money laundering regulation to be increasingly wary of privacy-enhancing technologies. The European Banking Authority includes the use of privacy-enhancing technologies – as mixers, privacy wallets, and privacy coins – among the risk factors to be considered by a covered entity for the application of Enhanced Due Diligence. At the same time, privacy-enhancing technologies are increasingly labelled as crime facilitators. An extreme case being the sanctioning by OFAC, and contemporary arrest of the developer, of the mixer Tornado Cash analysed in the following chapter.

If this is the position of the anti-money laundering regulation, the GDPR seems to hold an opposite view. Particularly, the progressive identification of core developers as data processors and/or controllers may impose a duty (or at least a justification) to provide the anonymization which is contrasted by anti-money laundering.[216] In a similar fashion, the right to be forgotten

[212] For a definition of OSINT see A. Shere, *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis,* cit., 8.

[213] C. Rueckert, *Cryptocurrencies and fundamental rights*, cit., 6, distinguishes among tools that simply analyse the data and those that also store it (with the second being identified as more problematic in terms of privacy protection).

[214] For an analysis concerning the relation existing between GDPR and blockchain see M. Finck, *Blockchains and Data Protection in the European Union*, cit.

[215] See the discussion by M. Finck, *Blockchains and data protection in the European Union,* cit., 25, which identifies privacy coins as a possible solution to the privacy problem.

[216] For a discussion concerning the possible identification of data controllers and processors in permissionless blockchain see I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 5 – 8 which also argues for the inclusion of core developers.

clashes with the usefulness of unmodifiable data for blockchain analysis.[217] There seems to be, hence, a clash at the principles level when it comes to development of blockchain ledgers and applications.[218] The GDPR promotes the anonymization of data.[219] The anti-money laundering considers risky, or even criminal, the development of such tools.

As stated by Karasek-Wojciechowicz:

> *"GDPR requirements for personal data protection push permissionless blockchain-based networks towards ensuring the anonymization of data processed on a public ledger. Ensuring data anonymization is currently needed if public ledgers are to enable GDPR-compliant data processing on ledgers by data controllers and data processors. However, at the same time, the privacy-blockchains which use anonymity-enhanced technologies, as well as their native privacy-coins, are combated by AML/CFT policies"*[220]

A further development of this theme is out of the purview of the present dissertation. However, the normative dissonance is certainly one that will recur in the future debate concerning blockchain transparency and analysis. A conflict that sees two opposed concepts of compliance-by-design, the privacy and anti-money laundering one.

The anti-money laundering regulation seems to have so far prevailed. Faced with growing crime rates connected with the pseudonymous and disintermediated nature of blockchain, the policymaker has responded by tightening crime control measures; curbing the opacity of the blockchain ledger has been one of the main purposes of such an action. Privacy-enhancing services – as mixers, or privacy coins – have been labelled as crime facilitators and discouraged. However, as the market normalizes, new and contraposing instances will emerge. The privacy risk posed by blockchain's data structure will have to be assessed and money laundering measures will need to be balanced with such opposing interests.

[217] M. Finck, *Blockchains and data protection in the European Union,* cit., 25.

[218] See I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 10.

[219] This is the conclusion reached by I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 9, which states "*Therefore, in my opinion, the GDPR leaves only one option available for permissionless networks to create a protocol enabling GDPR-compliant processing of data written on the ledger: implementing the technology which will ensure the anonymization of data stored on the ledger. The GDPR does not apply to anonymized data*".

[220] See I. Karasek-Wojciechowicz, *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces,* cit., 10.

In this sense, the legislature should provide for a clear legal basis for blockchain analysis. One that strikes a balance between the need to guarantee transparency for financial monitoring and opacity for individual privacy. The innovative nature of this analytics technique demands for a legal basis to frame blockchain's data structure and its use by covered entities and supervisors.

# Chapter Five

## Reigning Decentralized Arrangements

### DAOs, between covered and excluded entities

### 1. Introduction

We close our analysis regarding the European anti-money laundering regulation of crypto-assets with one of the thorniest problems in the field: the treatment of decentralized arrangements. As detailed throughout this thesis, one of the main innovations purported by blockchain is the possibility of creating arrangements that function autonomously.[1] By autonomously it is meant that the actions of such arrangements – also known as Decentralized Autonomous Organizations or DAOs – are not controlled by any governance body as their behaviour is solely dictated by their underlying code.[2] Once the DAO is launched, no one (except if such a possibility is provided by the code itself) can stop or influence its behaviour.[3]

[1] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 86.

[2] See the definition by FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, cit., 3, "*Decentralized (distributed) application (DApp) is a term that refers to software programs that operate on a P2P network of computers running a blockchain platform (a type of distributed public ledger that allows the development of secondary blockchains), designed such that they are not controlled by a single person or group of persons (that is, they do not have an identifiable administrator)*"; see also the definition provided by H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 2; S. Hassan – P. De Filippi, *Decentralized autonomous organization*, in *Internet Policy Review,* 2, 2021, 1.

[3] M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 3, "*By default, the contract logic cannot be changed after deployment. Any asset that is sent to the smart contract will remain in control of this smart contract until a condition in its code is met that will transfer the assets to a new address*"; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 86, "*The design of DeFi infrastructure is for direct*

From an anti-money laundering perspective, the establishment of such an arrangement creates a fundamental problem: compliance duties are thought for human-operated, vertical[4] organizations.[5] A machine-operated, headless organization is, hence, largely unfit to comply with the anti-money laundering regulations as they are currently structured. Questions such as: who should design and apply the compliance duties? Who is liable if such controls are not correctly applied?[6] Are difficult (if not impossible) to answer in the absence of a management body, or even just humans, that govern, control, and run the organization.

This is a problem the anti-money laundering regulator has increasingly grappled with. Eminently, the development of DAOs – especially in the field of finance, with the emergence of Decentralized Finance or DeFi – has steadily increased over time.[7] Virtually any covered activity under the FATF Guidance or MiCaR can be pursued through a decentralized organization.[8] If DAOs were to not

*participation on a peer-to-peer or peer to platform systems, and all features and functionality are coded and once executed are immutable on the underlying blockchain in a tamper-resistant and transparent form*".

[4] For "vertical" we mean a governance model that is based on a certain level of hierarchy in the decision-making process, and that is governed through apical bodies that have a power of organization with respect to the entity – what we would call management.

[5] H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization,* cit., 9, "*The core problem (…) is that the technological development around blockchain and DAOs offers a transformational shift that challenges the existing regulatory paradigm in which an identifiable legal entity is presupposed*"; H. Axelsen - J. Rude Jensen – R. Omri, *When is a DAO Decentralized?*, cit., 52.

[6] This problem is clearly underlined the World Economic Forum in its report, World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 10, which states "*identifying the "whom": Accountability of stakeholders in the crypto-assets ecosystem is a core concern for policy-makers. Not to be confused with anonymity, accountability refers to the ability of enforcers to hold actors accountable in accordance with their relevant legal obligations. Accountability may become even more difficult where, for example, wallets are either controlled by multiple actors, by automated bots or software or by decentralized autonomous organizations without clear governance structures in place. In each of these instances there arises a risk not of anonymity but of dispersed accountability, making it difficult to causally attach the actions of the wallet or decentralized autonomous organization (DAO)",* on a similar note the US Department of Treasury*, Illicit Finance Risk Assessment of Decentralized Finance*, cit., 28, "*In some cases, the lack of a clear organizational structure may make it difficult to identify any person, group of persons, or entity operating a DeFi service, whether because no such person exists or because of distributed, poor, or purposefully confusing organization. This poses critical challenges for conducting supervision and, when appropriate, enforcement against DeFi services that are not fulfilling their AML/CFT obligations.113 This challenge can be compounded by the fast pace of change in the virtual asset industry, the large and growing number of DeFi services, and limited resources at some regulatory agencies*".

[7] Financial Action Task Force, *Targeted update on implementation of the FATF standards on Virtual Assets and Virtual Asset Service Providers,* cit., 19; for an analysis see OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, cit.

[8] A good example being Decentralized Exchangers or DEX, as explained by US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 11, "*In the case of a DEX, liquidity pools are funded by participants who may be incentivized by a portion of fees collected by the DEX. Liquidity providers may receive a separate virtual asset from the service in exchange for locking in their assets, often referred to as a "liquidity provider token" (LP token) that entitles them to their portion of the pool, including any accrued fees.46 Other users, accessing the liquidity pool through the DEX, can then exchange a certain quantity of one virtual asset for a certain quantity of another virtual asset. For these types of DEXs, the exchange rate between tokens is typically set by an algorithm.47 Users often pay a fee to use the service, which is shared with LP token holders. Similarly, with liquid staking, users stake virtual assets with a DeFi service and*

be covered under the sectorial regulation this would generate a relevant loophole.[9] Anyone who wished to avoid controls could simply turn to a decentralized arrangement and receive the equivalent service.[10] At the same time, as controls are currently structured, it seems extremely difficult to have them applied to an organization such as a DAO.[11]

The present chapter is structured as follows. Section two and three will analyse two regulatory avenues that have been explored by the legislator to address this problem: the identification of responsible entities within DAOs through an expanded notion of control and the increasing inclusion of software developers among the covered entities. The fourth section will delve into the proposal by the European Parliament to regulate DAOs. The fifth section will explore a recent case, the Tornado Cash case, that underlines how supervisors are responding to the anti-money laundering challenges posed by DAOs. The sixth section will reflect on possible future solutions to the regulation of decentralized arrangements.

## 2. A quest for control. Identifying governance in decentralized autonomous organizations

The first avenue the legislator has traced to address the problem of DAOs' regulation has been the identification within such organizations of an individual or an entity that, *in concreto,* can be charged with CASP functions.[12] To achieve this goal, supervisors are urged to always evaluate the

*receive a separate virtual asset in return, which represents the staked virtual assets and any accrued fees from the staking service validating transactions on the blockchain. Since LP tokens and virtual assets representing staked assets can be exchanged between different persons, it is possible for a different person than the user who original staked the asset to redeem the LP or other tokens for the assets that were initially locked in the liquidity pool*".

[9] Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets/VASPs*, Paris, 2021, 33, "*A second major challenge to the FATF definition of VASP is its application to so- called 'decentralised' structures (…) how the FATF Standards apply to such structures is a challenge, as it may be difficult in some cases to identify the parties involved with clear responsibility for AML/CFT obligations*".

[10] As underlined by US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 4, "*industry providers may purposefully seek to decentralize a virtual asset service in an attempt to avoid triggering AML/CFT obligations".*

[11] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 26.

[12] Financial Action Task Force, *Targeted update on implementation of the FATF standards on Virtual Assets and Virtual Asset Service Providers,* cit., 20.

single arrangement in its concrete functioning and not based on the labels it comes with.[13] Supervisors are invited to analyse the specific DAO to evaluate whether there is an underlying individual or entity that can be deemed to have control of the latter.[14]

Eminently, as with all blockchain-based application, there is frequently a gap between label and concrete implementation. Blockchain and smart contracts theoretically permit the creation of fully autonomous organizations. However, in practice, most of these organizations labelled as autonomous are only partially decentralized. The developers tend to retain a certain level of control over the arrangement, especially in the initial phase. Full decentralization is frequently an aspiration rather than a concrete reality of DAOs.[15] It is relevant to remember that the fact an organization is rooted in blockchain and functions through smart contracts does not mean it is autonomous. Rather, it means its fundamental rules are executed automatically. If the smart contract gives to an individual or a group thereof special management rights, the organization is, at best, only partially autonomous. In this sense, the conundrum connected with autonomous organizations shall be restricted to that part of the market which is truly decentralized and not to any self-declared DAO.

This search for control is facilitated by an increasingly wide notion of governance by the sectorial anti-money laundering policies. The 2021 FATF Guidance talks, for the establishment of CASP duties, about "*control or sufficient influence*".[16] To better circumscribe these vague notions, the FATF has developed a number of indexes to spot the human behind the DAO. These are:

[13] See Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 27, "*Countries should apply the principles contained in the Standards in a manner that interprets the definitions broadly, but with regard for the practical intent of the functional approach. It seems quite common for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence, and jurisdictions should apply the VASP definition without respect to self-description*". In this sense also, US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 3.

[14] European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 95, "*in case a person or a managing body can be identified, despite its qualification, the DeFi application shall be treated as a crypto-assets services provider and fall under the same AML/CFT obligations. Therefore, much like with NFTs, DEFIs may be subjected to the application of the relevant rules covering crypto- assets on a case-by-case basis but keep posing regulatory challenges that are not yet fully addressed and could conduct to take additional measures to better tackle them in the future*". European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, SWD(2022), 27th October 2022*, 95

[15] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 138.

[16] See Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 27.

> *"who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations, who generated and drove the creation and launch of a product or service, who maintains an ongoing business relationship with a contracting party or another person who possesses and controls the data on its operations, and who could shut down the product or service".* [17]

However, it is the same FATF to clarify that this list is merely illustrative as "*individual situations will vary and this list is not definitive and offers only some examples".*[18]

This first policy avenue could be defined as more conservative. The idea is to expand the notion of control to somewhat fit the functioning of a DAO within that of classic centralized firm. This is not to mean that this approach is unjustified. As mentioned, many DAOs are indeed only partially decentralized.[19] Meaning that, while part of the DAO's activity is automatized, there is still a centre of control that retains the means to shut the arrangements, modify its code, influence the decision-making process etc.[20] Furthermore, most DAOs – despite being registered as NGOs or Foundations – are created by individual/s that intend to profit from the latter. It can be argued

[17] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 36.

[18] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 36; on the vagueness of the concept of decentralization and for a proposal to define and discern decentralized v. centralized arrangements, see H. Axelsen - J. Rude Jensen – R. Omri, *When is a DAO Decentralized?,* cit., 55; see on the multidimensional nature of this definition Hassan – P. De Filippi, *Decentralized autonomous organization*, cit., 6 – 7.

[19] OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, cit., 20; H. Axelsen - J. Rude Jensen – R. Omri, *When is a DAO Decentralized?,* cit., 55; O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 7; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 12; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 136, "*in practice, most so-called DAOs are in fact DOs, because although both have internal capital (i.e. a treasury, however structured), few so-called DAOs are capable of making autonomous decisions and instead rely on human interaction and decision-making, with some degree of automation and blockchain technology involved in the governance process and implementing the outcome of decisions*".

[20] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023*, cit., 4, "*while FATF standards do not apply to soft- ware such as DeFi protocols themselves, they can apply to persons who maintain control or sufficient influence over a DeFi arrangement or protocol providing VASP services (…) Similarly, although DeFi currently falls outside the EU's Market in Crypto- Assets (MiCA) legislation, individual entities could potentially be answer- able to the Fifth Anti-Money Laundering Directive (5AMLD) if a supervisor identified a "person with significant control" that should be registered as a cryptoasset service provider due to the services the DAO is carrying out";* on a similar note US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 11; The law society, *Blockchain: Legal and regulatory guidance. Third Edition*, cit., 139, "*As a rule of thumb, if a party can intervene in the operations of a DAO or its protocol in the case of an emergency, that party may be construed as having a control relationship. DAOs and their legal advisors should carefully consider such arrangements, their purpose and intended duration. Eventually, that link may need to be severed to defend against a control challenge with legal and regulatory obligations potentially also arising if such a determination is upheld*".

that with profit comes certain responsibility – like ensuring such a profit is not the result of processing ill-sourced money.

At the same time, this case-by-case approach is problematic in terms of legal certainty and may lead to a chaotic regulation-through-enforcement scenario.[21]

Eminently, neither the FATF nor the MiCaR provide for a customized regulation of DAOs nor of partially decentralized DAOs. The same exclusion of decentralized arrangements by MiCaR, is only spelled out by recital 21 which states:

> "*This Regulation should apply to natural and legal persons and certain other undertakings and to the crypto-asset services and activities performed, provided or controlled, directly or indirectly, by them, including when part of such activities or services is performed in a decentralised manner. Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation. This Regulation covers the rights and obligations of issuers of crypto-assets, offerors, persons seeking admission to trading of crypto-assets and crypto-asset service providers. Where crypto-assets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation. Crypto-asset service providers providing services in respect of such crypto-assets should, however, be covered by this Regulation*".

The absence of any reference to decentralized arrangements in the binding part of the Regulation leaves their policing in a legal vacuum. Particularly, the main question is where the line should be drawn between partially and fully decentralized arrangements. In the absence of a clear definition of decentralization, this question is hard to answer. Furthermore, in the absence of any duty of registration on DAOs, there is no moment when the supervisor can evaluate *ex-ante* whether the arrangement is only partially decentralized and, hence, signal to the regulated entity its duty to comply with relevant regulations. The risk is to transform enforcement in a case-by-case exercise, pursued *ex-post* on entities that may ignore their duty to comply.[22] In such a scenario, the imposition of sanctions, especially when criminal in nature, may result complex due to a *de facto* impossibility to comprehend when compliance duties apply and by whom they should be applied.

[21] For an example of how such a scenario may look like see the Tornado Cash case described in the last section of the present chapter.

[22] Which seems exactly what suggested by European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, cit., 95.

This lack of clarity is even more troubling if we analyse how control is wielded in DAOs. While some DAOs do have a certain form of governance, such governance is usually exercised in non-traditional manners. A good example being the use of governance and voting tokens.

In a DAO most decisions are taken through voting.[23] The idea is to eliminate centralized decision-makers and leave, instead, each decision to the shareholders/investors, this way eliminating internal intermediaries – as directors or managers. In a sense, the difference between DAOs and traditional corporations can be equated to the distinction between representative and direct democracies. A traditional corporation is an exercise of representative democracy. Shareholders nominate their representatives – the director/s and/or the president – who then make the decisions for them. The representatives are then (theoretically) held accountable for their actions and, if not satisfactory, replaced. In contrast, a DAO is an exercise of direct, Athenian, democracy. Every decision is taken by the totality of the shareholders through direct voting. To exercise this voting right, the shareholder is provided with a voting or governance token. One of the main avenues for developers to retain control is, thus, to hold a majority of the governance tokens so to always have a decisive influence on the decision-making process. However, holding such a majority is a *de facto* notation, one that derives from the participation in the capital of the arrangement or from contractual agreements. How stable and how relevant should this voting majority be to qualify as control remains an open question. Furthermore, currently, shareholders are under no duty to design or apply an anti-money laundering compliance system. Hence, if such a prevalence in the concrete governance was to be recognized as control it would surreptitiously introduce a duty on shareholders to design and apply an anti-money laundering compliance framework, at least in DAOs.

This seems to be the avenue taken by the United States' Department of Treasury.[24] Which states:

> *"Moreover, distribution and concentration of governance tokens and voting demonstrate control over decentralized applications. In some services, governance tokens or voting rights may be concentrated and held by a limited number of actors. Developers and early investors in a DeFi service may keep control of the service by allocating significant shares of governance tokens to themselves or otherwise maintaining de facto control. Concentration of*

[23] Bank of England, *Financial Stability in Focus: Cryptoassets and decentralised finance*, cit., 29.

[24] A similar parallel between voting rights and control is made by The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 138, "*if the concentration of voting power is too high then this questions whether, in fact, the DAO can be considered decentralised due to power to making decisions on sitting with so few*".

> *influence within a DeFi service can also result from a low level of participation by governance token holders in voting, providing outsized voting power to the minority of token holders that do participate. Separately, some services allow for the delegation of voting rights associated with governance tokens to other persons, called delegates, while the token holder retains the economic benefits of the token. In some cases, delegates accumulate significant voting rights associated with a large number of governance tokens, and this model can result in a relatively small number of delegates holding a large portion of voting power for a DeFi service. Within this framework, the use of governance tokens does not necessarily equate to decentralization in decision making for the services, and the ownership of voting rights for many governance tokens can be highly concentrated. As a result, in many cases a small number of persons may be able to exercise a high degree of control even if the governance structure purports to be decentralized".*[25]

Such an extension is not unreasonable per se. However, it warrants a clear legal basis. Eminently, currently, the Union's anti-money laundering framework ascribes the duty to comply to the "senior management".

Article 5, paragraph 8, of the Directive states:

> *"Member States shall require obliged entities to obtain approval from their senior management for the policies, controls and procedures that they put in place and to monitor and enhance the measures taken, where appropriate".*

Similarly, the upcoming Anti-money Laundering Regulation requires, at article 9, paragraph 1, obliged entities to:

> *"appoint one executive member of their board of directors or, if there is no board, of its equivalent governing body who shall be responsible for the implementation of measures to ensure compliance with this Regulation ('compliance manager'). Where the entity has no governing body, the function should be performed by a member of its senior management".*

Senior management is, in turn, defined by article 3, paragraph 12, of the Directive as:

[25] US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 12.

> *"an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors".*[26]

The current framework makes, hence, no mention of shareholders as involved in the compliance process. The definition of senior management is shaped around the concept of traditional firms and seems hardly adaptable to fluid structures such as DAOs. In this sense, *de iure condito* the identification of governance centres with anti-money laundering duties will be left to case-by-case decisions taken by the supervisors.

This uncertainty is underlined by the World Economic Forum in its analysis of crypto-assets regulation:

> *"case law in the United States has suggested that jurisdictions may treat unincorporated DAOs as general partnerships, with liability attributed to individuals holding tokens in the DAO as general partners. Where the governance structures of such organizations are not clear, it may mean that policy-makers and regulatory authorities may find it difficult to single out individual actors to hold accountable".*[27]

This case-by-case approach seems hardly like a good option and certainly not in line with MiCaR's resolve to provide for a clear legal basis to market participants. Rather, a clear definition of what decentralized means should be provided as well as parameters to ascertain when such decentralization is insufficient to warrant an exclusion of the compliance duties. Furthermore, criteria should be offered to identify, in cases of only partial disintermediation, the bodies responsible for the establishment, maintenance, and implementation of compliance programs.

In favour of a similar clear identification is the report requested by the European Parliament on the remaining challenges left by MiCaR which states:

> *"fully decentralized platforms have evaded regulation so far, arguing they lack an entity that could provide the disclosure. As we have pointed out frequently, we do not believe this argument holds merit; most often, an entity or a group of persons drives the code development and marketing of its tokens. It is for these reasons that we suggest*

[26] A nearly identical definition is provided by the upcoming Anti-money Laundering Regulation which at article 2, para. 28 defines senior management as "*in addition to executive members of the board of directors or, if there is no board, of its equivalent governing body, an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure*".

[27] World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach*, cit., 10

*granting entity status for regulatory purposes to DAOs, for micro-prudential and also sustainable finance regulation. These regulated entities should then be added to the scope of the SFDR and the Taxonomy Regulation, subject to reasonable size thresholds. However, the legal entity engaged in product development and distribution of services of the fully decentralized platform may register itself as an operator for the purposes of EU financial regulation and comply with sustainability disclosure obligations on behalf of the platform".*[28]

In this sense, the legislator should clearly define what a Decentralized Autonomous Organization is (as the European Parliament had proposed in one of MiCaR's earlier versions).[29] It should also spell out the characteristics that distinguish a fully and a partially decentralized DAO as well as the who, how, and where of connected compliance duties. In this sense, a good option may be to extend the general duty of registration to DAOs. Through the registration process, the supervisor could evaluate the DAOs governance structure and apply, *ex ante*, the necessary compliance measures.

## 3. Compliance-by-design and software developers. Pushing back the compliance threshold

The second regulatory avenue taken by the legislator to reign on DAOs starts from a factual notation: in a DAO, a participant can only do what the code affords them. The DAO, if decentralized, cannot be bent into doing anything that is not provided by its code.[30] In this sense, it would be disproportionate to ask for compliance with anti-money laundering duties to parties that miss the concrete code-given capacity to implement them. Hence, to apply compliance duties the corresponding powers should already be provided by the code underlying the DAO.

Let's give two examples to clarify.

[28] D.A. Zetzsche - R.P. Buckley - D.W. Arner - M.C. van Ek, *Remaining regulatory challenges in digital finance and crypto- assets after MiCA,* cit., 73.

[29] See section four of the present chapter.

[30] H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 2.

The first one concerns token holders. One of the key requirements under the anti-money laundering framework is to identify customers. Let's say that token holders are recognized as entities with sufficient control and, thus, responsible for the implementation of a compliance framework. The imposition of mandatory identification is only possible for token holders if the smart contract underlying the DAO allows them to take and implement such a decision. If the DAO's smart contract does not allow this action, the token holders would be concretely unable to implement a Know Your Customer program. As it is clear, such an impossibility would frustrate the aim of the legislator to extend to the latter compliance duties and corresponding criminal and administrative liabilities, *ad impossibilia nemo tenur.*

The second example concerns the key players of this section: software developers. One of the indexes identified by the FATF to ascertain control is profit.[31] If an entity profits from the functioning of a DAO, then it should also be responsible for the connected compliance duties. The main problem with this approach is that if the developer lacks the code-given power to change the smart contract they are concretely unable to adapt it to the regulatory requirements. While the idea that profit corresponds to responsibility seems theoretically fair, it may be concretely impossible to implement. If the developer is to be responsible for implementing compliance, then this duty should be imposed when they are designing the smart contract not once is up and running.

This notation brings us to the second, more innovative, strategy taken by the policymaker to extend compliance to DAOs: the expansion of the purview of the anti-money laundering duties to the software developer by, at least partially, including the latter among the CASPs.[32] The main idea behind such expansion is that if a developer computes a software that will pursue a covered activity autonomously, then they should ensure the same software will, or at least can, comply with the relevant regulations. This concept of engrained compliance is increasingly common in the regulation of autonomous software under the brand of compliance-by-design.[33] For instance, a

[31] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 36.

[32] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 138, "*The obvious point here is that a DAO does not spontaneously come into existence. The above components evidence a concerted effort by a group of people acting together to create the infrastructure through which a DAO can be created and operated. The number of participants in that group, and their geographic spread may vary, but they are very clearly not decentralised, by necessity*".

[33] For a compliance-by-design proposal in the field of DeFi see B. Mesquita – S. Maranhao – J. Seigneur, *Enabling KYC and AML verification in DeFi service,* cit.; H. Axelsen – J. Jensen – R. Omri, *When is a DAO Decentralized?*, cit., 70. On the shift from an activity-based to a risk-based concept of criminal liabilities in

similar perspective underlies the European Proposal for an AI Act.[34] There, pre-launch engrained compliance is mandated for autonomous software depending on their risk rating.[35]

A similar, by-design, approach was proposed by the European Banking Authority in its first opinion on virtual currencies in 2014.[36] In that opinion the EBA recommended that any virtual currencies have a "Scheme Governance Authority". The Authority was envisioned as a non-governmental, legal person accountable to the regulator for the implementation of legal requirements. The institution of such an entity would have been *"a mandatory requirement for a VC scheme to be regulated as a financial service and for it to be allowed to interact with existing regulated financial services"*.[37] The idea was, hence, to impose to developers a certain level of centralization, through the mandatory creation of a "command centre" that could guarantee compliance with legislative requirements.

However, the implementation of this approach in the anti-money laundering field is particularly contentious. This type of compliance clashes with one of the principles we have identified as fundamental in the sectorial regulation: technological neutrality.

As clearly stated by the FATF:

> *"the FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that may use technology or software applications to facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person. A person that develops or sells either a software application of a new VA platform (i.e., a software developer) may therefore not constitute a VASP when solely developing or selling the application or platform, but they may be a VASP if they also use the new application or platform to engage as a*

modern digital societies see G. Morgante, *Criminal Law and Risk Management: From Tradition to Innovation*, in *Global Jurist*, 16/3, 2016, 321.

[34] The AI Act is envisioned by the Commission as the first European comprehensive regulation of artificial intelligence to play a similar role as the MiCa Regulation in the crypto-assets space. For more on the proposal see, Proposal for a Regulation of the European Union, 21st of April 2021, n. 0106; T. Madiega, *Artificial intelligence act*, European Parliament: European Parliamentary Research Service, 2021.

[35] For the connection between risk and regulation in the AI Act see J. Schuett, *Risk management in the artificial intelligence act,* in *European Journal of Risk Regulation,* 2023.

[36] European Banking Authority, *Opinion on "Virtual Currencies",* cit.

[37] European Banking Authority, *Opinion on "Virtual Currencies",* cit., 39 – 40.

> *business in exchanging or transferring funds or conducting any of the other financial activity described above on behalf of another natural or legal person".*[38]

The same approach is taken by MiCaR at recital 22, mentioned in the previous section of the chapter.[39]

*Prima facie* then, the line between covered and excluded activity can be traced in the distinction between designing and operating a software.[40] The first activity being outside of the regulatory corral. At the same time, behind such statements of principle there seems to be an increasing interest, especially at the FATF level, to move beyond the exclusion.[41] This is done, so far, with nuanced affirmations that seem to contradict the clear, above-quoted, exclusion. For example, it is the same Guidance of 2021 that affirms:

> *"A person that creates or sells a software application or a VA platform (i.e., a software developer) may therefore not constitute a VASP, when solely creating or selling the application or platform (…) a party directing the creation and development of the software or platform, so that they can provide VASP services as a business for or on behalf of another person, likely also qualifies as a VASP, in particular if they retain control or sufficient influence over the assets, software, protocol, or platform or any ongoing business relationship with users of the software even if this is exercised through a smart contract. Such a VASP is therefore responsible for complying with the relevant AML/CFT obligations. As such, they should undertake ML/TF risk assessments prior to*

[38] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 17, this same approach is confirmed the following year in the Financial Action Task Force, *Targeted update on implementation of the FATF standards on Virtual Assets and Virtual Asset Service Providers,* cit., 19. See also the opinion of FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, cit., 5, "*The development of a DApp financed through ICO fundraising activity consists of the production of goods or services, and therefore is outside the definition of money transmission. Thus, the developer of a DApp is not a money transmitter for the mere act of creating the application, even if the purpose of the DApp is to issue a CVC or otherwise facilitate financial activities denominated in CVC However, if the developer of the DApp uses or deploys it to engage in money transmission, then the developer will qualify as a money transmitter under the BSA*".

[39] See section two of the present chapter.

[40] B. Mesquita – S. Maranhao – J. Seigneur, *Enabling KYC and AML verification in DeFi service,* cit., 3; US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 2; 32, "*Globally, under the standards set by the Financial Action Task Force (FATF), the global standard setting body for AML/CFT, DeFi services that lack an entity with sufficient control or influence over the service may not be explicitly subject to AML/CFT obligations*".

[41] See also Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 23.

> *the launch or use of the software or platform and take appropriate measures to mitigate the risks in an ongoing and forward-looking manner".*[42]

Here, the FATF first excludes software developers but then seems to reintroduce them, precisely by imposing the above-mentioned by-design compliance duties – i.e., software developers should mitigate the risks in the design phase in a forward-looking manner.

A similar approach emerges from the advises the Guidance directs to States. These are not directly binding; they are rather suggestions aimed at helping Countries to better manage high-risk areas. In particular, the FATF, analysing the risks posed by DeFi and possible avenues to mitigate them, asserts:

> *"Potential mitigation measures could include, for example (…) controlling whether/how AML/CFT preventive measures are built into the arrangement and/or by ensuring that AML/CFT obligations of obliged entities within the arrangement are fulfilled, e.g. by using software to monitor transactions and detect suspicious activity. Supervisors should look for these mitigation measures to be in place before granting registration/licensing and on an ongoing basis. It will be more difficult to mitigate risks of these products once they are launched".*[43]

A similar code-centric approach is proposed by the French *Autorité de contrôle Prudential et de Resolution* in its opinion on MiCaR. Particularly, the Authority proposes to:

> *"to explore other types of solutions as well, drawing in particular on non-financial regulations, such as those governing product safety in the European Union (EU). In these particular regulations, a number of requirements are placed directly on products, thus building a chain of obligations for all players involved in their manufacture and distribution, which may notably lead to substitution mechanisms when one of these players is located outside the European Union. Thus, this paper proposes a certification system for smart contracts, which would apply to the product itself, without the need to define a person that would be directly responsible for compliance with this obligation. If no one wants to have a product certified, that product will simply not be distributed. This makes it*

[42] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 32.

[43] Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* cit., 39.

> *possible to define a set of products deemed "safe", which will be the only ones that can be offered by the intermediaries ensuring access to DeFi services for the greatest number of people".*[44]

A similar position is taken by the Bank of Italy in its evaluation concerning DeFi regulation. As it states:

> *"Taking into consideration the difficulty in some cases - think, for example, of the case of DeFi in its "pure" sense - of identifying specific subjects to which certain requirements are to be applied, the possibility of intervening in the processes of defining and developing the technological standards used is susceptible to further study, with a view to strengthening the necessary risk mitigation safeguards".*[45]

While not clear-cut statements, these may point in the direction of an increasing direct involvement of anti-money laundering supervisors when it comes to the technological architecture underlying crypto-assets.[46] This would be an interesting development as it would signal a partial departure from the traditional intermediary-based approach towards an increasingly code-based one. However, it is still too early to evaluate the extent to which compliance-by-design will penetrate as an enforcement strategy in the decentralized market. We will further discuss the hurdles connected with enforcing by-design compliance on autonomous software in section four of the present chapter. Let's, however, first focus on how such an engrained compliance model may work in a decentralized autonomous organization.

The main trade-off when introducing, by-design, compliance in DAOs is, as in most of our analysis, between decentralization and centralization. The reason why DAOs are perceived as a valuable tool is precisely their decentralization. The business case advanced by decentralized organizations is to get rid of intermediaries and solely trust the code. DAOs, it is argued, would

[44] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 73; advocating for a similar product-centric solution the Bank of Italy, see Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 10, "*specie nelle aree più distanti dal perimetro regolamentare, dove più avvertita è la dominanza del fattore tecnologico e dei soggetti che lo generano e lo condizionano – esiste lo spazio per lavorare alla definizione di standard a cui fare riferimento quali "parametri di qualità" degli aspetti costitutivi delle tecnologie decentralizzate (come gli smart contracts)"*.

[45] Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 23, translation from italian, "*Considerata anche la difficoltà in alcuni casi – si pensi ad esempio al caso della DeFi nella sua accezione "pura" – di individuare soggetti specifici cui applicare determinati requisiti, è suscettibile di approfondimento, nell'ottica di un rafforzamento dei necessari presidi di mitigazione dei rischi, la possibilità di intervenire sui processi di definizione e di sviluppo degli standard tecnologici utilizzati*".

[46] On the central role of developers in the DeFi space and connected regulation see Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* cit., 6 – 7.

allow investors to take back control of their assets. However, compliance systems require some form of centralized human intervention to guarantee overview and liability allocation. In this sense, the main problem is how to reintroduce centralization without thwarting the core of DAOs innovation: code-enabled trust. Eminently, while many activities could be automatized – as KYC controls through digital identities – human supervision is still needed. In this sense, supervisors and developers should study how to build compliance systems which do not interfere with the core elements of a DAO's decentralized model.

The trade-off does not mean the problem is unsurmountable. Let's make an example of what a possible solution could look like: a compliance oracle system. As we have seen in chapter two, section eight, oracle systems are an integral part of smart contract development. They permit feeding a smart contract with external information to make decisions. A compliance oracle system – which would mimic the functioning of a compliance department – could, then, be built within a DAO.[47] The DAO's smart contract would be required to refer any compliance-sensitive question – as whether to onboard a client or file a Suspicious Activity Report – to such oracle. The oracle would then decide the course to take or could submit – at least in the most relevant cases – its opinion to the token holders for their ultimate decision. Such an oracle system would certainly recreate a certain level of centralization. However, the centralization would be limited in scope and visible to anyone joining the DAO who, by analysing the smart contract, would know in which cases a centralized decision will be taken. In addition, it would also allow precise identification of liabilities as decisions taken would be recorded in a shared, immutable record. Furthermore, given the deterministic nature of the smart contract, the oracle system could be submitted to the supervisor at the registration phase and be provided with a seal of compliance regarding the overall anti-money laundering strategy.

From a supervisory perspective, an oracle system managed through blockchain could ease supervision. On the one hand, given the immutability of the ledger, the decisions taken by the oracle would be transparent and auditable by the supervisors and external auditors. On the other hand, the publicity of the ledger could allow real-time supervision of the organization and trigger an inspection only when specific red flags are identified.

[47] The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 89

This is just an example of how compliance could work in a decentralized system. What is key here is underlining that to respond to the challenges created by DAOs new responses are needed. To adapt, legislators and supervisors have to increasingly focus on the supervision of coding. Informatic code is a neutral means filled with content by developers. The legislator has to act on such developers to guarantee legal principles are part of that content. *Ex-post*, reactive supervision and regulation are no more sufficient. Direct architectural intervention is key if we intend to adequately respond to the emerging challenges.

## 4. The Parliament's proposal for the Market in Crypto-assets Regulation. Lights and shades of an attempt to customized compliance.

*De iure condito*, the duties laid down by the European regulation on decentralized arrangements follow a traditional approach. DAOs are excluded from the regulatory purview and are not even categorized as a separate entity under MiCaR. Throughout this chapter, we have underlined how this approach seems to generate a lacuna, one that opens the way to legal uncertainty and criminal opportunities. However, as part of the MiCaR's legislative process, a proposal for a more tailored strategy to decentralized arrangements had surfaced.

The first position (hereinafter Proposal) taken by the European Parliament on the MiCaR's initial text included a specific regulation for decentralized autonomous organizations.[48] While this part of the Proposal has not been included in the final text, it represents an interesting example of the complexities, and possible solutions, connected with the regulation of decentralized autonomous organizations.

Let's then delve into this policy.

Article 3 of the Proposal included a definition of decentralized autonomous organization, which was defined as:

[48] European Parliament, *Report - A9-0052/2022 on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937*, 17 March 2022.

> "*a rule-based organisational system that is not controlled by any central authority and whose rules are entirely routed in its algorithm*".

This definition traced the line, between autonomous and traditional arrangements, in the concept of control. Autonomous is an organization where control solely lies in the rules established by the algorithm and no central, human authority retains unilateral governance powers.

Besides the definition, the Proposal laid down a specific discipline for DAOs. Particularly, the text shifted the authorization process from the issuer/offeror to the organization. As clarified by recitals 11 and 13, if the issuance of crypto-assets was to be pursued in a decentralized fashion there was no need for the issuer/offeror to "*organise as a single legal entity and should not be subject to regulation until the offering of the crypto-assets to the public is centralized*".[49]

Notwithstanding this exclusion, the Proposal, rather than ignoring decentralized autonomous organizations, provided for a customized discipline. This intention was clearly laid down by recital 13-a which stated:

> *"some types of crypto-assets are not issued by legal entities, but are instead managed by decentralised autonomous organisations. Provided that such crypto-assets are compatible with the requirements of this Regulation and do not pose a risk to investor protection, market integrity or financial stability, competent authorities should be permitted to admit such crypto-assets to trading on a Union trading platform for crypto-assets".*

Let's then see what this discipline looked like.

[49] See European Parliament, *Report - A9-0052/2022 on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937*, cit., recital 12 states "*given the different risks and opportunities raised by crypto-assets, it is necessary to lay down rules for issuers of crypto-assets that should be any legal person who offers to the public any type of crypto-assets or seeks the admission of such crypto-assets to a trading platform for crypto-assets. An issuer of crypto-assets should be a legal or natural person who issues any type of crypto-assets. An offeror of crypto-assets should be a legal entity that offers to the public any type of crypto-assets or asks for admission to trading of such crypto-assets on a trading platform for crypto-assets. Sometimes the issuance and exchange of crypto-assets may be decentralised, and that should be reflected and considered by the relevant legislation. Such decentralised issuers should not be required to organise as a single legal entity and should not be subject to regulation until the offering of the crypto-assets to the public is centralized",* recital 13 stated "*To ensure that all offers to the public of crypto-assets, other than asset-referenced tokens or e-money tokens, in the Union, or all the admissions of such crypto-assets to trading on a trading platform for crypto-assets are properly monitored and supervised by competent authorities, all issuers of crypto-assets should be legal entities. In order to promote, rather than to hinder, the decentralised issuance of crypto-assets, that requirement should not apply to decentralised issuers of crypto-assets unless and until the issuance of their crypto-assets is centralised"*.

As clarified by article 4, DAOs were among the entities authorized to offer crypto-assets to the public. However, to perform such an issuance, the same article, at paragraph 3-b, required *"competent authorities shall ensure that (decentralized autonomous organizations follow) steps identical to those set out in paragraph 1, points (b) to (d), have been taken"*.

These requirements are, in sum, two. First, draft, notify, and publish a white paper with the characteristics mandated by MiCaR (as detailed in chapter three, part two, section three of this text). Second, receive an authorization to operate within the Union by the competent authority of the home jurisdiction. According to the Proposal, then, DAOs were not obliged to follow all the duties laid down for a crypto-assets offers. Specifically, they were exempted from the requirements connected with the issuers/offerors company structure and composition. The Proposal, thus, recognized the specificities connected with the DAO's business model and, in particular, their detachment from any centralized issuer or offeror.

At the same time, the Proposal required DAOs to undergo an authorization process before operating within the Union. Interestingly for our ends, among the requirements imposed on a DAO the Proposal excluded the one laid down by letter ea) of the same article which required a crypto-assets offeror to guarantee it "*has measures in place to prevent the misuse of the offering of crypto-assets to the public or trading on a platform for crypto-assets for the purposes of money laundering or financing of terrorism in accordance with Directive (EU) 2015/849 of the European Parliament and of the Council*". Such an exclusion, if read together with the above-mentioned recital 13-a would have led to include among the elements to be evaluated by the competent authority only the risks posed to investor protection, market integrity, or financial stability. This exclusion is not clearly explainable and seems an oversight rather than a conscious choice also considering the initial stage of this Proposal. Eminently, there is no apparent reason why, once a DAO's structure is evaluated for registration, elements such as market integrity and investor protection should be assessed and not money laundering prevention.

The Proposal certainly included elements of great interest and innovation.

Particularly, the introduction of a definition of decentralized autonomous organization contributed to legal certainty and gave legal recognition to a pervasive phenomenon of the crypto-sphere. In addition, rooting the definition of DAO around the concept of control seems a correct choice. As underlined throughout this text, what distinguishes centralized and decentralized arrangements –

and generates the connected risks – is not the data storage model, or the technological infrastructure, but the governance structure. An arrangement or network is decentralized when its functioning does not depend on and cannot be influenced by a single (or a consortium) entity and is instead solely entrusted to the algorithm and distributed community of nodes. It is in this shift in the governance model that the key innovation of blockchain resides. Of great significance is the distinction made by the definition of algorithmic rules and centralized control. Following the definition, for an arrangement to be classified as decentralized both elements have to be present. This is a welcomed distinction. Eminently, algorithmic governance per se is not a guarantee of decentralization. The mere fact an organization's rules are encoded in an algorithm does not equate to decentralization. Algorithmic rules are a neutral medium, they can equally warrant centralized, unilateral control to a single or a group of individuals or decentralized, algorithmic governance. It is, hence, relevant that the definition distinguishes among the two characteristics that, together, define a DAO: an architecture rooted in algorithmic rules and the absence of centralized governance.

Shifting to the content of the Proposal, including DAOs within the purview of the registration regime seems a reasonable choice. Once a DAO is up and running it is complex to control its actions. However, if the control is imposed *ex-ante*, it is much easier to assess risks and mitigate them. Furthermore, the registration requirement is also more in line with the nature of the DAO. A DAO is essentially a string of code, a product, which once launched provides services according to its fundamental rules of functioning. In this sense, as with products, an *ex-ante* assessment concerning their safety is more effective and better addresses the risks.[50] If a failure or a weakness is identified in a DAO this can be addressed directly by the manufacturer (the developer) before the product enters the market. In a similar sense, extending the duty to draft a white paper seems reasonable as it constitutes a moment for developers to reflect and explain, to supervisors and investors, their DAO's business model and compliance mechanisms.

## 5. A cautionary tale: the Tornado Cash case

[50] For a similar approach see the opinion of the French *Autorité de contrôle prudentiel et de resolution* at footnote 707.

If the above is the law in the books' response to the problem of decentralization, a recent case allows us to take a peek into how the law in action will address decentralized arrangements. While Regulators are grappling with the policing of decentralized arrangements, Law Enforcement Authorities and Courts are faced with their effects. Eminently, the abstract risks posed by decentralized organizations have indeed converted into reality. These arrangements are used by criminals as a means to blur their transaction trail without undergoing compliance checks. Faced with such a reality, enforcement authorities are urged to act.[51] In the absence of a clear regulatory strategy aimed at addressing the risks posed by DAOs, a chaotic regulation-though-enforcement strategy will necessarily emerge to address the emerging risks, at least when they become too big to ignore.

The first, and so far only, case of this kind occurred in the summer of 2022. On the 8th of August of 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the crypto-assets mixer Tornado Cash.[52] The mixer was accused of having been used to launder more than seven billion dollars' worth of crypto-assets, including 455 million dollars connected with the Lazarus Group, a hacking collective connected with the North Korean government.[53]

This was a very unusual enforcement action as Tornado Cash was, in fact, a decentralized mixer operating on various blockchains, including Ethereum.[54] This meant that the sanctioning was not mainly addressed towards an organization or a person, but rather to be sanctioned was the code –

[51] World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 22, defines this approach as "regulation by enforcement".

[52] For the press release, United States Department of Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,* Press Release, 8th of August 2022, https://home.treasury.gov/news/press-releases/jy0916; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 91; for a description of the Mixer's functioning see M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 6.

[53] H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 1; for another case connected with Tornado Cash see the Frosties NFT as detailed by US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 23.

[54] M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 4 – 6; H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit., 1.

the smart contract – underlying Tornado Cash.[55] Any US person using that code interacts with a sanctioned entity, hence, infringing US Sanctions.

Tornado Cash constitutes the first case of direct sanctioning of informatic code, and, as so, raised numerous doubts.[56] Some argued that sanctioning of informatic code equalled to speech censorship, with Coin Center – a pro-crypto advisory group – launching a lawsuit on this basis.[57] Furthermore, others argued that Tornado Cash, not being an individual or an entity but a software, could not be the object of sanctions and was out of the purview of OFAC's powers.[58]

From our perspective, of great interest is not as much the sanctioning of the entity *per se*. Eminently, the OFAC's action was not aimed at ascertaining whether Tornado Cash was an obliged entity under the anti-money laundering regulation. The sanctioning of Tornado Cash does not bear any direct consequence for the classification of DAOs, also considering that the enforcement action was connected with international sanctions which are under a special, partially separate discipline.

What is crucial to our discussion is rather what happened to Tornado Cash's developer. On the 10th of August of 2022, just two days after the smart contract had been sanctioned by OFAC, the

[55] TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023*, cit., 4.

[56] H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization*, cit. 2.

[57] R. Miller, *Tornado Cash Sanctions By U.S. Treasury Draw Outrage, Suits From Crypto Community*, in *Forbes*, 26th October 2022, https://www.forbes.com/sites/rosemariemiller/2022/10/26/tornado-cash-sanctions-by-us-treasury-draw-outrage-suits-from-crypto-community/?sh=78a69cd1584c; this was not the only lawsuit initiated with other companies claiming the sanctioning infringed crypto-users' right to privacy, see M. Sun, *Removing Sanctions on Crypto Mixer Tornado Cash Won't Be Easy,* in *The Wall Street Journal,* 27th October 2022, https://www.wsj.com/articles/removing-sanctions-on-crypto-mixer-tornado-cash-wont-be-easy-11666891513; for an analysis of the connection between freedom of speech and software development in the EU see C. Rueckert, *Cryptocurrencies and fundamental rights,* cit., 14.

[58] N. De, *US Treasury Adds to Tornado Cash Sanctions With North Korea WMD Allegations*, in *Coindesk,* 8th of November 2022, https://www.coindesk.com/policy/2022/11/08/us-treasury-adds-to-tornado-cash-sanctions/. This allegation was rebutted by OFAC that clearly affirmed that the code underlying the DAO could be framed as a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization and hence sanctioned see OFAC, *Frequently Asked Questions n. 1095*, at https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1095 ; on the criticalities connected with such an action see M. Nadler – F. Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers,* cit., 14, *"Smart contracts are deployed and stored in the form of code on the blockchain. The code for each smart contract is public and can be read directly from the blockchain. This makes it trivial for anyone to copy and redeploy a new instance of any protocol at a different address. As a result, regulatory actions against a specific smart contract address are at best a temporary solution. Redeployments with identical code will force frequent updates of a sanctions list and lead to a game of "whack-a-mole." Slight variations in the code can make the situation even more challenging, as it may be unclear if something is a functional copy of a sanctioned protocol or a new implementation that must be treated and analyzed separately*".

Dutch Police arrested a 29 years-old man on money laundering charges, he was Alexey Persev the developer of Tornado Cash.[59] Since August he has been held in jail with a request for bail being denied by a Dutch Court in November.[60] If the Court were to confirm the indictment and condemn Persev this would set a ground-breaking precedent. Eminently, Tornado Cash is a multipurpose platform whose primary role is to provide privacy to crypto-assets' users. The mixer has been used by hundreds of thousands of users for both nefarious and licit purposes. Tornado Cash is, hence, not ontologically criminal. Its services have, however, been used by criminals. If Persev were to be found guilty of money laundering for actions committed by a software he designed, this would *de facto* nullify the exclusion provided by the FATF. At the same time, it will be up to the Court to ascertain and motivate how the actions of the software are causally linked with the individual who developed it. It is certainly still too early to ascertain if such a level of connection (according to the abovementioned indexes) can be drawn between Persev and Tornado Cash.

Whatever the outcome, the case underlines how a complete exclusion of DAOs from the purview of the anti-money laundering regulation is not feasible in the long term. Faced with large scale crime, enforcement authorities will have to react, and liabilities will have to be attributed.[61] In this sense, instead of excluding decentralized arrangements as a statement of principles, it would be more useful to devise a clear, certain framework customized to these new governance models.[62] The lack of any reference to DeFi and DAOs, in both the MiCaR and the Anti-money Laundering Package, constitute an important loophole and one the European policymaker should address before the introduction of the Package.

[59] For more information see the press release by the Dutch Police, FIOD, *Arrest of suspected developer of Tornado Cash,* Press Release, 12th of August 2022, https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/.

[60] J. Schickler, '*We Are All F****d': The Developers of Tornado Cash and the Future of Crypto,* in *Coindesk*, 5th of December 2022, https://www.coindesk.com/consensus-magazine/2022/12/05/alexey-pertsev-most-influential-2022/.

[61] As underlined by H. Axelsen – R. Omri, *How Should DAOs be Regulated? A New Perspective on Decentralization,* cit., 5, regarding the causes of the actions towards Tornado Cash "*While the source of the decision is unclear, it is to be presumed that the choice of issuing blanket sanctions was made due to a) a lack of appropriate regulation to enable proactive review, evaluation, and intervention in a proper format, b) the inability to identify any definite legal subject alongside growing concerns by the illegitimate activities conducted using Tornado Cash*".

[62] As underlined by World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* cit., 22, "*Enforcement actions are necessary to address issues relating to fraud and market manipulation, especially where crypto-assets blatantly resemble securities and are being used for explicitly prohibited activities such as money laundering. However, this approach is not recommended to build out a framework, as "regulation by enforcement" precludes any meaningful discussion of what should and should not be regulated*".

## 6. Closing remarks

Decentralized autonomous organizations pose a unique challenge to the legislature. The creation of headless organizations exclusively governed by code, tests concepts such as control and liability key to the sectorial policymaking strategy. The Union's regulator seems to have decided to ignore rather than address such a challenge. The exclusion of any reference to such arrangements both in MiCaR and the Anti-money Laundering Package, leaves DAOs in a legal vacuum. At the same time, the risks posed by such organizations which, *de facto*, provide a parallel unregulated market to centralized CASPs makes such a strategy untenable in the long term.

The risk is the emergence of a case-by-case regulation-through-enforcement strategy which undermines legal certainty and the orderly development of the market. The United States seems to have taken such an approach by equating centralized and decentralized arrangements and focusing on the activity carried out.[63] However, such an approach at the European level not only raises a problem of fairness but also contradicts the overall strategy underlying MiCaR to provide a clear playing field for crypto-companies.

A way forward could be to go back to the first approach proposed by the Parliament. That Proposal, while not transposed in the final version of the Regulation, could still be implemented. Eminently, it is the same MiCa Regulation to require the Commission to draft a report, within eighteen months of its entry into force. Among the topics the Report has to cover, MiCaR explicitly includes an "*assessment of the development of decentralised-finance in the crypto-assets markets and of the adequate regulatory treatment of decentralised crypto-asset systems*".[64]

It is in light of this upcoming Report that the French *Autorité de Contrôle Prudentiel et de Résolution* has recently published an, already cited, paper focused on the regulation of Decentralized Finance.

[63] See US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance,* cit., 3. "*However, a DeFi service that functions as a financial institution as defined by the BSA, regardless of whether the service is centralized of decentralized, will be required to comply with BSA obligations, including AML/CFT obligations. A DeFi service's claim that it is or plans to be "fully decentralized" does not impact its status as a financial institution under the BSA*".

[64] See article 122, paragraph 2, letter jc.

The paper takes a stance very similar to the one of the Parliament's proposal. Eminently, after clarifying that:

> *"the regulation of disintermediated finance cannot simply replicate the systems that currently govern traditional finance. On the contrary, regulations must take into account the specific features of DeFi"*[65]

It proposes to assign a legal statute to decentralized autonomous organizations,[66] and to, at least partially, assimilate CASP and DeFi intermediaries.[67]

A more balanced approach to the regulation of DAOs should, hence, pass by two fundamental moments.

First, the legislator should clearly define decentralized autonomous organizations. The definition should identify those elements that distinguish a fully decentralized from a partially decentralized organization. Second, impose on all DAOs a registration requirement. The registration would constitute a moment when the supervisor could signal to the DAO its status as fully or partially decentralized. In the former case, the DAO's developers should be mandated to introduce certain by-design elements to guarantee that the organization, while decentralized, can comply with relevant regulations. In the latter case, the supervisor would identify who the individuals or bodies with sufficient controls are so to clarify their qualification as covered entities.

In the presence of such a clear normative architecture, individual responsibilities could then be ascribed in case of non-compliance. Particularly, developers, as key players in the operation of decentralized software, would be fully aware of their need to introduce engrained compliance elements as part of their activity if their DAO is to operate within the Union or suffer the related consequences. Eminently, if the values enshrined by the anti-money laundering regulation are fundamental for our society there seems to be no reason why code-creation could be allowed to circumvent them. At the same time, the developers would always have the possibility to avoid the European market. The standard for such an exclusion has already been spelled out by the

[65] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 2.
[66] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 3.
[67] O. Fliche – J. Uri – M. Vileyn, *"Decentralised" or "disintermediated" finance: what regulatory response?*, cit., 39, "*It would therefore appear appropriate, as a first step, to explicitly extend the scope of the provisions of the MiCA Regulation concerning CASPs to DeFi intermediaries*"; see also D.A. Zetzsche - R.P. Buckley - D.W. Arner - M.C. van Ek, *Remaining regulatory challenges in digital finance and crypto- assets after MiCA*, cit., 29; The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* cit., 89

European Court of Justice, even though in a different setting. In Google versus Commission Nationale de l'Informatique et des Liberte´ s (CNIL)[68] the Court clarified that to be exempt from European rules the provider has to take sufficiently effective measures to ensure the protection of the data subject's fundamental rights. In this sense, the DAO's developers could be exempt from the registration requirement by introducing engrained processes to avoid investors and customers from the Union – by for example screening the connected IP addresses. This would guarantee that the Union's regulation is not perceived as an attempt to globalize the connected strategy and stays within its territorial boundaries.

In sum, simply ignoring a problem does not make it go away. The Regulator has to address the new governance structure proposed by DAOs and introduce innovative solutions customized to the latter.

[68] European Court of Justice, C 507/17 Google v. CNIL, C 507/17, 2019.

# Closing Remarks

The inexorable dance between law and reality is one of the most fascinating aspects of legal scholarship. The law is, at the same time, source and product of the reality it regulates, being influenced while influencing its development.[1] Sometimes the law precedes a societal change, many times it is the result of one. Maintaining this synergy is key in guaranteeing its continuing efficacy.

Digital technologies are testing this delicate relationship. The speed and depth of the change such technologies have spurred are challenging the limits of policymaking. At the same time, their impact on the physiognomy of the world means their development and conformation is per se a normative act, frequently in competition with traditional legislation. Through coding, the developer fills machine-readable text with content. In so doing it makes normative choices that influence fundamental characters of our pervasively digitalized society.

Blockchain constitutes an example of such an exercise of legislation through code. The introduction of a new governance model for the management of valuable data affects how humans interact and organize. Most importantly it affects the architecture of trust in complex immaterial societies. By moving the horizon of what is possible, blockchain challenges the existence of the current networked society rooted in trust brokers.

The present text has analysed one act of this dance between blockchain and the law: the interrelation between crypto-assets and financial monitoring. Bearers of conflicting interests – freedom through privacy the former, security through monitoring the latter – they have struggled to find a common ground.

[1] As stated by A. Barak, *The Judge in a Democracy,* Princeton University Press, 2006, 8, "*As change in social reality is the law of life, responsiveness to change in social reality is the life of the law*".

The introduction of a decentralized, disintermediated value transfer system constitutes an inevitable challenge for a policy field rooted in centralized, intermediaries. On the one hand, crypto-assets, through peer-to-peer transactions, allow to circumvent the anti-money laundering monitoring architecture. On the other hand, blockchain-based organizations introduce horizontal, code-based governance models for which the current compliance regulation - envisioned for hierarchical, human-operated organizations - seems unfit.

The main overarching critique we can move to the policymaker's strategy so far is a lack of imagination. Faced with a ground shifting technology, the legislator has been unable to modify its pre-existing tactic. The legislations introduced so far simply extend pre-existing duties to a series of intermediaries identified in the crypto-market. The peculiarities of blockchain's recordkeeping structure and governance model have been mostly ignored. Furthermore, the legislator has shied away from the most complex issues, as the regulation of DAOs or the treatment of self-hosted wallets. This has created a legal vacuum that is being filled by enforcement authorities through a case-by-case approach.

However, momentum seems to be building. As underlined by the Reports published by the French and Italian supervisors there is an increasing interest for customized, innovative policies. If the law has to be in synergy with reality, it can't remain rigid in the face of changing circumstances. In turn, it has to adapt, and mould to the new reality.

The present text aims at facilitating such an adaptation process in two synergic ways.

On the one hand, by providing a complete picture of blockchain's functioning, historical development, intersection with financial monitoring, and policy approaches. Rational choices need complete information. This thesis provides scholars, stakeholders, and policymakers with such information to foster better informed discussion and legislation.

On the other hand, by proposing possible avenues for better adaptation and customization. While such proposals have already been detailed throughout the thesis, there are three main policy points we would like to reiterate as key to a future strategy.

First, the legislator needs to clearly distinguish between decentralized and centralized crypto-assets. The governance structure of the network and/or organization is key in defining the risks and opportunities of the specific crypto-asset for anti-money laundering purposes: a centrally governed network is not different from centralized systems: it is in the decentralization of the governance that the key innovation and risk of blockcahin resides. Equating centralized and decentralized crypto-assets constitutes, hence, a hindrance to customization.

Second, the transparency of blockchain data should be better exploited. The direct availability of financial data should push for a more direct intervention of the supervisor. The current system rooted in profiling may be rebuilt as a system based on financial data analysis, through pattern and macro-trend analysis software. This way the precision of money laundering investigations would be enhanced as the Suspicious Activity Reports would originate from the supervisor and then be investigated by the intermediary. Furthermore, the burden on private companies would be alleviated, hence, reducing the barriers of entry to the market and fostering competition. Furthermore, given the forthcoming introduction of a Digital Euro, such an approach could be piloted in the crypto-assets market to then be expanded in the overall financial market.

Third, for decentralized arrangements, it is necessary to move towards a product-like regulation by reinforcing the role of software developers and compliance-by-design. In decentralized networks/organizations code is king. It is on the code that the regulator has to act in order to guarantee compliance. Not by mandating standards, but by dictating specific goals the code has to achieve. If coding is a normative activity, then it should include the goals and norms expressed through law by the society. To this end, software developers of decentralized arrangements should be included among the Crypto-assets Service Providers. A registration procedure should be introduced to guarantee their product (the autonomous software) is compliant with regulations and not harmful to society. A clear definition of DAO, along the lines of the one proposed by the Parliament, shall be developed.

# Bibliography

## Books, book chapters, and articles

Accorsi, C. – Brening, R. – Müller, G., *Economic analysis of cryptocurrency backed money laundering* in *Twenty-Third European Conference on Information Systems (ECIS)*, 2015

Allen, S., et al. *Design choices for central bank digital currency: Policy and technical considerations*, No. w27634. National Bureau of Economic Research, 2020

Anderson, P., *Cypherpunk ethics. Radical ethics for the digital age*, Routledge, 2022

Antonopoulos, A., *Mastering Bitcoin. Programming the Open Blockchain*, O'Reilly, 2017

Armer, P., *Computer Technology and surveillance,* University of Stanford - Center for Advanced Study in the Behavioral Sciences, 1975

Asmundson, I. – Oner, C., *What is money?*, in *Finance & Development,* 49/3, 2012

Auer, R., *Embedded Supervision: How to build regulation in decentralized finance*, CESIFO Working Papers, 9771, 2022

Axelsen, H. – Jensen, J. – Omri, R., *When is a DAO Decentralized?, in Complex Systems Informatics and Modeling Quarterly,* 31, 2022

Axelsen, H.– Omri, R., *How Should DAOs be Regulated? A New Perspective on Decentralization*, in *AMPLIFY*, 35/10, 2022.

Azar, C. – Sandén, B. A., *The elusive quest for technology-neutral policies* in *Environmental Innovation and Societal Transitions,* 1/1, 2011

Bains, M., *Blockchain consensus mechanisms: A primer for supervisors*, International Monetary Fund, 2022

Balaskas, A. - Franqueira, V., *Analytical tools for blockchain: Review, taxonomy and open challenges*, in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE,* 2018

Barak, A. *The Judge in a Democracy,* Princeton University Press, 2006

Bello, A. – Harvey, J., *From a risk-based to an uncertainty-based approach to anti-money laundering compliance,* in *Security Journal,* 30, 2017

Berggren, C. – Asplund, J., *Identifying and Analyzing Digital Payment Flows Regarding Illegal Purposes on the Internet: I Samarbete Med Cgi Och Finanskoalitionen*, Independent thesis advanced level, Linköping University, 2016

Bergström, M., *The Global AML Regime and the EU AML Directives: Prevention and Control,* in King, C. – Walker, C. – Gurulé, J. (Eds.), *The Palgrave handbook of criminal and terrorism financing law*, Palgrave Macmillan, 2018, 34.

Bilotta, N. *CBDCs and Stablecoins: The Scramble for (Controllable) Anonymity* in Bilotta, N. – Botti, F. (eds.) *The (Near) Future of Central Bank Digital Currencies*, Peter Lang International Academic Publisher, 2021

Blandin, A. et al., *Global cryptoasset regulatory landscape study*, in *University of Cambridge Faculty of Law Research Paper,* 23, 2019

Blandin, A. et *al., 3rd Global Cryptoasset Benchmarking Study*, Cambride Center for Alternative Finance*,* 2020

Bohannon, J., *The bitcoin bust* in *Science*, 351, 2016

Bolt, W. – Lubbersen, V. – Wierts, P., *Getting the balance right: Crypto, stablecoin and central bank digital currency*, in *Journal of Payments Strategy & Systems,* 16.1, 202

Boreiko, D. – Ferrarini, G. – Giudici, P., *Blockchain startups and prospectus regulation*, in *European Business Organization Law Review*, 20, 2019

Bradford, A., *The brussels effect* in *Nw. UL Rev.,* 107, 2012

Brown, D., *Cryptocurrency and Criminality: The Bitcoin Opportunity* in *The Police Journal: Theory, Practice and Principles*, 2016

Brunton, F., *Digital Cash. The unknown history of the anarchist, utopians, and technologists who created cryptocurrencies,* Princeton University Press, 2019

Budish, E., *The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain* in *University of Chicago, Becker Friedman Institute for Economics Working Paper,* 83, 2022

Campbell-Verduyn, M., *Bitcoin, crypto-coins, and global anti-money laundering governance*, in *Crime, Law and Social Change*, 69, 2018

Campbell, R., et al., *Distributed Ledger Technologies in the Public Sector: Learnings on the application of Distributed Ledger Technologies across international public services and their role in realising Scotland's full potential in a digital world*, The Scottish Government, 2018

Carlisle, D., *Virtual currencies and financial crime: Challenges and opportunities*, Royal United Services Institute for Defence and Security Studies, London, 2017

Caria, R., *Definitions of Smart Contracts: Between Law and Code*, in Di Matteo, L. – Cannarsa, M. – Poncibò, C. (Eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge University Press, 2019

Carney, M., *The Future of Money,* Bank of England, 2018

Cassara, J., *Money laundering and illicit financial flows,* 2020

Chaum, D., *Security without identification: Transaction systems to make big brother obsolete*, in *Communications of the ACM,* 28.10, 1985

Chaum, D., *Achieving electronic privacy*, in *Scientific American*, 267.2, 1992

Cocco, L. – Marchesi, M., *Modeling and Simulation of the Economics of Mining in the Bitcoin Market*, in *PLoS ONE*, 11(10), 2016

Coelho, R. – Fishman, J. – Garcia Ocampo, D., *Supervising cryptoassets for anti-money laundering*, Bank for International Settlements, Financial Stability Institute, 2021

Coghlan, E. – McCorkell, L. – Hinkley, S. *What Really Caused the Great Recession?*, Berkley Institute for Research on Labor and Employment Policy Brief, 2018

Dalla Pellegrina, L. – Masciandaro, D., *The risk-based approach in the new European anti-money laundering legislation: a law and economics view* in *Review of law & economics,* 2, 2009

Dalla Pellegrina, L. – Di Maio , G.– Masciandaro, D. – Saraceno, M., *Are Bankers "Crying Wolf"? Type I, Type II Errors and Deterrence in Anti-Money Laundering: The Italian Case* in *Italian Economic Journal,* 2022

D'amelio, A. – Soana, G., *Blockchain technology to prevent tax frauds and money laundering in the European Customs Union: quo vadis?,* in *Dirittto e Pratica Tributaria Internazionale*, 2021

De Filippi, P. – Loveluck, B., *The invisible politics of bitcoin: governance crisis of a decentralized infrastructure*, in *Internet policy review,* 5.4, 2016

De Filippi, P. – Wright, A., *Blockchain and law. The rule of code*, Harvard University Press, 2018

De Filippi, P. – Mannan, M. – Reijers, W., *Blockchain as a confidence machine: The problem of trust & challenges of governance*, in *Technology In Society,* 62, 2020

De la Dehesa, G., *Twelve Market and Government Failures Leading to the 2008–09 Financial Crisis*, Group of Thirty, 2009

dell'Osso, A., *Riciclaggio di proventi illeciti e sistema penale***,** Giappichelli, 2017

Delivorias, A., *Understanding initial coin offerings. A new means of raising funds based on blockchain*, European Parliamentary Research Service, 2021

Devdeepta, B. – Camerer, C., *Trust and Behavioral Economics* in F. Krueger (eds.), *The Neurobiology of Trust*, Cambridge University press, 2021

Durner, T. – Shetret, L., *Understanding bank de-risking and its effects on financial inclusion: an exploratory study*, Global Center on Cooperative Security Oxfam International, 2015

Escudero-Pascual, A. – Hosein, I., *Questioning lawful access to traffic data*, in *Communications of the ACM,* 47/3, 2004

Fatjon, K. – Martino, E. –Pacces, A. M., *fintech and The Law and Economics of Disintermediation*, Routledge Handbook of Financial Technology and Law, 2021

Ferreira, A. – Sandner, P., *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*, in *Computer Law & Security Review,* 43, 2021

Finck, M., *Blockchains and data protection in the European Union,* in *European Data Protection Law Review,* 4, 2018

Finck, M., Blockchain regulation and governance in Europe, Cambridge University Press, 2018

Findlay, C., *Participatory cultures, trust technologies and decentralisation: innovation opportunities for recordkeeping*, in *Archives and Manuscripts*, 45/3, 2017

Fliche, O. – Uri, J. – Vileyn, M., *"Decentralised" or "disintermediated" finance: what regulatory response?*, Banque de France Fintech-Innovation Hub, Paris, 2023

Forgang, G., *Money Laundering through Cryptocurrencies* in *Economic Crime Forensics Capstones*, 2019

Frick, T., *Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland*, in *Era Forum*, 20/1, 2019

Gilmour, N., *Understanding the practices behind money laundering–A rational choice interpretation,* in *International Journal of Law, Crime and Justice,* 44, 2016

Gorton, G. – Zhang, J., *Bank Runs During Crypto Winter*, in *University of Michigan Law & Econ Research Paper*, 2023

Greenberg, B., *Rethinking Technology Neutrality* in *Minn. L. Rev*, 2016, 100

Grimmelmann, J., *All Smart Contracts are Ambiguous*, in *Journal of Law & Innovation*, 2019

Gullo, A., *Autoriciclaggio e reati tributari,* in *Diritto Penale Contemporaneo,* 2018

Gullo, A., *Nuove Frontiere tecnologiche e Sistema penale: alcune note introduttive,* in *Diritto Penale Contemporaneo Rivista Trimestrale,* 2, 2019, IX

Gullo, A., *Compliance*, in *Archivio Penale*, 1, 2023

Haber, S. - Stornetta, W.S., *How to time-stamp a digital document* in *Journal of Cryptology*, 3/2, 1991

Hacker, P. – Thomale, C., *Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law*, in *European Company and Financial Law Review*, 4, 2018

Haffke, L. – Fromberger, M. – Zimmermann, P., *Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them*, in *Journal of Banking Regulation,* 2, 2020

Hardy, R. - Norgaard, J., *Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web* in *Journal of Institutional Economics,* 12, 3, 2016

Harlev, M., et al., *Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning*, in *Proceedings of the 51st Hawaii International Conference on System Sciences,* 2018

Hassan, S. – De Filippi, P. *Decentralized autonomous organization*, in *Internet Policy Review,* 2, 2021

Hileman, G. – Rauchs, M., *Global cryptocurrency benchmarking study*, Cambridge Centre for Alternative Finance, 2017

Hirshman, J. – Huang, Y. – Macke, S., *Unsupervised approaches to detecting anomalous behaviour in the bitcoin transaction network,* Technical report, Stanford University, 2013

Hobbes, T., *The Leviathan*, London, 1651

Hornuf, L. – Kück, T. – Schwienbacher, A,. *Initial coin offerings, information disclosure, and fraud* in *Small Business Economics,* 4, 2022

Houben, R., – Snyers, A., *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament, 2018

Hughes, E., *a cypherpunks manifesto*, 1993

Hughes, S., '*Gatekeepers' Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes As Permission-less Blockchain-Based Transactions Pose Challenges to Current Means to'Follow the Money'* in *Indiana Legal Studies Research Paper*, 408, 2019

Hütten, M., *The soft spot of hard code: blockchain technology, network governance and pitfalls of technological utopianism*, in *Global Networks*, 19.3, 2019

Ittay, E. – Gün Sirer, E., *Majority is not enough: Bitcoin mining is vulnerable*, in *International conference on financial cryptography and data security*. Springer, 2014

Jakubenko, A. et. al., *Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument,* in *KnE Social Sciences*, 3, 2, 2018

Jarvis, C., *cypherpunk ideology: objectives, profiles, and influences (1992-1998),* in *Internet Histories,* 2021

Karasek-Wojciechowicz, I., *Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces* in *Journal of Cybersecurity*, 1, 2021

Kahn, C. – Roberds, W., *Why pay? An introduction to payments economics*, in *Journal of Financial Intermediation,* 18/1, 2009

Kolachala, K., et al., *SoK: Money Laundering in Cryptocurrencies*, in *The 16th International Conference on Availability, Reliability and Security*, 2021

Koops, B. – Jaap-Henk, H.– Leenes, R., *Open-source intelligence and privacy by design*, in *Computer Law & Security Review,* 6, 2013

Koster, H., *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework* in *Journal of Money Laundering Control,* 2, 2020

Kruisbergen, E.W. – Leukfeldt, E.R – Kleemans, E.R. - Roks, R.A., *Money talks money laundering choices of organized crime offenders in a digital age* in *Journal of Crime and Justice,* 5, 2019

Kuner, C. – Cate, F. – Lynskey, O. – Millard, C. – Ni Loideain, N. – Svantesson, D., *Blockchain versus data protection* in *International Data Privacy Law*, 2, 2018

Legal, D. – Ortiz Ibarrola, G. – Blanco, C., *Moneda Digital del Banco Central: Implicancias para la estabilidad financiera y la politica monetaria en Paraguay,* Documentos de Trabajo n. 27 Banco Central del Paraguay, 2022

Leuprecht, C. – Jenkins, C. – Hamilton, R., *Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency*, in *Journal of Financial Crime*, 2022, 4

Lennart, A., *The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum*, in *FinTech*, 1.3, 2022

Luciano, D. – Prichett, G., *Cryptology: From Caesar ciphers to public-key cryptosystems* in *The College Mathematics Journal,* 18/1, 1987

Lyle, A., *Legal considerations for using open source intelligence in the context of cybercrime and cyberterrorism*, in *Open Source Intelligence Investigation: From Strategy to Implementation,* 2016

Maia, G. –Vieira dos Santos, J., *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*, 2021

Manes, V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale,* in *Rivista Trimestrale di Diritto Penale dell'economia,* 2004

May, T., *The cryptoanarchist manifesto,* 1988

Martino, E., *Comparative Cryptocurrencies and Stablecoins Regulation A framework for a functional comparative analysis,* EBI Working Papers, 145, 2023

MeikleJohn, S., et al., *A Fistful of Bitcoins: Characterizing Payments among Men with No Names*, in *Proceedings of the 2013 Conference on Internet Measurement Conference*, 2016

Mesquita, B. – Maranhao, S. – Seigneur, J., *Enabling KYC and AML verification in DeFi service*, Crypto Valley Association, Zug, 2022

Minto, A., *The legal characterization of crypto-exchange platforms*, in *Global Jurist,* 22/1, 2021

Minto, A., *Riflessioni sull'applicabilità della disciplina antiriciclaggio ai Non-Fungible Tokens ("NFT")*, in *Rivista di Diritto Bancario*, 1, 2023

Minto, A. – Skovmand Rasmussen, N., *Approaching the Danske Bank Scandal in a "Tragedy of the Commons" Perspective: Implications for Anti-Money Laundering Institutional Design and Regulatory Reforms in Europe,* in *European Company and Financial Law Review,* 19/2, 2022

Mitsilegas, V. – Vavoula, N., *The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law* in *Maastricht Journal of European and Comparative Law*, 2

Moffett, T. A., *CFTC & SEC: The Wild West of Cryptocurrency Regulation, U. Rich. L. Rev.*, 52, 2022

Mohan, C., *State of public and private blockchains: Myths and reality*, in *Proceedings of the 2019 International Conference on Management of Data*, 2019

Morgante, G., *Criminal Law and Risk Management: From Tradition to Innovation*, in *Global Jurist*, 16/3, 2016

Morrison, R. – Mazey, N. – Wingreen, S., *The DAO controversy: the case for a new species of corporate governance?*, in *Frontiers in Blockchain* 3, 2020

Moiseienko, A. – Kraft, O., *From money mules to chain hopping. Targeting the finances of cybercrime,* Royal United Services Institute for Defence and Security Studies, London, 2018

Moiseienko, A., *Does international law prohibit the facilitation of money laundering?* in *Leiden Journal of International Law*, 2022

Möser, M. – Böhme, R. – Breuker, D., *An inquiry into money laundering tools in the Bitcoin ecosystem*, in *2013 APWG eCrime Researchers Summit*, 2013

Muller, W., *Anti-money laundering–a short history*, in W. Muller – C. H. K ̈alin – J. G. Goldsworth (eds.) *Anti-Money laundering: International law and practice*, Wiley, 2007

Nadler, M. – Schär, F., *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, Federal Reserve Bank of Saint Louis, 2023

Nadini, M. – Alessandretti, L. – Di Giacinto, F. – Martino, M. – Aiello, L. – Baronchelli*,* A., *Mapping the NFT revolution: market trends, trade networks, and visual features,* in *Scientific reports*, 11,1, 2021

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009

Nofer, M., et al. *Blockchain* in *Business & Information Systems Engineering* , 59/3, 2017

O'Dwyer, K. – Malone, D., *Bitcoin Mining and its Energy Footprint,* in, *Proceedings of the 25th Joint IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 2014

Panetta, P., *Crypto-assets or virtual currencies as they were called before it was realized that they cannot perform the functions of money* in *SUERF Policy Notes*, 40, 2018

Pelker Alden, C. – Brown, C. – Tucker, R. *Using Blockchain Analysis from Investigation to Trial*, in *Department of Justice Journal of Federal Law and Practice*, 69

Piergallini, C., *Autoriciclaggio, concorso di persone e responsabilità dell'ente*, in *Criminalia*, 2015

Pol, R., *Anti-money laundering: The world's least effective policy experiment? Together, we can fix it*, in *Policy design and practice,* 1, 2020

Porat, A. –Avneesh, P. – Shah, P. – Adkar*,* V., *Blockchain Consensus : An analysis of Proof-of-Work and its applications*, 2017

Rajamäki, J. – Sarlio-Siintola, S. – Alapuranen, N. – Nevanperä, M., *Privacy and data protection in open source intelligence and big data analytics: Case 'MARISA'* in *Ethics as a resource. Examples of RDI projects and educational development*, 2020

Ranganathan, G. – Fernando, X. – Fuqian*,* S., *Inventive Communication and Computational Technologies*, Springer, 2021

Reed, C., *Taking sides on technology neutrality,* in *SCRIPTed: Journal of Law, Technology and Society*, 4/3, 2007

Ross, S. – Hannan, M., *Money laundering regulation and risk-based decision-making*, in *Journal of Money Laundering Control*, 1, 2007

Rousseau, D., et al., *Not so different after all: A cross-discipline view of trust* in *Academy of management review*, 23/3, 1998

Rousseau, J., *Du Contrat Social, ou principes du droit politique* in *Collection Complète des Oeuvres*, Geneva, 1789

Rueckert, C., *Cryptocurrencies and fundamental rights*, in *Journal of Cybersecurity*, 1, 2019

Savona, E. - Riccardi, M., *Assessing the risk of money laundering: research challenges and implications for practitioners*, in *European Journal on Criminal Policy and Research*, 25, 2019

Schwarcz, S., *Regulating Digital Currencies: Towards an Analytical Framework*, in *Boston University Law Review*, 102

Shahaab, A., et al., *Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review*, in *IEEE Access*, 7/2, 2019

Shams, H., *Legal Globalization: money laundering law and other cases,* in *Sir Joseph Gold Memorial Series*, 2004

Shere, A., *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis*, in *The New Collection,* 3, 2020

Simonova, A., *The risk-based approach to anti-money laundering: problems and solutions* in *Journal of Money Laundering Control*, 4, 2011

Soana, G., *Regulating cryptocurrency checkpoints. Fighting a trench war with cavalry?,* in *Economic Notes,* 2021

Soderberg, G., *Behind the Scenes of Central Bank Digital Currency Emerging Trends, Insights, and Policy Lessons*, Fintech Notes International Monetary Fund, 2022

Sompolinsky, Y. – Zohar, A., *Bitcoin's underlying incentives*, in *Communications of the ACM,* 61.3, 2018

Sudipta, B. – Waymire, G. B., *Recordkeeping and human evolution*, in *Accounting horizons* 20/3, 2006

Szabo, N., *Smart Contracts*, 1994

Szabo, N., *Smart Contracts: Building Blocks for Digital Markets*, 1996

Thapa, R. – Sharma, P. – Hüllmann, J. – Savarimuthu, B., *Identifying Influence Mechanisms in Permissionless Blockchain Communities: The Bitcoin Case* in *42nd International Conference on Information Systems (ICIS)*, 2021

Thompson, M., *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, in *B.U. J. Sci. & TECH. L.*, 18/303, 2012

Tovanich, N. – Cazabet, R., *Pattern Analysis of Money Flows in the Bitcoin Blockchain* in *Complex Networks and Their Applications* in *XI: Proceedings of The Eleventh International Conference on Complex Networks and Their Applications: COMPLEX NETWORKS 2022*, 1, 2023

Tronnier, F. – Harborth, D. - Hamm, P., *Investigating privacy concerns and trust in the digital Euro in Germany*, in *Electronic Commerce Research and Applications,* 53, 2022

Trozze, A., et al., *Cryptocurrencies and future financial crime*, in *Crime Science,* 11/1, 2022

Tucker, O., *The flow of illicit funds. A case study approach to anti-money laundering compliance,* Georgetown University Press, 2022

Van Duyne, P. – Harvey, J. H. – Gelemerova, L. Y., *The critical handbook of money laundering: Policy, analysis and myths*, Springer, 2018

Van Meerbeeck, J., *The principle of legal certainty in the case law of the European court of justice: from certainty to trust*, in *European Law Review,* 41, 2016

Veerpalu, A. – da Cruz Rodrigues e Silva, E., *Hitting the White Ball: The Technology Neutrality Principle and Blockchain-Based Applications* in *The Indian Journal of Law and Technology,* 15,2, 2019

Villányi, B., *Money laundering: History, regulations, and techniques*, in *Oxford Research Encyclopedia of Criminology and Criminal Justice*, 2021

von Wachter, V. – Regner, J. R. – Ross, O., *NFT wash trading: Quantifying suspicious behaviour in NFT markets,* in *Financial Cryptography and Data Security. FC 2022 International Workshops,* 2022,

Werbach, K., *The Blockchain and the new architecture of trust*, The MIT Press, 2018

Xia, Y.A. – Grover, S. - Lieb, R.C., *Keeping PACE with blockchain in ocean transportation*, in *Supply Chain Management Review,* 2021, 25

Zetzsche, D. – Annunziata, F. – Douglas, W. - Buckley, R. P., *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy* in *Capital Markets Law Journal*, 16.2, 2021

Zetzsche, D. A. – Buckley, R.P. – Arner, D.W. - van Ek, M.C., *Remaining regulatory challenges in digital finance and crypto- assets after MiCA,* European Parliament, 2023

Zou, M., *Code, and other laws of blockchain* in *Oxford Journal of Legal Studies*, 40/3, 2020

## Website pages and web articles

Adler, D., *Silk Road: The Dark Side of Cryptocurrency*, in *Fordham Journal of Corporate and Financial Law Blog*, 21 February 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/

Bogost, I., *Cryptocurrencies may be a path to authoritarianism*, The Atlantic, 30 May 2017, https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/

Browne, R., *Man makes last-ditch effort to recover $280 million in bitcoin he accidentally threw out*, in *CNBC*, 15 January 2021, https://www.cnbc.com/2021/01/15/uk-man-makes-last-ditch-effort-to-recover-lost-bitcoin-hard-drive.html

Choo, R., *Bitcoin's Impacts on Climate and the Environment,* in *State of the Planet (Columbia Climate School Blog)*, 20 September 2021, https://news.climate.columbia.edu/2021/09/20/bitcoins-impacts-on-climate-and-the-environment/

De, N., *US Treasury Adds to Tornado Cash Sanctions With North Korea WMD Allegations*, in *Coindesk,* 8th of November 2022, https://www.coindesk.com/policy/2022/11/08/us-treasury-adds-to-tornado-cash-sanctions/

Allen-Ebrahimian, B., *The man who nailed the jello to the wall*, in *Foreign Policy,* 29th June 2016, https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/

Elliott, F. – Duncan, G., *Chancellor Alistair Darling on brink of second bailout for banks*, in *The Times*, 3 January 2009, https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

Ennis, P., *An Anatomy of Bitcoin's Great Scaling Debate,* in *Coindesk,* 15th May 2016, https://www.coindesk.com/markets/2016/05/15/an-anatomy-of-bitcoins-great-scaling-debate/

European Banking Authority, *EBA issues Guidelines to challenge unwarranted de-risking and safeguard access to financial services to vulnerable customers,* Paris, 31 March 2023, https://www.eba.europa.eu/eba-issues-guidelines-challenge-unwarranted-de-risking-and-safeguard-access-financial-services

European Central Bank, *Eurosystem launches digital euro project*, 14th July 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

European Central Bank, *Digital Euro Project Timeline*, 2021, https://www.ecb.europa.eu/paym/digital_euro/shared/pdf/Digital_euro_project_timeline.en.pdf

Eurogroup, *statement on the digital euro project*, 16th January 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/01/16/eurogroup-statement-on-the-digital-euro-project-16-january-2023/

European Parliament, *Cryptocurrencies in the EU: new rules to boost benefits and curb threats,* Press Release, 14th of March 2022, https://www.europarl.europa.eu/news/en/press-room/20220309IPR25162/cryptocurrencies-in-the-eu-new-rules-to-boost-benefits-and-curb-threats

FinCEN, *What is Money Laundering?,* FinCEN website, https://www.fincen.gov/what-money-laundering

FIOD, *Arrest of suspected developer of Tornado Cash,* Press Release, 12th of August 2022, https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/

Huang, K., *Why Did FTX Collapse? Here's What to Know,* in *The New York Times,* 10 November 2022, https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html

Handagama, S., *Proposal Limiting Proof of Work is rejected in  EU Parliament Committeee vote*, in *CoinDesk*, 14 March 2022, https://www.coindesk.com/policy/2022/03/14/proposal-limiting-proof-of-work-is-rejected-in-eu-parliament-committee-vote-sources/

Jayachandran, P., *The difference between public and private blockchain*, in *Blockchain Pulse: IBM Blockchain Blog*, https://www.ibm.com/blogs/blockchain/2017/05/the-differen- ce-between-public-and-private-blockchain/

Kahn, C., *Tokens vs. Accounts: Why the Distinction Still Matters,* Federal Reserve Bank of Saint Louis, 5 October 2020, https://www.stlouisfed.org/on-the-economy/2020/october/tokens-accounts-why-distinction-matters

Leisig, M., *My trip Down the Crypto Rabbit Hole in search of the DAO hacker,* in *Bloomberg,* 16 September 2020, https://www.bloomberg.com/news/articles/2020-09-16/a-trip-down-the-crypto-rabbit-hole-in-search-of-the-dao-hacker

Levy, S., *Battle of the Clipper Chip*, in *The New York Times*, 12 June 1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

McCaul, E., *Mind the gap: we need better oversight of crypto activities*, European Central Bank Blog, 5th April 2023, https://www.bankingsupervision.europa.eu/press/blog/2023/html/ssm.blog230405~03fd3d664f.en.html

B. Moens – E. Wax, *African diplomats can't open bank accounts in Brussels — and Qatar scandal could make things tougher,* Politico, 22nd December 2022, https://www.politico.eu/article/african-diplomats-cant-open-bank-accounts-in-brussels-and-qatar-scandal-could-make-things-tougher/

Mosna, A. – Soana, G., *When art goes virtual: what status for collectible NFTs under the current EU Anti Money-Laundering regime?,* in *Eu Law Analysis,* 13th of August 2022, http://eulawanalysis.blogspot.com/2022/08/when-art-goes-virtual-what-status-for.html

Miller, R., *Tornado Cash Sanctions By U.S. Treasury Draw Outrage, Suits From Crypto Community*, in *Forbes*, 26th October 2022, https://www.forbes.com/sites/rosemariemiller/2022/10/26/tornado-cash-sanctions-by-us-treasury-draw-outrage-suits-from-crypto-community/?sh=78a69cd1584c

New York Times, *Al Capone guilty of tax evasion,* 17th October 1931, https://archive.nytimes.com/learning.blogs.nytimes.com/2011/10/17/oct-17-1931-al-capone-guilty-of-tax-evasion/

New York Times, *The Coin that could wreck crypto*, 17th June 2022, https://www.nytimes.com/2022/06/17/technology/tether-stablecoin-cryptocurrency.html

Nicolle, E. – Pronina, L., *EU Crypto Proposal Seen as De-Facto Bitcoin Ban Fails in Vote*, in *Bloomberg,* 14th of March 2022, https://www.bloomberg.com/news/articles/2022-03-14/eu-crypto-proposal-seen-as-de-facto-bitcoin-ban-fails-in-vote?leadSource=uverify%20wall

Popper, N., *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes,* in *The New York Times*, 12 January 2021, https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

Roberts, S. *How 'Trustless' Is Bitcoin, Really?* in *The New York Times,* 6 June 2022, https://www.nytimes.com/2022/06/06/science/bitcoin-nakamoto-blackburn-crypto.html

J. Schickler, '*We Are All F****d': The Developers of Tornado Cash and the Future of Crypto,* in *Coindesk,* 5th of December 2022, https://www.coindesk.com/consensus-magazine/2022/12/05/alexey-pertsev-most-influential-2022/

Schmahl, A. – Mohottala, S. – Burchardi, K. – Egloff, C. – Govers, J. – Chan, T. - Giakoumelos, M., *Resolving the Blockchain Paradox in Transportation and Logistics*, Boston Consulting Group, 2019, available at https://www.bcg.com/it-it/publications/2019/resolving-blockchain-paradox-transportation-logistics.aspx

Sun, M., *Removing Sanctions on Crypto Mixer Tornado Cash Won't Be Easy,* in *The Wall Street Journal,* 27th October 2022, https://www.wsj.com/articles/removing-sanctions-on-crypto-mixer-tornado-cash-wont-be-easy-11666891513

United Nations Office on Drugs and Crime, *Money Laundering,* https://www.unodc.org/unodc/en/money-laundering/overview.html

United States Department of Justice, *Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars*, 6th May 2006, https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars

United States Department of Treasury, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,* Press Release, 8th of August 2022, https://home.treasury.gov/news/press-releases/jy0916

Vigna, P., *Who Is Bitcoin Creator Satoshi Nakamoto? What We Know—and Don't Know,* in *Wall Street Journal,* 7 December 2021, https://www.wsj.com/articles/who-is-bitcoin-creator-satoshi-nakamoto-what-we-knowand-dont-know-11638020231

Wagstaff, J., *Mt. Gox bitcoin debacle: huge heist or sloppy glitch?,* in *Reuters,* 28 February 2014, https://www.reuters.com/article/bitcoin-mtgox-heist-idUSL3N0LX2SP20140228

Wintermeyer, L., *Bitcoin's Energy Consumption Is A Highly Charged Debate – Who's Right?,* in *Forbes,* 10th May 2021, https://www.forbes.com/sites/lawrencewintermeyer/2021/03/10/bitcoins-energy-consumption-is-a-highly-charged-debate--whos-right/?sh=756343e87e78

## Reports

Banca d'Italia, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività,* Rome, 2022

Bank of England, *Central Bank Digital Currency Opportunities, challenges and design,* London, 2020

Bank of England, *Financial Stability in Focus: Cryptoassets and decentralised finance*, London, 2022

Chainalysis, *The 2022 Cryptocrime Report*, February 2022

Committee on Homeland Security and Governmental Affairs, *Beyond Silk Road: potential risks, threats, and promises of virtual currencies*, Washington, 2013

Department of Finance Canada, *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada,* March 2023

Elliptic, *Financial Crime Typologies in cryptoassets. The concise guide for Compliance Leaders,* London, 2020

EU Blockchain Observatory and Forum, *Demystifying Non-fungible Tokens (NFTs)*, 2021

European Banking Authority, *Opinion on "Virtual Currencies",* Paris, 2014

European Banking Authority*, Report with Advice for the European Commission on Crypto-assets*, Paris, 2019

European Banking Authority, *EBA Report on the future of AML/CFT Framework in the EU*, Paris, 2020

European Banking Authority, *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* Paris, 2021

European Banking Authority, *Opinion of the European Banking Authority on 'de-risking',* Paris, 2022

European Banking Authority, *Opinion of the European Banking Authority on money laundering and terrorist financing risks affecting the EU's financial sector*, Paris, 2023

European Banking Authority, *Consultation Paper Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849,* Paris, 2023

European Central Bank Crypto-assets Task Force, *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures*, Occasional Paper series no. 223, 2019

European Central Bank, *Opinion of the European Central Bank on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, 16 February 2022

European Commission, *Report from the Commission on the assessment of recent alleged money laundering cases involving EU credit institutions, (COM/2019/373 final*), 2019

European Commission, *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (C/2020/2800), OJ C 164*, 2020

European Commission, *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities,* COM(2022), 27th October 2022

European Commission, *Commission Staff Working Document Accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, SWD(2022), 27th October 2022

European Insurance and Occupational Pensions Authority, *Discussion paper on blockchain and smart contracts in insurance,* Luxembourg, 2021

European Parliament, *Report - A9-0052/2022 on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937*, 17 March 2022

European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets*, 6th of April 2022, Rapporteurs: Ernest Urtasun, Assita Kanko

Europol, *Internet Organized Crime Threat Assessment,* 2020

Europol, *Policing in the Metaverse. What law enforcement needs to know,* 2022

Financial Stability Board, *Regulation, Supervision and Oversight of" Global Stablecoin" Arrangements: Final Report and High-Level Recommendations,* 2020

FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, 9th of May 2019

International Monetary Fund, *Regulatory Frameworks For Hawala and Other Remittance Systems,* Washington D.C., 2005

IMF Staff, *Casting Light on Central Bank Digital Currency,* International Monetary Fund, Washington, 2018

Norges Bank, *Central Bank Digital Currencies,* 1, 2021

OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, Paris, 2022

Security and Exchange Commission, *Release No. 81207 / July 25, 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Washington, 201

The law society, *Blockchain: Legal and regulatory guidance. Third Edition,* London, 2023

The White House, *Technical evaluation for a U.S. Central Bank digital currency system,* Washington, 2022

TRM Labs, *Compliance in the second age of digital assets: How crypto compliance programs are evolving in 2023*, 2023

US Congressional Research Service, *Non-fungible Tokens (NFTs)*, Washington, 2022

US Department of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, April 2023

World Economic Forum, *Decentralized Finance (DeFi) Policymaker Toolkit*, White Paper, 2021

World Economic Forum, *Pathways to the Regulation of Crypto-Assets: A Global Approach,* White Paper, 2023

## Legislation

Council of Europe, *Criminal Law Convention on Corruption*, 27th January 1999

Directive of the European Union, 16th September 2009, n. 110

Directive of the European Union, 20th May 2015, n. 849

Directive of the European Union, 27th of April 2016 n. 680

Directive of the European Union, 25th November of 2016, n. 2366

Directive of the European Union, 30th May 2018, n. 843

Directive of the European Union, 23rd October 2018, n. 1673

European Parliament, *Amendments 503 – 838 Markets in Crypto-assets, and amending Directive (EU) 2019/1937 2020/0265(COD),* 3rd of June 2021

Financial Action Task Force, *The forty recommendation of the financial action task force on money laundering,* Paris, 1990

Financial Action Task Force, *FATF IX Special Recommendations*, Paris, 2001

Financial Action Task Force, *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations,* Paris, 2012

Financial Action Task Force, *Virtual Currencies. Key definitions and potential AML/CFT risks*, Paris, 2014

Financial Action Task Force, *Guidance for a risk-based approach. Virtual Currencies,* Paris, 2015

Financial Action Task Force, *Concealment of Beneficial Ownership,* Paris, 2018

Financial Action Task Force, *Guidance for a risk-based approach. Virtual assets and virtual asset service providers,* Paris, 2019

Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Paris, 2020

Financial Action Task Force, *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, Paris, 2020

Financial Action Task Force, *Updated Guidance for a risk based approach to Virtual Assets and Virtual Asset Service Providers,* Paris, 2021

Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets/VASPs*, Paris, 2021

Financial Action Task Force, *Targeted update on implementation of the FATF standards on virtual assets and virtual asset,* Parigi, 2022

G7/8 Summits, Economic Declaration, Paris, 16th July 1989

OECD, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*, 17th December 1997

Proposal for a Regulation of the European Union, 21st of April 2021, n. 0106

Proposal for a Regulation of the European Union, 20th of July 2021, n. 0241.

Proposal for a Regulation of the European Union, 20th of July 2021, n. 0239.

Proposal for a Directive of the European Union, 20th of July 2021, n. 0250

Regulation of the European Union, 27th of April 2016, n. 679

Regulation of the European Union, 14th June 2017, n. 1129

Regulation of the European Union, 31sr May 2023, n. 1113

Regulation of the European Union, 31st May 2023, n. 1114

United Nations, *UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, Vienna, 1988

United Nations, *United Nations Convention against Transnational Organized Crime and the Protocols Thereto,* 15 November 2000

United Nations, *United Nations Convention against Corruption,* 31st October 2003