Alma Mater Studiorum – Università di Bologna
in cotutela con **Universitat Autònoma de Barcelona**
e **Katholieke Universiteit Leuven**

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo XXXV

Settore Concorsuale: 12/H3 - FILOSOFIA DEL DIRITTO
Settore Scientifico Disciplinare: IUS/20 - FILOSOFIA DEL DIRITTO

DISTRIBUTED LEDGER TECHNOLOGIES BETWEEN ANONYMITY AND TRANSPARENCY: AML/CFT REGULATION OF CRYPTOCURRENCY ECOSYSTEMS IN THE EU

Presentata da: Nadia Pocher

Coordinatore Dottorato
Monica Palmirani

Supervisore
Carles Górriz López

Co-Supervisore
Anton Vedder

Co-Supervisore
Monica Palmirani

Esame finale anno 2023

Abstract

The advent of Bitcoin suggested a disintermediated economy in which Internet users can take part directly. The conceptual disruption brought about by this Internet of Money (IoM) mirrors the cross-industry impacts of blockchain and distributed ledger technologies (DLTs). While related instances of non-centralisation thwart the regulatory efforts to establish accountability, in the financial domain further challenges arise from the presence in the IoM of two seemingly opposing traits: anonymity and transparency. Indeed, DLTs are often described as architecturally transparent, but the perceived level of anonymity of cryptocurrency transfers fuels fears of illicit exploitation. This is a primary concern for the framework to prevent the misuse of the financial system for money laundering and the financing of terrorism and proliferation (AML/CFT/CPF), and a top priority both globally and at the European Union level.

Nevertheless, the anonymous and transparent features of the IoM are far from clear-cut, and the same is true for its levels of disintermediation and non-centralisation. Almost fifteen years after the first Bitcoin transaction, the IoM today comprises a diverse set of socio-technical ecosystems. Building on a preliminary analysis of their phenomenology, this dissertation shows how there is more to their traits of anonymity and transparency than it may seem, and how these features range across a broad spectrum of combinations and degrees. In this context, given implemented trade-offs can be evaluated by referring to techno-legal benchmarks, to be established through socio-technical assessments grounded on teleological interpretation. Valuable insights are drawn to this end from the various models of central bank digital currency.

Against this backdrop, this work provides framework-level recommendations for the EU to respond to the two-fold nature of the IoM legitimately and effectively. The methodology cherishes the mutual interaction between regulation and technology when drafting regulation whose compliance can be eased by design. Consistently, it presents the idea of creating a transposition model between red flag indicators and techno-regulatory standards, informed by a preliminary risk-based taxonomy of the trade-offs displayed by IoM ecosystems. It suggests its implementation should be informed by an institutionalised and multi-stakeholder model of co-regulation, known in the literature as polycentric. This approach mitigates the risk of overfitting in a fast-changing environment, while acknowledging specificities in compliance with the risk-based approach that sits at the core of the AML/CFT/CPF regime.

Acknowledgments

I could not have completed this research without the continuing support of my main supervisor, Prof. Carles Górriz of the Autonomous University of Barcelona (UAB). I warmly thank him not only for his helpful guidance, but also for constantly reminding me of the human side of this journey. I am extremely grateful to Prof. Monica Palmirani of the University of Bologna, for co-supervising my work and for her enormous effort in coordinating the Law, Science and Technology Joint Doctorate – Rights of the Internet of Everything, funded under the Marie Skłodowska-Curie Actions ITN EJD GA No 814177 EU H2020. Special thanks also go to my co-supervisor Prof. Anton Vedder and Mrs. Shuki Tang of the KU Leuven – CiTiP, for their help in organising my stay in Belgium, and to Dr. Mario Macías of the UAB's Institute of Law and Technology, for his kind and precious assistance in navigating bureaucracy.

Over the past years, I discovered how inspiring the interplays between law and technology can be and how much focusing on these fascinating issues fulfils me. This interdisciplinary PhD challenge would not have been as exciting without the opportunity of collaborating with, and learning from, brilliant and future-oriented experts. Above all, my gratitude goes to Prof. Andreas Veneris of the University of Toronto and my friend and colleague Mirko Zichichi. Not only they allowed me to benefit from their competence, but they also showed me how to be a better researcher by firmly believing in our work. I would like to express my sincere thanks to Prof. Stefano Ferretti of the University of Urbino for sharing his expertise on enticing topics, and to Daria Kocher and Gabriela Zilkha of Bequant for their support before and during the internship. I am also truly grateful to the reviewers and the members of my defence committee, for their constructive feedback to help improve my current and future work.

A considerable amount of courage and resilience was needed to start and continue this endeavour. A lot of determination is required to plan the next steps of my personal and professional journey. Nothing would have been, nor would be, the same without the affection and encouragement of a few amazing people. As usual in life, some of them came and went, but my special thanks go to those who decided to stay. Words cannot express my gratitude to my family, friends and loved ones – they know who they are and how much they mean to me, but I will make sure to remind them –, for evolving through life with me and for being the brightest part of my days. Finally, a special thanks goes to my PhD colleagues, especially to those that became friends, for their invaluable advice and for sharing this complex experience with me.

"*Curiosity will conquer fear even more than bravery will.*" – James Stephens

Table of Contents

List of Acronyms

AEC	Anonymity Enhanced Currency
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Authority
AMLD	Anti-Money Laundering Directive
AMLR	Anti-Money Laundering Regulation
BIS	Bank for International Settlements
BCBS	Basel Committee on Banking Supervision
BSA	Bank Secrecy Act
CASP	Crypto-Asset Service Provider
CBDC	Central Bank Digital Currency
CEX	Centralised Exchange
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CIoT	Consumer Internet of Things
CJEU	Court of Justice of the European Union
CPF	Countering the Financing of Proliferation
CPMI	Committee on Payments and Markets Infrastructure
CT	Confidential Transactions
DeFi	Decentralised Finance
DEX	Decentralised Exchange
DLT	Distributed Ledger Technology
DNFBP	Designated Non-Financial Businesses and Professions
EBA	European Banking Authority

EC	European Commission
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
EMD	Electronic Money Directive
EMD2	Electronic Money Directive 2
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
FTR	Fund Transfers Regulation
GAT	Graph Attention Network
GCN	Graph Convolutional Network
GDPR	General Data Protection Regulation
I2P	Invisible Internet Project
IASB	International Accounting Standards Board
ICO	Initial Coin Offering
IMF	International Monetary Fund
IoM	Internet of Money
IOSCO	International Organisation of Securities Commissions
IoT	Internet of Things
IoV	Internet of Value
IP	Internet Protocol
ISO	International Standardisation Organisation
ITIN	International Token Identification Number
ITS	Implementing Technical Standard

ITSA	International Token Standardisation Association
ITU	International Telecommunication Union
KYC	Know Your Customer
LEA	Law Enforcement Agency
LEI	Legal Entity Identifier
M2M	Machine to Machine
ML	Money Laundering
MSB	Money Service Business
NFT	Non-Fungible Tokens
OFAC	Office of Foreign Assets Control
OSINT	Open-Source Intelligence
OSP	Online Service Provider
P2P	Peer to Peer
PCN	Payment Channel Network
PET	Privacy Enhancing Technology
PF	Proliferation Financing
PoC	Proof of Concept
PoS	Proof of Stake
PoW	Proof of Work
PPP	Public-Private Partnership
PSD	Payment Services Directive
PSD2	Payment Services Directive 2
PSP	Payment Services Provider
RBA	Risk Based Approach
RTS	Regulatory Technical Standard
SAR	Suspicious Activity Report
SRA	Supranational Risk Assessment

SSM	Single Supervisory Mechanism
STR	Suspicious Transaction Report
STS	Socio-Technical System
TEU	Treaty on the European Union
TF	Terrorism Financing
TFEU	Treaty on the Functioning of the European Union
TOR	The Onion Router
TT	Trustworthy Technologies
TTF	Token Taxonomy Framework
TTI	Token Taxonomy Initiative
TXID	Transaction ID
UN	United Nations
UTXO	Unspent Transaction Output
VA	Virtual Assets
VASP	Virtual Asset Service Provider
VC	Virtual Currency
VPN	Virtual Private Network
WMD	Weapons of Mass Destruction
XML	Extensible Markup Language
ZKP	Zero Knowledge Proof
ZK-SNARK	Zero Knowledge Succinct Non-Interactive Argument

Introduction

"*Blockchains' future will probably lie somewhere between the utopian and dystopian extremes of hope and fear that are currently formulated. Where exactly is up to us to delineate. Technology is in itself "neither good nor bad; nor is it neutral". Rather, it is what those who control it manipulate it to be*".
Finck M (2019a), citing Kranzberg M (1986)

0.1. Introductory Remarks

The genesis block of the Bitcoin blockchain, mined in January 2009, marked a decisive change in the way monetary transactions are envisioned. Building on years of research in distributed systems and cryptography, the Bitcoin whitepaper suggested not only new mechanisms to handle the drawbacks of traditional payment means, but also seemingly safe alternatives to intermediation. The consequent "blockchain hype" inspired the idea of an alternative global economy to which Internet users can take part directly thanks to an economic layer embedded into the web. This disintermediated exchange of value on distributed ledgers was made possible by peer-to-peer (P2P) transfers and by the creation of digital representations of (physical or non-physical) assets or rights, the so-called tokenisation.

When compared to the level of intermediation of the traditional financial system, this setup shows a conceptual disruption. Hence, it is not surprising that the advent of blockchain and distributed ledger technologies (DLTs) had global repercussions that are challenging to grasp in their entirety. Blockchain-based solutions are now deployed in a vast range of industries, but the seeds of this revolutionary wave were first sown in the financial world. In this context, the term Internet of Money (IoM) was coined to label the interplay between individuals and disintermediated monetary transactions. Meanwhile, the concept of *ledger transparency* as implemented in Bitcoin informed the public perception of these solutions, generating the (debated) opinion that a public display of transactions can replace the need to trust a third-party.

Despite their fascination, these concepts cause significant legal problems. Indeed, while the non-centralised nature of (many of) these networks played a key role in supporting the socio-economic claims that accompanied their uptake, it troubles regulatory frameworks as they need to pinpoint accountable entities for compliance purposes. Although the development of the IoM

shows how these ecosystems do not always mirror the traditional image of a DLT-based monetary system, also in terms of *ledger transparency*, the supposed impossibility to reach (some of) them by regulatory and supervisory means generated considerable controversies. In particular, their perceived level of *anonymity* and ubiquity fuels fears of exploitation for borderless illicit transactions. Indeed, the debate on the legal consequences of *anonymity* in online communication intensified when the *anonymous* exchange of information started to have a financial content. Meanwhile, several scandals linking cryptocurrencies to darknet markets spurred the exploration of advanced forensic techniques to trace these funds.

Nowadays, the IoM comprises an enigmatic set of ecosystems whose traits of *anonymity* and *transparency* range across a broad spectrum of combinations and degrees. Hence, pressing regulatory questions are generated by the consequent twofold nature of cryptocurrency transactions. These fears are related primarily to the regulatory framework to prevent the misuse of the financial system for purposes of money laundering and financing of terrorism and proliferation (AML/CFT/CPF). The final goal of these measures is to prevent criminals from enjoying the profit of illicit activities, thwarting their capacity to disguise the origin of funds and provide them with a legitimate appearance, and from financing terrorist activities or the proliferation of weapons of mass destruction. The domain is overseen by the Financial Action Task Force (FATF), in its function of international standard setter. Its Recommendations have been transposed at the European Union level through a process of harmonisation started in 1991 and climaxed with the 2021 proposal to establish a directly applicable rulebook.

The AML/CFT/CPF framework relies on a set of regulated entities to implement preventive measures and to monitor financial transactions to timely report suspicions of illicit activities to the authorities. Inherently, their oversight on activities assumes a condition of *financial transparency*, where specific actors can access certain information to perform compliance and/or supervisory checks. Nonetheless, the nature of this regime as intermediary-based seems inadequate to confront the issues arising in the IoM, and recent controversies in this ever-evolving field have displayed possible inadequacies. To mitigate the current pitfalls in the AML/CFT/CPF approach to cryptocurrency transactions, new methodological and compliance approaches are investigated. The most promising methods are grounded on a proactive use of technological solutions and on innovative interpretations of the interplay between regulation and technology.

At the same time, the IoM has witnessed a consistent growth of industry-led stablecoin initiatives, where the price volatility inherent to traditional cryptocurrencies is managed by tying the coin value to a reference asset. Furthermore, over recent years public and private stakeholders have been experimenting with the design of sovereign digital money, to be used

for retail transactions or restricted to wholesale scenarios between financial institutions. The various models of Central Bank Digital Currency (CBDC) spurred debates on their regulatory repercussions, chiefly in terms of user privacy, security and fight against illicit misuse. The worldwide interest in these initiatives provides insights into the elements to be considered when addressing the relationship between regulation and the design of digital currency ecosystems.

Against this multi-faceted backdrop, this work addresses the following research question: *In the cryptocurrency ecosystems forming the Internet of Money, anonymity and transparency purportedly coexist in ever-evolving combinations and to varying degrees. How can the EU regulatory framework to prevent the misuse of the financial system for purposes of money laundering and terrorist and proliferation (AML/CFT/CPF) legitimately and effectively respond to the consequent two-fold nature of payment-type cryptoassets – i.e., cryptocurrencies?*

0.2. Notes on Methodology

The ultimate goal of this dissertation is to provide EU-level regulatory recommendations to address the challenges posed in the AML/CFT/CPF field by IoM monetary applications – *i.e.*, cryptocurrencies. In this respect, the methodological foundation of this work pursues the mitigation of the risk of (regulatory) overfitting in a fast-changing environment, while acknowledging specificities in compliance with a key element of the AML/CFT/CPF regime, the risk-based approach (RBA), pivoting on tuning compliance measures to the principle of proportionality. As the reader may notice, the title of this work bears reference to AML/CFT, while the remainder of the dissertation refers comprehensively to AML/CFT/CPF, except for references to EU provisions. This falls in line with the current stance of EU law, since the extension of AML/CFT/CPF measures to the fight against the financing of proliferation of weapons of mass destruction, introduced by the FATF in 2008 and more frequently referred to starting from 2021,[1] is yet to be added explicitly to the titles of legislative and policy documents.[2]

0.2.1. Scope definition

In this research, I explore the challenges posed for the integrity of the financial system by the janiform nature of the IoM as both *anonymity*- and *transparency*-oriented. Accordingly, in

[1] Financial Action Task Force (2021b)
[2] However, the proposed AML Regulation put forward in 2021 as part of the AML Package, described in Chapter 4, would introduce requirements to include CPF in the scope of the regime (Articles 7 and 8 AMLR proposal).

the preliminary phase of this work I singled out two intertwined elements as the components of its scope: a specific regulatory domain and a specific category of cryptoassets. From the first perspective, the addressed regulatory area is the EU-level AML/CFT/CPF framework, while considering its interplay with global standardisation. Although the regime features interactions with the privacy and data protection regime – notably, the General Data Protection Regulation (GDPR) framework in the EU –, and the two often seem to display opposing requirements, a comprehensive analysis of the interplay falls outside the scope of this research. Accordingly, the methodological standpoint is not one of privacy and data protection. Similarly, beside contextual remarks, this work is not focused on tax law, criminal law or criminal procedure.

From the second perspective, among the existing types of cryptoassets the scope of this dissertation is explicitly limited to the category labelled as *payment-type* cryptoassets – *i.e.*, cryptocurrencies. The latter are the sub-type of cryptoassets known as *payment-type* or *exchange-type*. The respective tokens are labelled *payment tokens – i.e.*, the architectural representation of *payment-type* cryptoassets –, meant to be used as a means of payment or exchange for goods and services, in principle external to the DLT where the tokens are issued and transferred. Chapter 1 provides further information on related terminological choices.

It is important to point out that there is no universal definition of the Internet of Money. While the term is generally used to depict the cryptocurrency sphere as the realm of pure monetary disintermediation, an idea debated and challenged in this work, this concept allows these ecosystems to be referred to in a way that is conceptually flexible, without resorting to technology-based definitions. Accordingly, as outlined extensively in the phenomenological analysis provided in Chapter 1, in this dissertation I interpret the concept of IoM broadly. It follows that for the sake of the narrative the terms "IoM ecosystems" and "cryptocurrency ecosystems" are used as synonyms when no specification is provided. At the same time, the extent to which I consider CBDCs as part of the IoM, and the limits of this equation, are outlined when relevant.

0.2.2. Legal research and cross-disciplinary approaches

While the final objectives of this research are recommendatory – *i.e.*, put forward framework-level regulatory suggestions –, the intermediary steps feature methods that are descriptive, classifying and evaluative.[3] These goals are pursued by dividing the analysis into different

[3] Kestemont L (2018) clarifies that "the different types of research objectives that legal scholars can pursue in their research: descriptive, classifying, comparative, theory-building, explanatory, evaluative and recommendatory" (Ibid, p 7). In particular, a *descriptive* research objective "will systematically analyze legal constructs in all

chapters with different, albeit ultimately convergent, methodological approaches. The main reason lies in the concurrent presence of legal, technical and socio-economic aspects, which need to be scrutinised in a way that can reflect their specificities while safeguarding the consistency of the legal structure of the work. Hence, relevant methodologies range from deductive (starting from regulatory provisions and policy documents), to inductive (starting from phenomenology), to abductive reasoning,[4] as specified below.

Firstly, as with any legal research a preliminary part of this work pursues a descriptive objective. Notably, the description angle is evaluative and classifying, to provide framework-level regulatory recommendations – *i.e.*, the analysis of AML/CFT/CPF rules in this work aims to evaluate their suitability to the IoM landscape and the socio-technical features of cryptocurrency ecosystems.[5] In particular, the description of the interplay of global financial regulation and AML/CFT/CPF complies with the need to perform a systematic interpretation for the sake of compliance with EU and international law. Accordingly, the parts of the dissertation oriented towards analysing the state of the art are methodologically based on a comparative documentary analysis of systems of values and concepts primarily enshrined by EU legal sources and policy instruments, in conjunction with international guidelines and Member State-level transposition and implementation of legal, regulatory, and operational measures.[6] They involved

---

their components in order to present them in an accurate, significant and orderly manner" (Ibid, p 19), a *classifying* research objective "aims to conceptualise or classify (legal) phenomena in the existing legal system" (Ibid, p 33), an *evaluative* research objective "aims to evaluate/assess legal constructs in view of a norm" (Ibid, p 60), and a *recommendatory* research objective "aims to formulate recommendations on how the law *should* be" (Ibid, p 63).

[4] To summarise the essence of these types of reasoning, mainly defined in philosophy, *deductive reasoning* equals to drawing deductive inferences, *inductive reasoning* derives general principles from specific observations, *abductive reasoning* is a type of logical inference that starts from observation and infers the most likely (*i.e.*, probable) conclusion. The meaning of abduction is debated: "some regard it as a variety of inductive reasoning, some regard it as a variety of deductive reasoning, and others claim that it is a potpourri of both deduction and induction. Some claim that it has to do with inference to the best explanation" (Abimbola K (2001), p 1684). Reportedly, the claim to have the "best" explanation is difficult to prove in real life, and legal scholars explored the value to understand "abduction as inference to the best viable (actual) explanation" (Ibid, p 1689). When I deploy abduction in this work the evaluative benchmarks are primarily legitimacy and effectiveness of EU regulatory actions, but also concepts and principles identified as pivotal in the research domain – *e.g.*, RBA, avoidance of overfitting.

[5] The notions used to provide methodological details on this work – *e.g.*, methodological features of the different objectives of legal research, description angles – were put forward by Kestemont L (2018).

[6] Despite building on a selection of resources that are at times jurisdiction specific, this work does not feature a comparative research objective – *i.e.*, one that "aims to compare two or more legal constructs in order to uncover their similarities and differences" (Kestemont (2018), p 12). This choice depends on the level of the investigation, that is explicitly: (a) targeting, for what concerns the dogmatic analysis, international standards and EU initiatives (please see chapter 4), (b) anchored to the interplay of socio-technical aspects of cryptocurrency ecosystems and AML/CFT/CPF provisions, (c) set to provide EU-level recommendations in terms of regulatory methodology. The comparative endeavor is fascinating and all-absorbing in an ever-evolving domain, especially when a primary goal is to avoid overfitting, as specified below. Due to the presence of *descriptive*, *classifying*, *evaluative* and *recommendatory* research objectives and of a strong cross-disciplinary imprint, adding a further layer of methodological complexity to the structure of the thesis would have threatened its internal consistency. However, its conceptual context is grounded on the knowledge of the relevant regulatory evolution, and developments from a

collecting present and historical information from publications issued by private and public entities. Accordingly, these parts mainly feature a deductive approach. Relatedly, all sections of this work are confronted with information technology, albeit they are still placed within the setting of legal arguments. They draw from both doctrinal and empirical analyses. They involved documentary research based on diverse legal, policy and technical sources, whose study focused both on quantitative and qualitative aspects, and they feature an inductive approach to impacts on principles and systems of values. They also feature a descriptive approach.

Secondly, in pursuing the formulation of framework recommendations, I deployed classifying and evaluative methods. This means the varied phenomenology of cryptocurrency transfers and the different interplays with the AML/CFT/CPF scheme are scrutinised to understand the effectiveness and legitimacy of EU regulation in various circumstances – *e.g.*, taxonomy of *anonymity-transparency* trade-offs, classification of the regulatory impacts of different applications into *dark box*, *recycle box* or *sandbox* categories in Chapter 6. In particular, the sections that elaborate on the conceptualisation of multi-layered findings draw from a deductive approach but are based on inductive and abductive reasoning, from both a normative and a non-normative perspective. Inherently, they also take an evaluative stance – *e.g.*, in tackling issues of legitimacy and effectiveness of the different (levels of) regulatory intervention in the IoM landscape. The normative criteria used in this work are both internal – *e.g.*, analysis of EU AML/CFT/CPF provisions in the context of the global financial system – and, as typical in interdisciplinary legal research, external – *e.g.*, effectiveness vis-à-vis the evolving phenomenology of the IoM. Notwithstanding a theoretical imprint, abductive reasoning is used, as a pragmatical standpoint is pivotal in tackling the complexities of the issues at hand.

Notwithstanding the foundational role of multi-disciplinary concepts, this dissertation remains primarily a legal work. Hence, technical and socio-economic aspects are explored within the framework of a legally oriented reasoning, to the extent they can inform legal considerations from both a normative and a non-normative standpoint. Notably, to determine whether the current regulatory approach is tailored to the specifics of the evolving phenomenology of the IoM, a domain inherently shaped by technology but whose development has a mutual relationship with socio-economic elements. Hence, the structure of this work does not deploy sociological, economic and financial methodologies, nor it follows a criminological method when analysing ML/TF/PF phenomena. Whenever a specific section draws from a previous

comparative perspective have been closely monitored. They were mentioned only when relevant to the research question, while other instances are addressed in other outputs (*e.g.*, project deliverable, past/ongoing publications).

publication by the author of the dissertation, the content of which may be primarily technical, the reader will be made aware of this through a reference at the beginning of the chapter.

Relatedly, it is worth clarifying that when the term "regulation" is used in this dissertation with no further specification, it refers in a comprehensive fashion to a significant array of legal sources – *i.e.*, legislation, regulation, standards, soft law, self-regulatory initiatives, caselaw – and to their interplay.[7] This choice does not mean to dismiss the differences among legislative and regulatory methodologies, which are indeed analysed separately in different parts of this dissertation and inform the recommendations provided in the final remarks. On the contrary, it aims to keep the narrative anchored to the multi-layered compound of AML/CFT/CPF rules that exert effect on regulated entities. Further, it encompasses various types of approaches in the scope of the analysis – *e.g.*, EU legislation, domestic legislation, soft law, EU standards, international standards – as outlined in Chapters 4 and 6. In this sense, "regulation" was broadly interpreted as "the process of writing the rules that apply to the regulated entities",[8] hence referring also to the resulting compound of rules applicable to AML/CFT/CPF regulated entities.[9]

0.2.3. Conceptual context and terminology

The techno-regulatory domain addressed by this research contains terminological and conceptual conundrums, and often a mutually reinforcing combination thereof. Hence, each chapter focuses on specific notions for the purpose of disambiguating them. Because many concepts crucial to the narrative of this dissertation are currently lacking universally agreed-upon definitions, it is not possible to delve into them without clarifying the terminology. Otherwise, the ultimate risk is to regulate "by streetlight" – *i.e.*, on the basis of what can be easily seen or

[7] When the term "regulation" is used to refer to the specific EU legislative act, the reference will be explicit.
[8] Auer R (2022), p 2
[9] To avoid over-simplifications that could be averted only by a thorough and specific analysis, this paragraph does not mean to take a stand on the controversial definition of what is "regulation". For the interested reader, valuable insights are offered by Bennett C, Raab C (2020), Black J (2002), Black J (2012), Finck M (2019a), Hofmann J, Katzenbach C, Gollatz K (2017), Kosti N, Levi-Faur D, Mor G (2019), Marsden C (2008), Pagallo U, Casanovas P, Madelin R (2019), among others. Although the task of defining "regulation", except for pinpointed aspects, goes beyond the scope of this work, the latter cherishes the nuances underlying the concept and the compound and multi-layered essence of AML/CFT/CPF rules. These elements are addressed extensively in Chapters 4, 6 and in the concluding remarks, focusing on current and prospective solutions (*e.g.*, in relation to models of co-regulation and self-regulation). Nevertheless, the need to elaborate on and/or refer to their complexity depends on the type of analysis conducted in the different sections. In particular, I argue it is possible to speak of "compliance with all relevant provisions" without claiming implicitly they have the same qualification, exert the same effects, are enforced in the same way and by the same actors. Evidently, this reasoning implies a process of abstraction that must be performed carefully in a legal doctoral dissertation. Accordingly, for the narrative's sake and to ease cross-disciplinary communication, when I considered their qualification bore no relevance to the given argument, I used the term "regulation" – *e.g.*, not "law and regulation" – in an inclusive fashion. Since the compound facets of legal terminology are not to be overlooked, to avert misunderstandings I add this specification.

(mis)understood –,[10] but also to incorporate common misconceptions into regulatory frameworks. Namely, in this work there are (a) terms strictly related to the investigated topics, that assume a particular connotation because of the context: *e.g.*, Internet of Money, *non-centralisation*, *disintermediation*; and (b) notions that do not exclusively pertain to this research area but must be contextualised to avoid ambiguities: *e.g.*, *anonymity, transparency.*

Meanwhile, several foundations of this research warrant, within these introductory considerations, the inclusion of preliminary clarifications. This is due to their cross-disciplinary nature – *i.e.*, most of them feature specificities that vary across domains – and/or because of the selective understanding made in this dissertation vis-à-vis their complexity. Accordingly, in the remaining part of this section, I describe the methodological traits underpinning this work.

From a first perspective, this work is structured to address the IoM as an ecosystem of DLT-based ecosystems, referring to specificities of (or derived from) these technologies. Indeed, DLTs and blockchain have informed the IoM significantly due to the key role in the origin and the evolution of this sphere. Nonetheless, the IoM is not exclusively DLT-based, and just as blockchains can be implemented in different ways and to different ends, other technologies can be implemented to reach the same or similar results. Hence, for the purposes of this analysis, the understanding of cryptocurrency ecosystems goes beyond DLTs. The reason is not only that not all relevant applications are based on this set of technologies, but also that architectural aspects are just one of the elements to consider, as described below. However, specific references to blockchains and DLTs are made when adequate.

Secondly, this work pivots on the interpretation of IoM ecosystems as "socio-technical systems (STSs)" – thus, of the IoM as an ecosystem of interconnected socio-technical ecosystems –, defined as such because they comprise interdependent human, social, organisational and technical components cooperating to achieve a task.[11] From a regulatory perspective, the value of a "system approach" lies in embracing the elements at play when devising a strategy to approach these ecosystems, thus avoiding reaching conclusions refuted by phenomenology. As outlined in Chapter 1, the literature applies the concept of STSs to domains close to the IoM and the AML/CFT/CPF regime.[12] However, the notion was originally coined in the context of organisational studies and work/enterprise systems. The concept I use in this work is drawn

[10] Walch A (2018), p 25

[11] The group of entities composing an IoM system is called "ecosystem": they belong to one of four areas: (a) hardware (*e.g.*, nodes), (b) business (*e.g.*, developers, users, miners, investors), (c) software development (*e.g.*, financial, semi-financial, non-financial), (d) protocol development (*e.g.*, developers, academia). ITU-T FG DLT (2019b), pp 2-4. This is explored in Chapter 2.

[12] Desmond DB, Lacey D, Salmon P (2019) De Domenico M, Baronchelli A (2019) Poblet M, Allen DWE, Konashevych O, Lane A (2020) Renwick R, Gleasure R (2020)

from the so-called "sociotechnical systems theory/approach", focusing on the holistic and interconnected contribution of technology and the human systems that interact with it.[13] Although there is no consensus on the specifics of what an STS is, the core revolves around the interdependency of humans, machines and context where they interact, and on the related possibility to make design choices. As pointed out in literature, the definition of the suitable level of abstraction when describing STSs is a primary challenge.[14] From this perspective, in this work I do not pursue a comprehensive analysis of the components of the STSs I address, nor do I delve into the possible interplays between the components of the systems from an organisational perspective. When tackling the design of an STS – *e.g.*, of a cryptocurrency ecosystem or of a CBDC model –, I do so through a selective (*i.e.*, teleologically-oriented, as defined below) analysis of the aspects that exert impacts on *anonymity* and on the *privacy-transparency* trade-off of the given ecosystem or proposed design. Notably, I leverage the STS concept to heed the different elements that influence the definitions of IoM features, and exert consequences from a regulatory standpoint, chiefly in terms of AML/CFT/CPF rules and compliance strategies.

Thirdly, in this dissertation one can witness the deployment of a teleologically oriented methodology when disambiguating the notions of *anonymity* and *transparency* in the IoM from an AML/CFT/CPF viewpoint. In other words, the analysis is informed by the specifics of the context, composed by the IoM and the AML/CFT/CPF framework. The concept of "teleological approach" draws from philosophy, ethics, and law. In broad terms, if an approach is *teleological* it means it involves "the explanation of phenomena in terms of the purpose they serve rather than of the cause by which they arise".[15] In scientific literature, an explanation can be described as *teleological* "when it resorts to notions such as ends, goals, purposes, or objectives",[16] and in ethics a *teleological* approach is results-oriented in defining ethical behaviour emphasising outcomes over process.[17] In the legal domain, *teleological* or *purposive* interpretation "interprets a legal provision in view of the legislator's original objective(s): protecting specific interests, obtaining a particular social or economic outcome, stimulating a specific type of behaviour, etc".[18] The value of this approach emerges in EU law from the frequent deployment by the Court of Justice of the European Union (CJEU) to provide an explanation by

[13] Baxter G, Sommerville I (2011), p 5. Relatedly, it was noted that "electronic wallets tied to a complex network of blockchain nodes, cryptocurrency users and miners, exchanges and tumblers/mixers all cooperate within a complex system of social and informational relationships" (Desmond DB, Lacey D, Salmon P (2019), p 487)
[14] Baxter G, Sommerville I (2011), p 8
[15] Oxford Languages Dictionary (2022)
[16] González Galli LM, Meinardi EN (2011)
[17] The Arthur W. Page Center (2022)
[18] Kestemont L (2018), p 28

reference to purposes or goals.[19] To the same end, the CJEU often applies "teleological argumentation".[20] In a broader fashion, in this work I apply a teleological approach both in a context that is not directly legal (but its consequences are), when interpreting the features of IoM ecosystems having regard to the regulatory purpose for which they come into play in this research – *i.e.*, AML/CFT/CPF regulation –, and in a legal scenario when interpreting the details AML/CFT/CPF rules provide about the definitions of those concepts – *e.g.*, *anonymity*, relevant risks.

Fourthly, the structure and content of this work mirrors the need to shape the regulatory approach to the foundational characteristics of the IoM. In other words, the need to strike a balance between a case-specific approach, to acknowledge the existing differences among cryptocurrency ecosystems, and the risk of overfitting – *i.e.*, the risk of rules becoming technologically outdated soon after their entry into force, or even beforehand. This risk manifests itself when rules are over-tailored to the state of evolution of the technology at the time of their conception, which generates a mismatch with later developments. Indeed, this is a recurring issue when regulating new technologies,[21] but it is more pressing in a case like the one addressed by this research: on the one hand the domain is ever-evolving in ways that disrupt both the domain to be regulated and the regulatory framework, and on the other hand the EU-level legislative process – although the same consideration could be raised at the domestic level – is bound to take a considerable amount of time from the start of the initiative to the entry into force of the rules. Because the goal to avoid the risk of overfitting underpins the structure of this work, it is worth noting that regulatory overfitting does not overlap with the concept of overfitting that is commonly used in data science, statistics and mathematics.[22] Nonetheless, from an abstract perspective the two notions express similar considerations.

Fifthly, the regulatory analysis and the framework recommendations are informed by the overarching role of the RBA. This is a common concept in regulatory compliance, deemed conducive to adopting implementation measures in a flexible way. This is especially true when the framework features a certain complexity and a disproportionate deployment of the same approach in all circumstances would overburden the stakeholders involved and originate a considerable inefficiency. In the AML/CFT/CPF sphere, both authorities and regulated entities can optimise the use of their resources if they adopt supervisory methods and preventive measures,

[19] "A goal is an extralegal element such as needs, interests and values, which are also considered an object of teleological argumentation" (Kuch P (2022), p 2)
[20] Because every legal provision has a goal, "among its possible meanings, the most significant one is why it has been adopted in the first place (its purpose)" (Ibid, pp 3-4)
[21] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), p 33
[22] In mathematics and data science, an overfitting model fits too closely to a dataset (*e.g.*, a machine learning model fits too closely to its training data) and is not reliable when applied to other contexts.

respectively, in a way that is commensurate to the nature of the different risks. From a domestic perspective, when authorities identify higher risks, they must make sure they are adequately addressed with stricter rules within their jurisdiction, while in cases of lower risk simplified measures can be allowed. For regulated entities, internal controls and procedures, but also everyday activities, must mirror the preliminary risk assessment and the risks identified in the concrete compliance exercise in a proportionate manner – *i.e.*, in brief, the identification of higher risks must originate enhanced controls and monitoring, up to the decision to discontinue (or not engage in) a given activity. The matter is detailed in Chapter 4.

Sixthly, a pillar of this dissertation is the possibility to conceive regulation "by design" by focusing on the interplay of legal rules and technology, and to embed compliance measures into an application or tool. In recent years, these considerations gave rise to manifold methodological approaches, at times divergent. In brief, they are at the root of design-based regulatory and compliance techniques, which have been labelled as embedded regulation/compliance, regulation/compliance by/through design. These concepts and their variety, as well as the specific approach I take in my work based on a literature review, is outlined in Chapter 6. In broad terms, I conceive this method not in terms of leveraging the opportunities offered by technological design to replace regulatory provisions and their essence, but on the contrary as a specific *techno-regulatory methodology* to think about the mutual interaction between regulation and technology when drafting regulation whose compliance can be eased by design. On the grounds of the outcomes of my research, I argue that the deployment of these strategies, provided given *caveats* are heeded, aids an efficient deployment of the RBA and mitigates the risk of overfitting in the regulatory and phenomenological domains under consideration.

0.3. Structure

The structure of this work is divided into six chapters, followed by concluding remarks. Notwithstanding the considerations outlined above, the introductory part of every chapter expands on the specifics of the methodological imprint of the different sections. The goal is to guide the reader through different topics and a few cross-disciplinary conceptual leaps. Meanwhile, below I outline the main content of the various chapters.

Chapter 1 outlines the phenomenological foundations of the ecosystems that fall into the scope of this research. Accordingly, it introduces key traits of the IoM by exploring its underlying combination of technologies and the role played by various stakeholders and architectures. It outlines the background against which the concepts of IoM and IoV were devised,

starting from P2P transfers and *tokenisation*, up to the advent of stablecoins and CBDCs. It defines the IoM, but also heeds the value of terminological disambiguation for what concerns cryptoassets and tokens. It explores the landscape of cryptocurrency transfers by deploying a teleological and *accountability*-based approach. It underlines the nature of the IoM as an ecosystem of interconnected socio-technical ecosystems, and the need to focus not only on the interplay of their components but also on the developments in terms of *non-centralisation* and *disintermediation*. Finally, it outlines methodology benchmarks to address the IoM from a regulatory perspective while heeding conceptual, ideological, and technical evolutions.

Against this backdrop, Chapter 2 presents the first part of the analysis of the concepts of *anonymity* and *transparency* in the IoM and pursues the conceptual clarity on which to ground the following investigation and the final conclusions. It addresses the role of encryption and the multifold concepts of *anonymity* and *transparency* in the IoM and related transactions, while attempting disambiguation efforts at the crossroads between different conceptual levels pertaining to the cyberspace, IoM ecosystems, financial transactions. It explores the traits featured by *anonymity* and *transparency* within an AML/CFT/CPF context and provides an analysis of several features of IoM *anonymity.* Meanwhile, it addresses the twofold notion of *transparency*, torn by the fact that the concept of *transparency of the ledger* and *ledger operations* is constitutively distant from the notion of *financial transparency.* Accordingly, it reframes the alleged paradox of public blockchains being both *anonymous* and *transparent*. Finally, it addresses *enhanced disintermediation*, showing the impact on *accountability*.

Chapter 3 provides the second part of the analysis of the concepts of *anonymity* and *transparency*, focusing on the socio-technical concepts of *obfuscation* and *traceability.* It heeds the impact of *anonymity*-enhancing strategies applied by different actors, and of investigative transaction analytics tools. It shows how cryptocurrencies can be deployed in the laundering process in multiple ways, and how this hampers identification and categorisation of risks. Relatedly, it focuses on red flag indicators released by the FATF, phrased without a clear separation between the ways in which *anonymity* can be enhanced. The chapter argues for deploying a teleologically oriented methodology when evaluating the meaning of features such as *anonymity – i.e.*, it vouches for the consideration of the context, composed by the IoM and the AML/CFT/CPF framework. Meanwhile, it suggests the identification of specific benchmarks to differentiate between the various degrees of *anonymity* enshrined by different IoM ecosystems without running into the risk of overfitting. It is in this context that the concept of *accountability*, ensured by the *auditability* of relevant transactions, emerges as pivotal.

Chapter 4 investigates the AML/CFT/CPF regulatory context and the evolution of the regime. It provides insights into the perceived IoM-related risks and the (purported) *anonymous* character of the sphere. The chapter heeds the importance of the activity of the FATF as a sector-specific player within the dynamics of global financial regulation, and analyses its Recommendations as instruments of soft-law. Meanwhile, it outlines the main obligations, through the lens of their EU-level implementation, and underlines the importance of the RBA that underpins all duties imposed on regulated entities. Moreover, it analyses selected technical standardisation initiatives on cryptocurrencies, blockchain technologies or DLTs, underlining the interplay between technical and regulatory standards. It expands on the nature of the AML/CFT EU regulatory methodology as minimum harmonisation, while addressing the main initiatives included in the AML Package to overcome fragmentation. Starting from the relationship between EU law and international standards, this chapter addresses the newly proposed authority and its task of drafting RTSs. It displays the problematic application of the intermediary-based approach to the IoM space, vis-à-vis the revolution brought about by DeFi platforms and DEXes also in terms of laundering trends. The matter is exemplified by the difficulty in complying with the crypto travel rule and the impacts of self-hosted wallet-related transfers.

Chapter 5 overviews sovereign digital currencies, heeding a selection of debates on digital fiat money elicited in publications by leading institutions and private actors. CBDC explorations provide a revolutionary insight into cross-disciplinary efforts, while CBDC projects feature various approaches, designs and architectures. The chapter focuses on *interoperability* and *standardisation*, and on the impact of public-private interplays and cross-border models. It explores regulatory issues raised by CBDCs from an AML/CFT/CPF perspective and contextualises the debate within the broader cash-related *anonymity problem* and the establishment of relevant limits. It tackles *privacy* and data protection concerns and the competence for AML/CFT/CPF compliance in different public-private designs. In light of the findings of the other chapters, it introduces the existing trade-offs between *anonymity* and *transparency* in CBDCs, whose designs can embed various balances between *confidentiality* and *auditability*. It underlines the interplay between technology, regulation, and standardisation, to provide preliminary benchmarks for thinking about *anonymity* and *transparency* in CBDCs.

Chapter 6 explores key aspects of a possible methodology to be applied at the EU level in the AML/CFT/CPF sphere. Chiefly, it heeds the ever-evolving presence of manifold assets, technologies, innovative and traditional stakeholders in IoM socio-technical ecosystems, the approaches put forward to regulate new technologies and their interplay with the AML/CFT/CPF regime. The analysis reviews the types of interplay DLT-based applications can have with

regulatory frameworks, focusing on how *proactive* instances could replace *reactive* approaches. It overviews a set of methodological features of AML/CFT/CPF regulation, tailoring the analysis to *anonymity-transparency* trade-offs. It proposes the creation of a taxonomy instrument to evaluate the levels of *anonymity* risk posed by IoM ecosystems and suggests the creation of a "transposition model" of risk indicators to techno-regulatory standards. It investigates the shift from the criticised "code is law" to a compound concept of "[regulation/compliance]-[by/through]-design" and advocates for the establishment of a multi-stakeholder co-regulatory model. It provides a case study of the proposed approach. Finally, it reviews methodological elements for the intervention of EU law in terms of legitimacy and effectiveness, overviewing its role in the design and implementation of the proposed methodology.

Finally, the concluding remarks mirror the multi-layered approach of the previous sections and pertain to various levels of reasoning, whose combination is the final output of the work. They outline findings concerning: (a) the *anonymity-transparency* trade-offs featured by IoM socio-technical ecosystems, (b) the application of a holistic approach to draft a risk-based taxonomy, (c) the value of establishing an EU-level polycentric techno-regulatory standardisation model, methodologically grounded on (d) "[regulation/compliance]-[by/through]-design".

1. Phenomenology of the Internet of Money: Cryptocurrencies, Architectures, Transactions

"*In all, if you're not careful, the question one poses about cryptoassets quickly becomes the answer, even when you're just grappling with defining what you're trying to study*".
Brummer C (2019)

1.1. Introduction

October 31, 2008, marks a milestone in the history of the Internet and of the global socio-economic development. The publication of the Bitcoin whitepaper by the mysterious Satoshi Nakamoto launched a revolutionary trend in P2P networks and distributed computing, with vast cross-industry repercussions.[23] The design of Bitcoin, and its open-source software Bitcoin Core, included the first blockchain database. Notably, a *blockchain* is a type of distributed ledger where data is recorded in a tamper-proof chain of *blocks* linked cryptographically.[24] For the first time, DLT was leveraged to allow groups of *nodes – i.e.*, network participants – to agree on actions and states with no need of a central trusted authority.[25] After the first bitcoin trade two months after the whitepaper's release, a plethora of cryptoassets followed. They amount today to a number estimated between 10,000 and 20,000.[26]

Although blockchain-based solutions are now deployed in a vast range of industries, the fact that the seeds of this disruptive wave were first sown in the financial world bears relevance to this day. Indeed, even though the field is still largely based on traditional infrastructures, the so-called "blockchain hype" introduced the idea of an alternative economy in which citizens and businesses can participate directly on a collective basis. While the development of the FinTech sector unlocked innovative scenarios, the *tokenisation* of assets has been implemented since 2017 with innovative projects of initial coin offering (ICOs) projects.[27]

[23] Nakamoto S (2008) The source code of Bitcoin was published on that occasion. The term "Bitcoin" refers to the protocol, the concept and the technology, whereas "bitcoin(s)" (with no capitalisation) labels the unit of currency.
[24] ITU-T FG DLT (2019a), pp 1-4. A *distributed ledger* is "shared, replicated, and synchronised in a distributed and decentralised manner", thus control is distributed among those "participating in the operation of system".
[25] Antonopoulos AM (2017a). Antonopoulos AM (2016). A *P2P system* is a "network of peers that directly share information and resources with each other without relying on a central entity" (ITU-T FG DLT (2019a), p 4).
[26] CoinMarketCap (2022). European Central Bank (2022). UK Government (2022)
[27] Arner D et al (2019), p 262. Werbach K (2020), p 4. ICOs are online crowdfunding schemes involving the issuance of digital tokens. The first step is the publication of a whitepaper with the fundamentals of the investment.

The Bitcoin whitepaper is often perceived as embodying the socio-political and techno-economic values of the cyber- and cypher-punk movements, in terms of heralding *anonymity* and people's freedom from authorities and intermediaries. Nevertheless, in contrast to the work of Timothy C. May,[28] explicitly fostering the crypto-anarchist movement, the economic orientation of Nakamoto's whitepaper is controversial. Arguably, it does not refer explicitly to the financial sphere from an ideological perspective, and idioms linked to the economy are absent. From this viewpoint, the work appears scientific in addressing computer security issues.[29] Although the matter is not inconsequential, dwelling on this controversy falls outside the scope of this work. Over the past decade, the evolution of P2P monetary interactions has amounted to much more (and much more complexity) than pursuing anarchist ideas. While there are *anonymity*-enhanced use cases such as Monero, described in Chapter 3, there are also initiatives on stablecoins and CBDCs.[30] Together with the role still played by various types of service providers, this shows the idea of complete *disintermediation* must be contextualised.

1.1.1. From distributed consensus to the Internet of Value

The creator(s) of Bitcoin did not put forward previously unknown concepts, and they virtually introduced no technical advances.[31] The whitepaper is more of a collection of existing ideas and technologies, and it builds on years of research in both distributed systems and cryptography. Its value lies in being the first application of a powerful combination: (i) a *decentralised* P2P protocol;[32] (ii) a public transaction ledger, an append-only and auditable log (*i.e.*, the blockchain); (iii) consensus rules for validating transactions and issuing currency independently; (iv) the proof-of-work (PoW) algorithm to reach *decentralised* consensus on the state of transactions.[33] Additionally, the ecosystem employs encryption in the issuance and in the validation phases, and consent is expressed by network participants through verifiable

[28] May TC (1988). The issue is explored in Chapter 2.
[29] Poblet M, Allen DWE, Konashevych O, Lane A (2020), p 2. Quiniou M (2019), p xii.
[30] CBDCs and stablecoins are addressed in Chapter 4. "Privacy coins" are investigated in Chapter 2.
[31] Werbach K (2020), p 3
[32] A *protocol* is a system of rules describing how a computer "can connect to, participate in, and transmit information over a system or network. These instructions define code syntax and semantics that the system expects. Protocols can involve hardware, software, and plain-language instructions". Dannen C (2017), p 3 referenced by Schrepel T (2021), p 26
[33] Antonopoulos AM (2017a), pp 1-4. Casey M, Crane J, Gensler G et al (2018), p 2. Nakamoto's combination solves two problems of distributed computing: (a) "Byzantine Generals" (a computer system needs to cope with the failure of one or more of its components, which may send conflicting information across the network) and (b) "double-spending" (*i.e.*, a participant manages to spend the same money multiple times. Bitcoin averts it by verifying the inputs of each added transaction).

digital signatures.[34] For the purposes of this analysis, the understanding of cryptocurrency ecosystems goes beyond DLTs. The reason is not only that not all relevant applications are based on this set of technologies, but also that architectural aspects are just one of the elements to consider. The historical role of distributed consensus mechanisms, however, is crucial.

The Bitcoin blockchain is *public* and *permissionless*, as explained below. In principle, in this type of systems participants are "mutually distrusting users that may only know each other by their public addresses", where an *address* is used as an identifier to the entity/entities that are performing activities.[35] In the Bitcoin system, the PoW algorithm incentivises participants to make use of their own processing power to validate transactions through solving cryptographic puzzles, hence becoming *miners*.[36] This is achieved by offering rewards to whoever solves the problem first, where the reward is the validation of a block of outstanding transactions – *i.e.*, the respective transaction fees.[37] In this way, participants reach a consensus over the order of the events recorded in the ledger. Prohibitive computational and operational (*e.g.*, energy-related) costs aim to deter single (groups of) miners to take over the network and subvert it by creating multiple versions of the ledger or tampering with it. The Bitcoin blockchain is watched over by *full-nodes*, and in this way reliance on third parties is replaced by a system of (cryptography-based) supposed "trustless trust".[38] Indeed, if one can legitimately identify the final goal of consensus algorithms in the *decentralisation* of the source of truth – *i.e.*, it is no longer necessary to rely on central authorities to agree on a univocal truth by a unique source of authenticity –,[39] the value of oracles in the blockchain sphere testifies to its limits.[40]

This innovative way of devising interactions is grounded on an understanding of online social dimensions that gave birth to a next generation of Internet compared to the "Internet of

[34] Cryptography is a form of applied mathematics. Here the applied technique is *public-key cryptography* or *asymmetric encryption*, "in which a public key and a corresponding private key are used for encryption and decryption, where public key is disseminated, and private key is known only to the key owner" (ITU-T FG DLT (2019a), p 5). In this way, "users can digitally sign data with their private key, and the resulting signature can be verified by anyone using the corresponding public key", while a *digital signature* consists of "data appended to data units, or cryptographic changes made to data units, which allows the recipient of the data unit to confirm the origin and integrity of the data and protect the data from being forged" (Ibid, pp 2 and 5). For an analysis of the role of encryption in blockchains: Schrepel T (2021), pp 18 ss

[35] ITU-T FG DLT (2019a), p 1

[36] PoW is not the only consensus algorithm in the world of blockchains. Among other reasons, the long-term sustainability and environmental impact of its energy-intensive design prompted the development of other consensus protocols, *e.g.*, Proof-of-Stake (PoS), Proof-of-Activity, Proof-of-Burn. Casey M, Crane J, Gensler G et al (2018), pp 2-3. Schrepel T (2021), p 24. An overview of consensus mechanisms is beyond the scope of this work.

[37] ITU-T FG DLT (2019a), p 8

[38] Schrepel T (2021), pp 18-19. The correctness of the "trustless trust" terminology is contested – *e.g.*, Walch A (2018), pp 1–27. Arruñada B (2018). Werbach K (2020).

[39] Freni P, Ferro E, Moncada R (2020), p 1

[40] In the DLT domain, an "oracle" is a third-party service or decentralised data feeds acting like bridges and providing external and off-chain information to the blockchain (since the latter cannot autonomously access them).

Information": an "Internet of Value (IoV)".[41] While the first one allows information to be shared by online means, the IoV leverages DLT-based solutions to foster the direct participation of every user in the global economy by embedding an economic layer into the web. In this respect, the concept of asset *tokenisation* emerges as one the most disruptive, as it depicts the process of issuing a token that digitally represents another (physical or non-physical) asset or right, to the end of storing it and exchanging it on the DLT. It is by leveraging *tokenisation* and P2P transfers that everyone can exchange value online directly, and blockchain technology creates the conditions for a "regulated" IoV, infused with public and democratic values.[42] In comparison with the level of intermediation featured by the traditional financial system, this setup shows a conceptual disruption. Despite their fascination, the concepts underlying the IoV need to be crafted carefully to reach a state of maturity, and cause bundles of problems that need to be addressed, especially in terms of legal and governance dynamics.[43]

1.1.2. What is the Internet of Money?

To refer to the monetary disintermediation and the dynamics of direct participation introduced by Bitcoin, Antonopoulos – one of the first knowledge disseminators in the field – conceived the term "Internet of Money (IoM)", and infused it with a libertarian ideological connotation.[44] Indeed, Bitcoin and other cryptocurrencies – referred to as "altcoins", *i.e.*, "alternative" to Bitcoin – are contextualised within a broader movement that is inherently influenced by the architecture of DLTs and their blockchain subset. This movement, in turn, holds a socio-economic promise of a technology-driven shift towards freedom and efficiency by getting rid of control bottlenecks – *i.e.*, intermediaries – through open and *decentralised* mechanisms.[45] This ecosystem is "as akin to the internet of money, a network for propagating value and securing the ownership of digital assets via distributed computation".[46]

More than a decade later, the set of ecosystems and applications that populate the cryptocurrency domain go well beyond Bitcoin itself. Meanwhile, new initiatives such as stablecoins and CBDCs have started leveraging value *tokenisation* to uphold various types of digital currencies that to a certain extent differ, ideologically and/or architecturally, from the first

[41] Casey M, Crane J, Gensler G et al (2018), p 7. Chen W, Zheng Z, Ngai ECH et al (2019), p 1. Garavaglia R (2019), pp 163-164. Tapscott D, Euchner J (2019). The Cryptocurrency Consultant (2019)
[42] Herian R (2019), p 81
[43] Casey M, Crane J, Gensler G et al (2018), p 7. Garavaglia R (2019), pp 163-164. Werbach K (2020), p 3
[44] Antonopoulos AM (2017a). Antonopoulos AM (2016). Antonopoulos AM (2017b)
[45] Werbach K (2020), p 2
[46] Antonopoulos AM (2017a), p 4

cryptocurrency projects. On the contrary, they grow near to the IoV and are often mentioned jointly.[47] Two major reasons for the lack of cohesion between the elements of the IoM is that there is no universal definition of it, and that it is influenced by constant evolutions. In this research, a broad concept of IoM is applied, to include the entire set of cryptocurrency ecosystems and their applications and to refer to them collectively and techno-economically. Hence, in this work the IoM includes the part of the IoV that relates to payment tokens but also payment-type cryptoassets issued on permissionless/private blockchains and/or that do not share Bitcoin's concept of disintermediation, while these concepts are explored below.

When exploring the interplay of cryptocurrency ecosystems and AML/CFT/CPF rules, I realised the topic is positioned within the ever-evolving phenomenological landscape where cryptocurrency transfers take place.[48] Given the dynamics of the AML/CFT/ CPF framework, outlined in Chapter 4, and specific traits of the IoM such as its *anonymity* and its *transparency*, it became clear to me that the regulatory analysis must be grounded on concrete considerations concerning the actors, elements and entities that populate these ecosystems. Moreover, the terminological unclarity tainting this sphere led me to consider making a preliminary disambiguation effort to define conceptual yardsticks that can act as foundations for my reasoning.

Accordingly, in this chapter I lay out the phenomenological setting that backs the investigation. To this end, I provide an overview of (i) the concepts of tokens and cryptoassets in terms of definitional impacts, (ii) the role of taxonomy initiatives to understand IoM components, (iii) the phenomenology of cryptocurrency ecosystems from a static (*i.e.*, architectural) and dynamic (*i.e.*, transactional) perspective, (iv) the socio-technical nature of this sphere, (v) the need to challenge the "blockchain hype" and distinguish between theory and practice, to safeguard *accountability*, (vi) the ambiguities surrounding *disintermediation*, (vii) the evolution of stablecoins and CBDCs, to finally (viii) provide preliminary remarks on how to approach the interplay between the IoM and the regulatory domain.

1.2. On a Hunt for Definitions: the Realm of Tokens and Cryptoassets

In the IoM, terminological consensus is far from being established. Not only does a large array of terms identify relevant applications, but their use varies across jurisdictions and research

[47] *E.g.*, Klarin A (2020)

[48] "Phenomenology" refers to the IoM from a concrete perspective, *i.e.,* what can be experienced observing relevant applications, stakeholders, implementations, features. This terminology highlights possible contrasts between abstract principles believed to be broadly applicable (*e.g.*, *anonymity*, *decentralisation*), and what can be observed.

communities. *Tokens*, *digital tokens*, *digital currencies*, *virtual currencies*, *cryptocurrencies*, *digital assets*, *virtual assets*, *cryptoassets, digital coins*, *virtual coins*, are often used indistinctly to refer to ecosystems, platforms, protocols, and assets. Because each of these options generates specific consequences, their interchangeability hinders the creation of a harmonised groundwork on which to build regulatory initiatives, rules for interpretation and enforcement schemes.

In particular, the establishment of a worldwide approach has been hampered by the pursuit of two understandable, albeit partly opposite, goals: safeguarding consumers, investors and the economy at large from new risks, while reaping the benefits from these ubiquitous markets.[49] The two sentiments originated inconsistent and frequently unprecise methodologies: (i) a general acquiescence and a wait-and-see attitude, sponsoring a general abstention from invasive initiatives, (ii) caution and fear in front of the (partially) unknown, which led to domain-specific definitions and terminological fragmentation. Almost fifteen years after the advent of Bitcoin and given the considerable developments of the IoM sphere, however, a *reactive* approach is no longer justifiable. On the contrary, it is pivotal to employ a teleological and pragmatic reasoning and to bear in mind to what end one is trying to set a definition. Avoiding over-simplifications and over-generalisations is key to understanding a complex domain, albeit not getting lost in inconsequential arguments is obviously a prerequisite for any sound analysis.

1.2.1. Terminological notes from an EU and FATF perspective

Since the financial domain harboured the first large-scale applications of DLTs, the most comprehensive set of terminological insights can be retrieved in this field. In past years, a vast number of studies showed multiple ways to approach these ecosystems from a regulatory standpoint. Institutions across the financial landscape provided a considerable, albeit divergent at times, set of definitions. They largely made use of the term *cryptoassets*, in line with the approach employed by standard-setting bodies. Because of the sense of urgency spurred by the fast development of these tools, however, most initiatives have been prompted by fear of abuses rather than by a structured desire to achieve consistency and grasp connecting factors between the technical and the legal essence of these instruments. Therefore, regulatory and policy documents offer a variety of definitions whose degree of specificity differs substantially.

An example is featured by the 2018 FinTech Action plan, whereby the European Commission (EC) requested the European Supervisory Authorities (ESAs) to provide an assessment of

[49] Athanassiou PL (2019), p 3

whether the EU framework was suitable for ICOs and cryptoassets.[50] On that occasion, the EC referred to "market developments in *crypto-assets*", "speculative investment in *crypto-assets* and ICO-*tokens*", while exchanges and service providers "allow investors to purchase *crypto-assets* and *tokens*, hold them and trade them".[51] In their January 2019 reports, the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) fell in line with this terminology.[52] The EBA report defined a *cryptoasset* as an asset that "(a) depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value; (b) is neither issued nor guaranteed by a central bank or public authority, and (c) can be used as a means of exchange and/or for investment purposes and/or to access a good or service".[53] ESMA, on its part, identified "*cryptocurrencies* or *virtual currenci*es" and "*digital tokens* issued through ICOs" as two sub-groups. In May 2019, the European Central Bank (ECB), referred to the term *crypto-assets* in a publication written by the Crypto-Assets Task Force,[54] albeit the scope of the definition was limited to "a new type of asset recorded in digital form and enabled by the use of cryptography that is not and does not represent a financial claim on, or a liability of, any identifiable entity".[55] Furthermore, it was argued the definition was consistent with the EU concept of *virtual currencies*, albeit the latter is deemed to be broader.[56] Terminological malleability was confirmed by a December 2019 note of the International Monetary Fund (IMF), according to which "the term *crypto asset* denotes *digital assets* that use cryptography for security and are *coins* or *tokens* of distributed ledgers and/or blockchains, including asset-backed *tokens*", thus honouring the fact that "the definition of a crypto asset is far from globally uniform".[57] Moreover, although the terms were interchangeably employed in the document, a distinction between *coins* and *tokens* was acknowledged.[58]

The preference of EU institutions for the term *cryptoassets* was confirmed by the Digital Finance Package adopted in September 2020.[59] Among the actions encompassed by its

[50] European Commission (2018). The ESAs are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA)
[51] Ibid, p 6
[52] European Banking Authority (2019). European Securities and Markets Authority (2019)
[53] European Banking Authority (2019), pp 10-11. The distinction sub (c) introduces the most widespread categorisation in the area.
[54] ECB Crypto-Assets Task Force (2019)
[55] Ibid, p 3
[56] Ibid, p 7
[57] Cuervo C, Morozova A, Sugimoto N (2019)
[58] Ibid. More specifically, "coins refer to bitcoin and altcoins, which were originally issued with a main purpose to serve as "currency," that is, with money and payments-related functions. Tokens have more functions than coins, for example, permitting the coin holders to participate in the service provided or the returns offered by the token issuer" (Ibid).
[59] European Commission (2020d)

timeline, the EC put forward two legislative proposals explicitly labelled to be "on *cryptoassets*" – one for a Regulation on Markets in Crypto-Assets (MiCA)[60], and one for a Regulation on a Pilot Regime for Market Infrastructures Based on DLT.[61] While the first one states that a *cryptoasset* is "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology",[62] its original text used to specify that "any definition of *crypto-assets* should […] correspond to the definition of *virtual assets* set out in the recommendations of the Financial Action Task Force".[63] However, the most recent text of the upcoming MiCA Regulation, as amended during the legislative process, does not bear explicit reference to this equivalence.[64] The specification is worth noting because a partial discrepancy can be found between EU terminology and that of the FATF, the most important international authority in the AML/CFT/CPF domain.[65]

Indeed, albeit the international standard-setter originally used the term *virtual currencies*, it introduced the notions of *virtual assets* (VAs) and *virtual assets service provider* (VASPs) in line with the evolution of the relevant space. While in 2015 the FATF published a "Guidance for a risk-based approach: virtual currencies", in 2019 the scope changed to "Guidance for a risk-based approach for virtual assets and virtual asset service providers", and the following reports reiterated the choice.[66] According to the provided definition, a *virtual asset* is a "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations".[67] This is the definition included in the Glossary from 2019 and referenced in October 2021 by the "Updated guidance for a risk-based approach to virtual assets and virtual asset service providers".[68] The document testifies to the importance of monitoring the impacts

[60] European Commission (2020b)
[61] European Commission (2020a)
[62] European Commission (2020b). Article 3(1)(2). The most recent text of the proposal, that is approaching the end of the legislative procedure, was agreed-upon by the Council on October 5, 2022, and maintains reference to the notion of *crypto-asset* (Council of the European Union (2022a)).
[63] European Commission (2020b), Recital 8
[64] Council of the European Union (2022a). In this version of the text, Recital 8 reads "'Crypto-assets' and 'distributed ledger technology' should therefore be defined as widely as possible to capture all types of crypto-assets which currently fall outside the scope of Union legislation on financial services. Such legislation should also contribute to the objective of combating money laundering and the financing of terrorism. For this reason, entities offering services within the scope of this Regulation will be required to follow applicable rules on AML in the EU, which integrate international standards".
[65] The Financial Action Task Force (FATF) is an intergovernmental organisation whose mandate focuses on setting standards to combat threats to the international financial system.
[66] Financial Action Task Force (2015). Financial Action Task Force (2019). Financial Action Task Force (2020d). Financial Action Task Force (2020a). Financial Action Task Force (2021d)
[67] Financial Action Task Force (2019), p 47
[68] Financial Action Task Force (2021e), p 109

of definitions, and one of its goals is the clarification of the definitions of VA and VASP to ensure they are "expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards (either as a VA or as another financial asset)".[69] The main question is related to the qualification of *stablecoin* arrangements, whose uncertain definition had been addressed by several institutions,[70] and in the upcoming EU MiCA Regulation.[71]

The *virtual* choice can also be found in EU legislation. Directive (EU) 2015/849 (the so-called 4AMLD), as amended by Directive (EU) 2018/843 (the 5AMLD), does not mention *cryptoassets*, but defines *virtual currencies* 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".[72] After the release of the AML Package addressed in Chapter 4, however, it can be argued the EU is converging towards the *crypto* option. Indeed, Article 2(1)(13) of the proposal for a Regulation on the prevention of the use of the financial system for ML/TF purposes refers to the definition of *crypto-asset* of the proposed MiCA Regulation.[73] Meanwhile, it focuses on *crypto-asset service providers*, which are also at the core of the recast of Regulation (EU) 2015/847 to expand traceability requirements to *crypto-assets*.[74]

Against this backdrop, preliminary conclusions may be drawn while heeding a flexible approach to terminological interpretation. If the context is clearly outlined, the terms *cryptoassets*, *digital assets* and *virtual assets* may be used interchangeably. Ostensibly, however, the wording *digital assets* has a more generic nuance, and can cause confusion.[75] Other expressions such as *cryptocurrencies* or *virtual currencies* identify a subset of the *assets*. This is the way they are used in this work, but a literature review shows how in early documents they were used to refer to the global set of *cryptoassets*. Albeit the term *digital currencies* was used in several cases, it arguably lacks specificity when compared to *virtual currencies* or *cryptocurrencies*.

To establish a structured approach, and for the sake of clarity, one may distinguish between two parts of these compound words: (a) *crypto*, *virtual*, *digital*, and (b) their possible objects –

[69] Financial Action Task Force (2021e), p 5
[70] *E.g.*, Financial Action Task Force (2020b). Financial Stability Board (2019) G7 W.G. on Stablecoins (2019)
[71] European Commission (2020b). Council of the European Union (2022a)
[72] 4AMLD Article 1(d)(18) as amended by 5AMLD Article 1(2)
[73] European Commission (2021a)
[74] European Commission (2021c). Details are provided in Chapter 4.
[75] A report provided a narrower definition of *cryptoassets* as "digital tokens exclusively issued and transferred via open, permissionless DLT systems that play an indispensable role in the economic incentive design of the underlying shared ledger or application. They do not represent any external rights or things, and, consequently, do not constitute a financial asset" (Allen JG, Rauchs M, Blandin A, Bear K (2020), pp 4, 12).

currencies, *assets*, *tokens*, and *coins*. The part sub (a) is often employed interchangeably, which leads to interpret *cryptoassets*, *virtual assets* and *digital assets* as synonyms. Literally, however, *crypto* is a subcategory of *virtual*, which is a subgroup of *digital*. Hence, *cryptocurrencies* are the subset of *virtual currencies* whose functioning relies on cryptography. Following this reasoning, *digital assets* is the most comprehensive expression, although the literature also defines *cryptoassets* as a neutral choice.[76] Undeniably, most of the retrievable definitions are sector-specific, and focus on financial regulation, cryptoassets market structure and relevant risks. This approach can cause discrepancies and may not relate to the architectural nature of these assets. In these cases, the use and usefulness of the definitions is limited to the specific framework, and they cannot be used as general benchmarks. As these inconsistencies hardly fit the legal need for certainty, in some jurisdictions (*e.g.*, United States) the tendency is to ignore the formal qualification of a specific instrument when establishing applicable rules, and they rather refer to the concrete activity or transaction undertaken in each case.[77]

1.2.2. Tokens: bridging techno-legal definitional gaps

Concurrently, the terms *tokens* or *digital tokens* are often used as a synonym of *cryptoasset* or, in conjoined expressions, to identify a subset of them – *e.g.*, ICO-tokens or asset-backed tokens. This is not wholly incorrect, but a useful distinction can be made. Seemingly, these items are referred to as *tokens* when a technological approach is employed, or when there is an attempt to visualise these instruments to describe them. Nonetheless, it was argued that "*digital assets*, sometimes called *tokens*, are poorly understood. That may be why they are used to describe a variety of things, some of which are contradictory", as well as "the different interpretations and uses of the word *token* are many, varied, and collectively confusing".[78] Although dwelling on terminological aspects may seem a triviality, the past years have proved this to be debatable at best. Indeed, the increasing variety of DLT-based *assets* is posing cross-disciplinary problems. Having no clear regulatory box in which to place an entity is not inconsequential, and technological development suffers from the causal link between the lack of (harmonised) definitions, lack of interdisciplinary dialogue, and lack of standardisation. In other words, the perception different communities have of new technologies is influenced by regulatory regimes. This public perception, in turn, is susceptible to shaping technological development.

[76] Brummer C (2019), p 1
[77] *E.g.*, "Howey test", deployed by the US Supreme Court to determine if a transaction qualifies as a security.
[78] Tapscott D (2020), pp 3 and 5

If uncertainties undermine cross-disciplinary cooperation in the field of cryptoassets, one can only imagine the extent to which the lack of a reference framework impairs public understanding.[79] The complexity of the DLT space, complemented by the impossibility of explaining the basics with a common language, can block communication with society. Under these circumstances, some perceived risks grow exponentially and are not caused as much by the features of cryptoassets as by widespread misconceptions. Since the average consumer is fascinated by the IoM, this calls for efforts by cross-disciplinary communities. In this respect, a valuable initiative finds *tokens* more suitable than other concepts to establish a common reference framework. While the expression *tokenisation* is getting a foothold, in line with a shift from *economics* to *tokenomics*,[80] tokens were described as one of the building blocks of the blockchain world.[81] Above and beyond, "far from being just a means of payment, tokens are the critical data structure that could underpin every aspect of the future society".[82]

There is a general agreement that *tokens* are *cryptoassets*. Besides, *tokens* have been conceptualised as the "legal wrap-up" of *cryptoassets* and depicted as crucial in the *tokenised economy*, while their legal validity might be ensured through smart contracts.[83] In a more descriptive way, *tokens* would be the way a legal right is embedded into a *cryptoasset*.[84] The value of this idea lies in linking the two concepts of *tokens* and *cryptoassets* without forcing them into an unstable and undefined unicum. *Cryptoassets* can be digital or digitised assets, which means a *token* can represent a primary digital asset (the asset exists exclusively on the blockchain) or be issued by tokenising existing assets (*e.g.,* physical assets or rights).[85] Arguably, *tokens* represent architecturally what *cryptoassets* are, which explains a broader use of the latter in legal discourse. The *tokenisation* process consists of encapsulating "value in tradeable units of accounts".[86] Legal components embedded in a *token* define what kind of *cryptoasset* is originated, as the *token* can be seen as a digitised version of the underlying value.

Whether and how a *token* is also a *coin* from a strict definition perspective, however, is not straightforward, although every *digital coin* is a cryptoassets and also a *token*, given that every

[79] Ibid, p 5
[80] Sandner P (2020) *Tokenisation:* conversion of a physical or non-physical asset into a digital token on a blockchain. *Token economics*: a type of economy reflected by the design of an ecosystem in a blockchain environment
[81] Athanassiou PL (2019)
[82] Skalex (2019) Arguably, tokens do not actually "exist", either physically or in code. In fact, there is no "code" that specifically refers to a "coin", a blockchain token is just a series of receipts.
[83] In the token economy, medium of exchanges feature embedded incentives and disincentives, while smart contracts and decentralised apps enable preprogrammed, (purportedly) trustless, interactions (Casey M, Crane J, Gensler G al (2018), p 5)
[84] Garavaglia R (2019), p 168
[85] Inozemtsev MI (2021)
[86] Freni P, Ferro E, Moncada R (2020), pp 1-2

digital coin technologically appears as a *token*. The matter rests on the meaning given to *coin* and *token*, which goes back to the definitory levels of *assets* and *tokens*. Clearly, it is necessary to create a framework to provide these terms with clearer scopes of application, hence the relevance of the taxonomical efforts described below. These initiatives single out types and uses of *tokens*, as well as their properties, from a legal and a technical standardisation perspective.

1.2.3. Taxonomy initiatives: cryptocurrencies as payment-type cryptoassets

When trying to establish what cryptoassets are, focus has been mainly on identifying subgroups.[87] A key concept leveraged to distinguish cryptoassets is their *purpose*, although over time this approach was complemented by details that emerged from developments in the area. From the standpoint of what a cryptoasset entails, three categories of underlying tokens were pinpointed:[88] (i) *exchange tokens*, also labelled as *payment tokens* or *currency tokens*; (ii) *security* or *investment tokens*; (iii) *utility tokens*. *Cryptocurrencies* fall within the category sub (i) and can be defined as *payment-type cryptoassets*. Hence, as per the reasoning above, *payment tokens* are the architectural representation of what *payment-type cryptoassets* (*i.e.*, *cryptocurrencies*) are. They are used as a means of payment or exchange for goods and services, where the latter, in principle, are external to the DLT ecosystem on which the tokens are built. When a token is used to access goods and services, with the latter being internal to the DLT ecosystem they are built on, it belongs to the group sub (iii). In practice, *utility tokens* can also feature investment purposes; when they are legally defined as financial instruments, however, they are deemed *security tokens*.[89] When a token falls into more than one category, it is *hybrid*.

In crypto-oriented publications, *utility* or *security* may refer to two extremes that are construed instrumentally and are complementary features of a collective whole. In this respect, the perception is that tokens should be touched by the law only if they are of the *security* type. On the contrary, if a token is of the *utility* kind, or advocated as such, regulatory legitimacy would be lacking.[90] However, it is common for a cryptoasset to be *hybrid*, and ever-evolving features may be the basis of different interpretations. This may explain why terms like *cryptocurrencies* and *digital coins* are sometimes used with a broader scope, to include *utility* or *security tokens*.[91]

---

[87] Examples of academic studies include Oliveira L, Bauer I, Zavolokina L, Schwabe G (2018). Euler T (2018)
[88] HM Treasury, Financial Conduct Authority, Bank of England (2018). Tapscott D (2020)
[89] In the United States, a *security token* is one that passes the "Howey Test"; in this case, the abovementioned transaction-oriented approach is employed, and the actual activity taking place is assessed.
[90] Tapscott D (2020), p 4
[91] Ibid, p 4. After the 2017 boom, certain Initial *Coin* Offerings were ruled as "unlicensed sales of *securities*" by the US Securities and Exchange Commission (SEC); later, the term "Security Token Offerings" (STOs) emerged.

Furthermore, a cryptoasset can be either *native* to its own blockchain, like Bitcoin or Ether, or *non-native – i.e.*, built on top of another blockchain (*e.g.*, a *utility token* built on Ethereum) – and acting as a proxy, representing assets that exist outside the given ledger.[92] Another label derives from Ethereum enabling projects and dApps to be developed through smart contracts deployed on its platform: *application* or *platform token*. When a token is created to be used on a dApp, its purpose depends on the application itself.[93] These tokens can be used as "facilitators" for users external and unrelated to the operation of the network that has created them.

The idea of *coins* and *tokens* being antithetical concepts is seemingly simplistic. However, it leads to a better understanding of the different levels these remarks should be attached to. As the crypto-economy evolved, especially through Ethereum-based options, some uses of the term *token* started to part from *cryptocurrencies*. Tokens started to be used to represent both real world objects (*e.g.*, land, artwork, vehicles) and rights (*e.g.*, intellectual property), and *tokenisation* processes allowed *decentralisation* to be applied to value-based heterogeneous contexts beyond the monetary sphere.[94] Accordingly, tokens were phrased to be *fungible* or *non-fungible*. Whereas the first group refers to money-related fungibility (*i.e.*, interchangeability or functional equivalence), the creation of unique crypto-items was enabled by the Ethereum ERC-721 standard. While a popular traditional example is that of crypto-collectibles like CryptoKitties, Non-Fungible Tokens (NFTs) have more recently reached not only the headlines and an impressive share of worldwide interest, but also incredible evaluations. In the words of the FATF, NFTs are "digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments".[95] In brief, while one bitcoin, or one ether, are equal, respectively, to another bitcoin or another ether, every CryptoKitty is one of a kind, and an NFT can represent anything in a unique form as an Ethereum-based asset. They leverage the smart contract technique provided by the Ethereum blockchain and they represent ownership of unique items. For instance, they allow digital fine art to be sold to collectors, leveraging the capacity of NFTs to ensure proof-of-ownership. They allow the ownership of any unique asset – *e.g.*, real estate, music – to be tokenised.[96]

The concept of *token* is familiar to technology-oriented domains and useful to connect legal arguments to it. The "Token Taxonomy Initiative (TTI)" by the Blockchain Research Institute

[92] Athanassiou PL (2019), p 3. In a slightly inconsistent way with the approach praised here, the words "coins" and "tokens" have been respectively linked to these two categories; only cryptoassets having their own platform can be "coins", while "token" identifies non-native assets.
[93] Distefano B, Pocher N, Zichichi M (2020)
[94] Freni P, Ferro E, Moncada R (2020), p 2
[95] Financial Action Task Force (2021e), p 24
[96] Ethereum (2022)

addresses these issues. It pursues standardisation and meta-standardisation,[97] not only to suit socio-legal needs of oversight and *accountability*, but also for technical and interoperability reasons. To make sense of what a *token* is, the "Token Taxonomy Framework (TTF)" was launched in 2019. The idea was to create a composition scheme from the ground up, by making use of concepts and terms that can define and describe token projects in a modular, flexible and expandable templatised way that is both intuitive and technical.[98] The TTF identified a set of token features: *valuable* (value can be determined), *representative* (of a claim to an asset, resource, right), *digital* (digitally stored), *discrete* (existence and number do not rely on observers), *authentic* (authenticity can be verified). It also defined token *types*, *behaviours* and *properties*. Token *types* are its first foundation; beside *fungible* and *non-fungible* tokens, the idea of *hybrid tokens* is introduced when both fungible and non-fungible features are embodied (*e.g.*, a reserved ticket). As to compositional elements, tokens can have different *behaviors*: rules for how they behave (*e.g.*, singleton, indivisible vs. divisible); and *properties/property sets*: descriptive values they must have, but only have external meaning (*e.g.*, a serial number).[99]

The fast-growing variety of tokens, however, does not only need classification templates; to increase security and avoid scams, they must be uniquely identified. The decentralised nature of the token-based economy makes it hard to distinguish between legitimate and fraudulent projects and to unambiguously refer to an item – *e.g.*, in sale and purchase agreements. Arguably, "any service that neglects to maintain unique references is contributing to corrupt the entire subsequent ecosystem relying on its data", which prevents market maturation. [100] The International Token Standardisation Association (ITSA) tackled the issue and developed holistic market standards as unique identifiers. The scope included all DLT-based cryptographic tokens; the goals were *identification*, *classification*, and *analysis*.[101] The "International Token Identification Number (ITIN)" was created. For decentralised items identification is pivotal; their being software-defined and fork-susceptible demands to adequately locate their addresses across protocols.[102] The ITIN framework addressed the different levels of the *token* and *asset*

[97] *Meta-standardisation* refers to being chain-agnostic and technology-neutral. Tapscott D (2020), pp 8-9
[98] Ibid, p 7. A specific syntax allows tokens to be defined by using a string of characters and a design tool eases the creation of puzzle-piece-looking tokens (Ibid, p 14).
[99] Ibid, pp 10-12. Notably, the TTF outlined a set of *behaviours* that highlight features of a token behaving like money (Ibid, pp 12-13). More information is provided below.
[100] Sandner P (2020)
[101] International Token Standardisation Association (2022)
[102] The concept recalls Uniform Resource Locators (URLs) to locate web resources. ITINs build on the "Uniform Token Locator" standard, consisting of genesis hash, post-fork hash, recent hash, smart contract address, token sub-address. Most tokens are identifiable through post fork hashes and smart contract addresses; for NFTs sub-address can be used. Reliability and unambiguity are guaranteed by recent hashes. ITIN acts as a UTL shortener.

definitions in an elaborate way. The term *asset* was used to identify the form of economic value represented by *tokens*.[103] In contrast to other identifiers, it did not assign a "name" to an asset. The ITSA interface allowed reference to all information about the token and the transaction. Taxonomy projects pursued by the BRI and ITSA show the concept of token is as crucial as multi-layered. Arguably, the token definition addresses two elements: their function and the essence of the asset they represent.[104] Hence, there are no inherent or self-standing definitions, and classification frameworks ought to focus on mapping value representations.[105]

1.2.4. The regulatory role of tokens

Taxonomy initiatives show the importance of token definitions to convey a meaningful image of the IoM. If one considers that a *token* is the representation, from an architectural viewpoint, of what a *cryptoasset* is, their legal value is easier to grasp. Indeed, the creation and exchange processes, the rights they symbolise, the difference and/or similarity to traditional assets, are all legally impactful topics. In broader terms, the perception of the role of tokens is increasing, and there is an emerging call to use them as regulatory benchmarks. Not many legal systems, however, have abided by this approach. It was argued that when the usefulness of tokens is not recognised, there is usually a lack of technical knowledge, and two consequences arise: an intensification of existing uncertainties and ambiguities and regulating intermediaries remains the only feasible methodology.[106] The last aspect is relevant to the AML/CFT/CPF domain, where current regulatory attempts are tainted by the insufficiency of applying "active cooperation" strategies to new socio-legal ecosystems. Meanwhile, most tokens remain unregulated, as they do not meet the standards of a type of recognised asset.

In this respect, valuable insights can be drawn from a legislative initiative adopted in Liechtenstein in October 2019: the so-called "Blockchain Act".[107] Its scope of application are "Tokens and Trustworthy Technologies (TT)", which are "technologies through which the integrity of Tokens, the clear assignment of Tokens to TT Identifiers and the disposal over Tokens is ensured".[108] A Token is defined as "a piece of information on a TT System which: (1) can

[103] ITSA represented the relationship between tokens and assets by using three layers: asset layer, protocol layer, token layer (token address, location and definition). The asset layer refers to the referenced asset, in terms of its economic value, *e.g.*, for a share it would be dividend payments or voting rights, for physical assets their value.
[104] Freni P, Ferro E, Moncada R (2020), p 2
[105] The proposed approach is grounded on General Morphological Analysis and aims to map all dimensions of the problem (*i.e.*, token identification and definition) and possible relationships to identify patterns (Ibid, p 3).
[106] Athanassiou PL (2019), pp 3 and 7
[107] Liechtenstein's Gesetz über Token und VT-Dienstleister (2019)
[108] Ibid, Article 1(1)(a)

represent claims or rights of memberships against a person, rights to property or other absolute or relative rights; and (2) is assigned to one or more TT Identifiers", *i.e.*, public keys, enabling token assignment.[109] In brief, Liechtenstein did not regulate DLTs but focused on tokens, treated as "containers of rights" and whose ownership/transfer is grounded on the interdependence between tokens and private keys. Meanwhile, the obligation of service providers to register depends on their functional relationship with tokens. Positive evaluations of the initiative consider that if it is through tokens that DLTs can unfold their potential and create new categories of assets and new ecosystems for their exchange, their regulation must be approached through the prism of tokens.[110] The EC's Digital Finance Package seemingly agrees, as it explicitly addresses *tokenisation*, and the MiCA Regulation is largely based on *tokens*.[111]

1.2.5. Cryptocurrencies and qualification as legal tender

Cryptocurrencies are referred to as *payment tokens*, also known as *currency* or *exchange-type tokens*. They are the prime implementation of blockchain technology, at the roots of the relevant hype. In this respect, a popular distinction is the one between *convertible* and *non-convertible* cryptocurrencies, which takes the possibility to exchange them with fiat currency as a benchmark.[112] The prevalence of *convertibility* over other categorisations mirrors a regulatory approach focused on the impact on the traditional financial system – *i.e.*, on funds entering/leaving the IoM through an intermediary. Although the evolution of regulatory frameworks shows an increasing awareness of how the convertibility argument may be simplistic, the perception that non-convertibility *per se* entails dwarfed risks stems from the fact that there is no agreement on legally classifying cryptocurrencies as money. Indeed, as of today the only two jurisdictions that qualify *Bitcoin* – only Bitcoin, not any cryptocurrency – as legal tender are El Salvador, which did so with a controversial initiative known as "Ley Bitcoin" (or "Bitcoin law"),[113] and more recently the Central African Republic.[114]

As far as El Salvador is concerned, in September 2021 the country adopted "bitcoin as unrestricted legal tender with liberating power, unlimited in any transaction, and to any title that public or private natural or legal persons require carrying out" (Article 1), hence "all

[109] Ibid, Article 1(1)(c) and (d)
[110] Athanassiou PL (2019)
[111] European Commission (2020a). Council of the European Union (2022a)
[112] *Fiat currency* has no intrinsic value and is legal tender by means of a governmental act.
[113] Decreto Nº 57, del 8 de Junio del año 2021. A comment was published by: Gorjón S (2021) An English translation of the "Bitcoin Law" can be found at: Roy A (2021)
[114] Kabré RJ (2022). The qualification of Bitcoin as legal tender was introduced by Law No. 22.004.

obligations in money expressed in USD, existing before the effective date of this, may be paid in bitcoin" (Article 13).[115] Accordingly, "tax contributions can be paid in bitcoin" (Article 4) and "exchanges in bitcoin will not be subject to capital gains tax, just like any legal tender" (Article 5). Although "every economic agent must accept bitcoin as payment when offered to him by whoever acquires a good or service" (Article 7), the Decree acknowledges the country's structural issues, and provides that "those who, by evident and notorious fact, do not have access to the technologies that allow them to carry out transactions in bitcoin are excluded from the obligation expressed in Art. 7 of this law. The state will promote the necessary training and mechanisms so that the population can access bitcoin transactions" (Article 12). Technical standards were later drawn up by the local Central Bank – *e.g.*, wallets, educational measures.

The Central African Republic adopted Bitcoin as legal tender in April 2022. Controversies ensued, due to the dramatic socio-economic and geopolitical situation of the country, and its being a member of the Central African Monetary Union. Further, the country features very low Internet access and digital literacy,[116] while Bitcoin's volatility discourages merchants from accepting bitcoins as a means of payment even if mandated by Article 10 Law No. 22.004.[117]

These cases show how the legal qualification of cryptocurrencies is an issue inherently addressed at the (supra)national level, in line with elements of "monetary law" and "central bank law" explored in Chapter 5. Obviously, this generates fragmentation that stems from different interpretations, while when supranational and international frameworks deal with *exchange-type cryptoassets* they tend to do so in silos, limiting their actions to the scope of each of their mandates. Overall, their goal is to prevent and mitigate risks and negative socio-legal impacts posed by these instruments. The general approach is not to state whether cryptocurrencies are legal tender, but to determine whether specific rules for monetary or financial transactions apply to them. This generates an intertwinement of fragmentations that adds to – and partially derives from – the difficulty in connecting the conceptual levels of being *money* from a legal perspective and a *token* from a computer science standpoint. This is made even harder by the linguistic impact of token discourse originating from the Bitcoin world, which developed in opposition to traditional monetary systems. Above all, traditional legal concepts of money and currency do not relate to technology, as they are built on conventions.

Against this backdrop, a major problem posed by DLT-based implementations lies in asking the law to apply unconventional reasonings. When living in the *tokenised economy*,

[115] US Dollar is the official currency of El Salvador
[116] It was estimated 15% of the population has access to electricity and 10% to the Internet. Kabré RJ (2022).
[117] Ibid. Law No. 22.004

however, it makes sense to distinguish tokens that behave like money from tokens that do not. Arguably, if one wants to use the concept of token as a legal benchmark and provide it with tailored rules, the role of technology is inevitably stronger than usual. After all, (a set of) blockchain-based solutions were described as replacing the traditional concept of trust with an innovative type of trust that is placed on technology itself, in the form of computer protocols.[118] From a pragmatic standpoint, the TTI maps features that a token must display to behave as money; as acknowledged, the list is a work in progress. Namely, such a token must: (a) have roles that are *definable* and *assignable*, and be (b) *delegable* (*i.e.*, the owner can delegate certain behaviours), (c) *transferable* and (d) *holdable* (*i.e.*, every token has an owner that can transfer it), (e) *compliant* with legal obligations (*e.g.*, AML/CFT), (f) *burnable*, (g) *mintable*.[119]

As far as payment tokens are concerned and depending on the source of their value, there is a difference between (i) *intrinsic value tokens*, and (ii) *asset-backed* or *asset-referenced tokens*. The first category derives its value from the activities (*e.g.*, acquisition and use) undertaken by the users, while the value of the second group depends on the value of the mirrored assets, as in stablecoins. In this regard, the upcoming MiCA Regulation provides for a subclassification of cryptoassets that distinguishes between (1) *utility tokens* – which are "only intended to provide access to a good or a service supplied by" their issuer (Article 3(1)(5)) – from (2) *asset-referenced tokens*, aiming "to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies" (Article 3(1)(3)); and (3) *e-money tokens*, which purport "to maintain a stable value by referencing to the value of one official currency" (Article 3(1)(4)).[120]

1.3. The Accountability Conundrum: the IoM – Architectures and Transactions

The IoM label was coined by Antonopoulos to discuss the innovative interplay between individual Internet users and *disintermediated* monetary transactions. His use of this expression features a strong ideologic characterisation, and in his speeches the *disintermediation* philosophy of the crypto-economy is an inspiration to change socio-economic dynamics, in line with the "blockchain hype".[121] Nonetheless, the concrete impact of cryptoassets on the general public has been as diverse as multifold. When new technologies meet established markets, they

[118] Athanassiou PL (2019), p 2
[119] Tapscott D (2020), pp 12-13
[120] Reference here is to the last available version of the text: Council of the European Union (2022a)
[121] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), pp 3 and 12

introduce both opportunities and new sets of risks. While some of them may be only perceived due to the fear of the unknown and of disruption, others may exert very concrete consequences. From a first perspective this work investigates dangers linked to the *anonymity problem*, tainting some cryptocurrency ecosystems with risks of money laundering, fraud, tax evasion, and other forms of exploitation for illicit purposes. Secondly, this analysis weighs *anonymity* against the features of *transparency* that may inform DLTs architecturally.

Since this endeavour requires disambiguation of the features of these instruments, the need arises to explore their origin and the various understandings developed in their respect. Indeed, when focusing on an architectural interpretation of cryptocurrencies that is mostly token-based, one may incur the risk of thinking they are deemed *anonymous* or *transparent* only because of how relevant tokens are construed. On the contrary, there are many aspects to be considered. The risks sketched above are not only inherent to tokens, but mostly relate to the structure of the systems that generate and exchange them, and to how governance is managed within them.[122] The main components that may influence such assessments are introduced below.

1.3.1. Cryptocurrency ecosystems: stakeholders and socio-technical traits

Notwithstanding the role of architectural features in cryptocurrency networks, important distinctions relate to the interplay of the actors involved in their lifecycle. A major example is that of the "trustless" characterisation of these systems, where the general perception is of a thorough departure from trust among parties, leading to describe DLT-based implementations as inherently trustless – or at least substituting interpersonal trust with one in technology and algorithms. These arguments have been debated with reference to the roles concretely played by specific actors,[123] and legal literature has explored the impacts of participating stakeholders on *accountability* and liability within *non-centralised* and *distributed* networks.

Scholars refer to cryptocurrency ecosystems, and to some related activities – *e.g.*, cryptolaundering or platforms for digital democracy –, as "socio-technical systems (STSs)".[124] This expression compounds the interrelation between different levels of what the system is and does, as well as the way it interacts with other networks and/or external sources.[125] As the label suggests, they are complex systems that comprise elements belonging to the human, technological

[122] Governance aspects are closely connected to the decentralisation debate (see below).
[123] Walch A (2018). Arruñada B (2018). Werbach K (2020)
[124] Desmond DB, Lacey D, Salmon P (2019), pp 481-482. De Domenico M, Baronchelli A (2019), p 1. Poblet M, Allen DWE, Konashevych O, Lane A (2020), p 3. Renwick R, Gleasure R (2020)
[125] Werbach K (2019), pp ix-x

and technical sphere, organised to pursue a common goal. To grasp their behaviours, one should not only examine separate components, but also their interactions – *i.e.*, the overall system should be taken as unit of analysis.[126] While sections below provide insights on interactions with external elements, this section outlines the basic stakeholders in an IoM ecosystem.[127]

The foundational stakeholders are: (a) users, (b) market participants, (c) nodes, (d) miners/forgers, (e) software developers.[128] Their concrete roles are defined by the specific algorithms, which means the extent of their power depends on structural and governance classifications. While a comprehensive individual analysis of these actors would prove inconsistent with the objectives of this work, their role is all but inconsequential. Indeed, regulatory efforts are constantly looking for targets to which their goals can be linked, especially when their traditional approach is based on intermediaries, such as in the AML/CFT/CPF sphere. In this respect, a substantial amount of literature provides analytical overviews of how their specific features may impact different DLT-based ecosystems, as well as of how technology itself prompts and encourages their participation and/or decisions, if any.

For instance, actors can be classified as per their relationship with the ecosystem, and were labelled as *essential*, *native*, or *metamorphic*. *Essential* stakeholders are necessary for the system to exist, but do not (purportedly) exert control over the network. In permissionless systems this is usually the case for users, nodes, miners and developers. It was argued they cannot be held legally *accountable* because they may be unaware of their activity, which is constrained by code.[129] Consensus on this classification, however, has yet to be reached. Regarding miners and developers, well-known hard fork cases (*e.g.*, Ethereum, Bitcoin) highlighted the power they may exert even within permissionless systems.[130] This circumstance is most likely to occur when there is a participation of mining pools – *i.e.*, groups of miners that join their computational power to increase the likelihood of mining a block.[131]

Indeed, *native* actors are not essential for the system to exist, but they originate within the cryptocurrency domain. Examples may refer to mining pools, a subset of entities that provide

[126] Desmond DB, Lacey D, Salmon P (2019), pp 481-482
[127] Capaccioli S (2020). The blockchain-based subset is likely to influence the discussion more than others. The approach employed here is teleological – *i.e.*, concepts are mentioned if impactful for this work, notably regarding the *accountability* of those active in the ecosystems.
[128] In PoS, validators are known as *forgers* and ensure cooperation by putting holdings at *stake*
[129] Capaccioli S (2020), pp 472-474. Arguably, the only approach is "code as law", explored in Chapter 6
[130] A *hard fork* is a substantial change of the protocol of a blockchain network. Consequently, previously blocks and transactions are made invalid. It requires all validators to upgrade the software.
[131] Since mining pools are usually managed by companies/individuals who relieve other participants from managing a full node, they are deemed *native* stakeholders. Walch A (2019), pp 52-58. Walch A (2018), p 5. Arruñada B (2018), pp 59-61

wallets and mixing services, consensus systems other than PoW. Finally, *metamorphic* actors are providers of services that can also be provided outside of the cryptocurrency sphere.[132]

1.3.2. Multi-layered dynamics: remarks on access control and governance

The actual operational weight exerted by the players active in DLT-based ecosystems is influenced by (i) the overall network and platform structure, and (ii) the link with external *off-chain* elements or *other on-chain layers* belonging to the same ecosystem. Hence, leading factors to consider pertain to (a) the *off-chain* or the *on-chain* world, and (b) the *network* or the *application/protocol* level. Significant misunderstandings stem from the phenomenological integration between these elements, which exerts a great impact on *accountability*. In this respect, it is high time for a specification. On the one hand, although *DLT* and *blockchain* are often used interchangeably, blockchain is a subset of DLTs and other types of distributed ledgers exist. This approach poses limitations and overlooks alternative structures, such as IOTA's Tangle, based on a Directed Acyclic Graph and designed for the Internet of Things (IoT) industry. Nonetheless, the IoM is significantly based on blockchains.

On the other hand, in the dynamics of a blockchain ecosystem some distinctions impact regulatory methodologies and enforcement actions. A distributed ledger system can be *public* (*i.e.*, "accessible to the public for use") or *private* (*i.e.*, accessible "only to a limited group of DLT users", hence the label *consortium* blockchains when multiple organisations are involved).[133] Meanwhile, it can be *permissionless* or *permissioned*; in the first case to maintain and operate a node it is not necessary to have permissions, which are required in a *permissioned* system. [134] A *permissionless* system such as the Bitcoin network is a decentralised ledger "open to anyone validating blocks, without needing permission from any authority", while in *permissioned* ones "users validating blocks shall be authorised".[135]

While these are conceptual distinctions grounded on architectural differences, the phenomenology of these ecosystems shows that even when network self-organisation is pursued, and control is supposed to be exerted by the algorithms, less visible and self-evident forces influence the management of these structures. Some of them depend on the relationship between the actors involved in the network and exerting impact on it. This group of entities is called an

[132] Capaccioli S (2020), pp 474-475. Arguably, their involvement with cryptoassets is just a diversification of their non-crypto activities, which means they can be addressed by traditional legal means.
[133] ITU-T FG DLT (2019), p 5
[134] Ibid, p 4. A *permission* refers to "intended allowable user actions (e.g., participate, read, write, execute)".
[135] Ibid, p 8. The topic is further explored in Chapter 2

"ecosystem". These entities belong to one among four areas: (a) hardware (*e.g.*, nodes), (b) business (*e.g.*, developers, users, miners, investors), (c) software development (*e.g.*, financial, semi-financial, non-financial), (d) protocol development (*e.g.*, developers, academia).[136]

1.3.3. Decentralisation and non-centralisation: a matter of degree

The *decentralised* element of the IoM played a key role in supporting the socio-economic claims that accompanied its uptake, while it troubles regulatory frameworks that rely on *accountability*. However, the development of the IoM shows how these ecosystems are increasingly complex and do not always mirror the traditional image of a DLT-based monetary system – *i.e.*, the Bitcoin network. Values and technologies, no matter how closely linked at initial stages, develop independently, especially when a plethora of actors pursue several goals by employing similar tools. It follows that IoM discourse is affected by over-generalisations.

In this respect, *decentralised* is not always an accurate description of DLT-based STSs. While the underlying network is *distributed* and features a P2P architecture, with nodes communicating in a direct and equal way, a system is *decentralised* only when it is not controlled by a (single) central authority – *i.e.*, no single user controls the data. In most legal fields, control can be exerted in different ways. In the DLT context, it can be measured using various criteria, and the quality of being *(de)centralised* is dynamic, multi-level and non-binary. Hence, the term *non-centralised* is more appropriate.[137] In this way, one can avert the risk of referring the concept to both the network itself and internal power dynamics (*i.e.*, governance). Indeed, "blockchains are not by definition decentralised. Rather, they can be centralised at both the software and the hardware levels. First, one may have a blockchain that runs only on very few nodes, which can all be located in the same room. Second, even when DLT is highly decentralised at hardware level, it can still be centralised at the software governance level".[138]

A recent analysis conceptualised the degree of *decentralisation* of a given blockchain by identifying nine layers: (i) "real space", (ii) cyberspace and the Internet, (iii) blockchain and ledger, (iv) blockchain infrastructure, (v) governance mechanism, (vi) applications, (vii) users, (viii) interaction/competition with other blockchain ecosystems, (ix) interaction/competition

[136] ITU-T FG DLT (2019b), pp 2-4. *Mining pools* are an example of a less-evident influential factor. Even in permissionless blockchains there is power recentralisation when individual actors are coordinated by a *pool manager*. This generates key governance consequences. As non-expert users seem to trust developers considerably, computer scientists and miners become *partially trusted fiduciaries* (Walch A (2018), pp 9-10. Szabo N (2017)).
[137] Quiniou M (2019), pp 6-11. Schrepel T (2021), pp 24, 56. Allen S, Capkun S, Eyal I et al (2020), p 16. Bodó B, Giannopoulou A (2019)
[138] Finck M (2019a), p 19

with other technologies, services and applications. Hence, a blockchain ecosystem is a "set of levels".[139] With regard to governance, even in *permissionless* ledgers deemed *fully decentralised* (*e.g.*, Bitcoin), an evaluation of *decentralisation* cannot disregard the possible presence of embedded governing structures, who ensure a degree of *(re)centralisation*. Furthermore, *consortium* systems (*e.g.*, Corda, Hyperledger) are *permissioned*, but labelled as *semi-decentralised*, because centrally coordinated changes are allowed. Parallelly, *centralised* systems can be equipped with features that limit the overall *decentralisation*.[140]

Indeed, there is an interplay of different dimensions. Beyond the specificity of *decentralisation* analyses, if one fails to notice the complexity of the notion, the resulting ambiguity may be exploited to infer *unaccountability* from a perceived diffusion of power. This gives rise to the "veil of decentralisation", mirroring the "corporate veil" that severs rights/duties of a corporation from those of its shareholders.[141] In this respect, "the degree of centralisation reflects the accumulation of interacting decisions and tradeoffs at various layers", and "the fluctuating nature of a system's level of decentralisation is worth emphasising, as every passing second could bring massive changes to it. So many factors affect how decentralised a blockchain system is, so a change to any of those factors can shift the blockchain on the decentralisation spectrum".[142] Hence, the *centralisation* vs. *decentralisation* debate does not account for the structure of STSs, which are, ultimately, governed by human behaviour.[143]

The topic can be represented visually. A study addressed the evolution of cryptocurrency systems as "interconnected systems of agents", quantitively measuring their *centralisation*.[144] The analysis focuses on the interactions of network entities through transactions, representing the *nodes* and using direct links to represent transaction flows. The work considered the effect exerted by (i) clustering;[145] (ii) degree distributions;[146] (iii) core-periphery structure;[147] (iv)

[139] Schrepel T (2021), pp 59-62. The author defines *decentralisation* as "a dynamic and multi-level concept that measures the autonomy enjoyed by a given subject in determining its competence", where *competence* means "the ability to determine the spheres of action within which a given individual can decide" (Ibid, p 56)
[140] Casey M, Crane J, Gensler G et al (2018), p 6. Allen A, Capkun S, Eyal I et al (2020), pp 18-21
[141] Quiniou M (2019), pp 10-11 and 28-29
[142] Walch A (2019), p 14
[143] De Domenico M, Baronchelli A (2019), p 1
[144] Campajola C, Cristodaro R, De Collibus FM, Yan T, Vallarano N, Tessone CJ (2022), p 1. The study investigates the networks Bitcoin, Ethereum, Bitcoin Cash, Litecoin, Dogecoin, Monacoin and Feathercoin.
[145] *Clustering* is explored in Chapter 3 and shows the economic structure of these networks. Switching to an entity-based perspective shows a *centralisation* process, proven by a decrease in the average amount of addresses per entity, in conjunction with the use of cryptocurrencies as speculative assets and the advent of big intermediaries. Consistently, *centralised* platforms are increasingly used to enter the systems (Ibid, pp 3, 7).
[146] A node's degree shows the number of counterparts and measures the importance of the entity within the given network. The distribution of degrees shows the way in which the network functions (Ibid, p 3).
[147] The minority of nodes are highly interconnected, and the others are connected to the *core* and scarcely linked to peripheral nodes. This resembles "other trading networks from traditional economic and financial systems, and as time goes on the cores become increasingly smaller compared to the total size of the network" (Ibid, pp 4, 8).

mining concentration;[148] (v) wealth inequality and spatial distribution.[149] It shows major cryptocurrencies are considerably *centralised* despite a supposed technological *decentralisation* and are transforming into something different from their original design. Indeed, the narrative of *decentralised* payment solutions, over which financial institutions exert no power in terms of money creation and distribution, is largely false: both miners and intermediaries exert considerable powers both from a technical and an economic perspective.[150] Likewise, an analysis of the distribution of voting powers in non-custodial projects of Decentralised Finance (DeFi) suggested a significant degree of concentration.[151] Indeed, in this field *centralisation* tendencies were deemed inevitable due to structural elements (*e.g.*, consensus mechanism) and governance needs.[152] The DeFi ecosystem is addressed in Chapter 2.

Given the difference between the ideological *decentralisation* and its actual implementations, legal experts ought to tread warily. Indeed, treating a system as thoroughly *decentralised* when it is not – *i.e.*, when it houses significant control points – leads to incorrect statements concerning *accountability*.[153] On the contrary, the term *non-centralised* allows for more room to consider that even if the network features no single central authority, some stakeholders may exert influence on the internal governance system – *e.g.*, at times they may be in a privileged position to edit code as well. This means this set of actors ought to be considered as potential access points to extend regulatory reach over these ecosystems.[154] In this respect, applying a critical approach may mitigate a dangerous regulatory tendency identified in the area of new technologies. The complexity of these domains may lead to the temptation of regulating "by streetlight" – *i.e.*, making regulatory determinations limiting the scope to what can be easily

[148] Since the analysed networks are based on PoW, ledger's consistency needs mining power to be both *distributed* and *decentralised*, to avoid a "51% attack" where the majority adds false information to the ledger. The "Nakamoto index" measures the distance from possible "51% attacks". Mining power is worryingly concentrated and there is stark wealth inequality, incompatible with the narrative of *decentralised* P2P systems (Ibid, pp 5, 8).
[149] It concerns the distribution of tokens among entities, where wealth refers to the balance held by an address (or cluster). Most wealth is in the hands of relatively few entities, in the immediate vicinity of miners (Ibid, pp 6-7).
[150] Ibid, pp 7-8
[151] Barbereau T, Smethurst R, Papageorgiou O, Rieger A, Fridgen G (2022), pp 6050-6051
[152] Aramonte S, Huang W, Schrimpf A (2021), p 21. The authors argue that even in DeFi projects full decentralisation seems to be nothing but an illusion. This is because "platforms have groups of stakeholders that take and implement decisions, exercising managerial or ownership benefits" (Ibid, p 33). Meanwhile, "operating in a decentralised way is not incompatible with market power-creating reconcentration" (Zunzunegui (2022), p 10).
[153] Walch A (2019), p 29. Walch A (2018), p 3
[154] In this respect, "the view that nobody controls the network cannot be accepted, because each network is controlled by somebody: by a more or less wide group of community members, coordinated by software (code) and the developed rules of off-chain governance" (Karasek-Wojciechowicz I (2021), p 6). Likewise, the abovementioned groups of actors that take and implement decisions in DeFi projects, together with their governance protocols, were described as natural entry points for policymakers (Aramonte S, Huang W, Schrimpf A (2021), p 33).

seen or (mis)understood.[155] I argue the most dangerous risk is not that of building frameworks around more visible sides of the IoM, but that of incorporating common misconceptions.

1.4. A World with Many Faces: Theory and Practice at Ever-Changing Crossroads

The dynamic and multi-layered features of the IoM hinder the attempts to conceptualise its defining traits. This worryingly leaves the cryptocurrency space vulnerable to being (mis)defined in different ways by various actors, mainly depending on their underlying motive. Although a portion of this dilemma is arguably inherent to the composability of the set of technologies that compose the IoM, I argue it is paramount to limit the negative effects on the efforts to devise regulatory strategies that fit the target domain. From this viewpoint, the *disintermediation* element, originally crowning blockchain technologies and relevant value exchanges, exemplifies the value of scrutinising the adequacy of given regulatory frameworks against the actual characteristics of the sphere and its evolution.

1.4.1. Disintermediation riddles

In light of the previous sections, I argue it is crucial to test the narratives of *decentralisation* and *disintermediation* against the phenomenology of the IoM. In other words, "separate fact from fiction".[156] This critical approach leads to challenge the description of all IoM-related exchanges as *disintermediated*, as opposed to markets intermediated by financial institutions.[157] What makes this assessment more complex is that these features are not only influenced by matters that are internal to each platform. Indeed, a very important role is played by the ways in which different networks communicate – *e.g.*, the ways in which they execute transactions, among themselves or with the traditional financial system – and the actors that enable this. Stakeholders such as *cryptocurrency exchanges* or *providers of wallet services* are the most common way to interact with the IoM space, where "most exchanges are centralised third parties that must be trusted with the custody of users' cryptocurrency balances".[158] These entities are acting as "chokepoints" and "*(re)centralisation* points".[159] Indeed, the history of the Internet itself can be conceptualised as "the history of the recentralisation of networks

[155] Walch A (2018), p 25
[156] Finck, M (2019a), p 19
[157] New forms of intermediation emerged, also in an automated fashion (Quiniou M (2019), p 18)
[158] Allen A, Capkun S, Eyal I et al (2020), p 26
[159] Their advent bridged the gap between cryptographic keys and human identities (Ibid, p 26)

which were initially designed to be decentralised. DLTs are no exception to this rule".[160] Further, a substantial *recentralisation* can be witnessed at different layers – *e.g.*, mining power, core code developers, major exchanges –, which generates "unexpected recentralisation of a technological infrastructure designed to be decentralised out of pure ideological reason".[161]

Concurrently, however, in the past years the advent of specific applications, products, and services – *e.g.*, decentralised exchanges (DEXs), other types of DeFi projects, self-hosted wallets or atomic swaps, addressed by Chapter 2 – can be seen as a transformation of the IoM towards *true disintermediation*. These events can be interpreted in two complementary ways: as a sign that there is room to challenge the actual *disintermediation* degree of previous more traditional (re)centralised IoM dynamics, and that the world of cryptocurrency transactions is developing beyond gatekeepers bringing *disintermediation* to a new level. The importance of these considerations is overarching in terms of regulatory strategies, given that aspects such as AML/CFT/CPF are still gatekeeper-based and largely rely on the "active cooperation" of a set of stakeholders, as explored in Chapter 4. Meanwhile, the feasibility of handling *true disintermediation* by regulatory means is highly debated and, may be limited to outlawing certain activities or imposing regulatory burdens on stakeholders that may or may not have the capacity to exercise actual "control" over the relevant networks. In this respect, the concept of *embedded regulation*, together with the relevant value and challenges, is addressed in Chapter 6.

1.4.2. The (r)evolution of (global) stablecoins and digital fiat money

A major hindrance to the public spread of cryptocurrencies lies in the high volatility of their value, which generates significant and unexpected fluctuations. Volatility prevents the "first wave of cryptoassets" from efficiently serving the three traditional functions of money: store of value, means of payment, unit of account. Over the years, this issue has been addressed by IT companies and financial service providers, mostly in the form of creating *stabilisation* mechanisms by backing the value of their coins with (an)other (less volatile) asset(s). The resulting instruments – still belonging to the cryptocurrency sphere and, according to the criteria employed by this work, to the IoM ecosystem – were labelled *stablecoins*, and are also referred to as *asset-referenced tokens*.[162] They were defined as a type of cryptoasset that aims "to

[160] Bodó B, Giannopoulou A (2019), p 4
[161] Ibid, p 12
[162] European Central Bank (2019), pp 1-2. G7 W.G. on Stablecoins (2019), pp 1-3. Bullmann D, Klemm J, Pinna A (2019). Dabrowski M, Janikowski L (2018)

maintain a stable value relative to a specified asset, or a pool or basket of assets".[163] Indeed, stablecoins are pegged to another asset, that can be: (a) another currency or set of currencies – in this case, they are known as *tokenised funds* (*e.g.*, Tether); (b) securities and/or commodities – *i.e.*, *off-chain collateralised* (*e.g.*, gold); (c) other cryptoassets – *i.e.*, *on-chain collateralised*; (d) expectations users have of future value – *i.e.*, *algorithmic stablecoins*.[164]

As far as terminology is concerned, the FATF highlighted how *stablecoins* are not a clear legal and/or technical category. In practice, they can be "*retail* or *general purpose*" or "*wholesale*", depending on the target user(s); either anyone can access them, or only a selection of actors can.[165] From a legal perspective, each category of stablecoins can be classified according to whether it provides for *decentralisation* of responsibilities, and *accountability* of the issuer. In general, these instruments are "inherently at the edge of the decentralised crypto world in the sense that the price stabilisation aspect, whatever its form, usually requires some kind of trusted intermediation or other centralised infrastructure".[166] For *tokenised funds* (whose value is backed to currency) and *off-chain collateral* (backed to other off-chain assets) responsibilities are *centralised*, and the issuer can be held *accountable*. On the contrary, for *algorithmic stablecoins*, linked to on-chain assets, no party can be held *accountable,* and responsibilities are *decentralised*. A hybrid situation relates to *on-chain collateral*, pegged to the expectations mentioned above; there is no *accountable* issuer although responsibilities may not be *decentralised*. The more innovative potential is embodied by these instruments, the less it is possible to control the volatility risk– *e.g.*, *algorithmic stablecoins* feature a high volatility risk.[167]

Stablecoins have not only attracted the attention of the public and regulators around the world, but also spurred companies and organisations to explore the underlying concepts in order to create new ecosystems to manage worldwide payment transactions. When stablecoins have this potential, they are addressed as *global stablecoins*. Their nature emerges from the wording of the upcoming MiCA Regulation, according to which "some asset-referenced tokens and e-money tokens should be considered significant when they meet, or are likely to meet, certain criteria, including a large customer base, a high market capitalisation, or a high number of transactions".[168] These arrangements are usually sponsored by the private sector – *e.g.*, big

[163] Financial Action Task Force (2020b), p 6. Financial Stability Board (2020), p 4
[164] European Central Bank (2019), pp 1-3. The MiCA Regulation defines *asset-referenced tokens* as those aiming "to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies" (Article 3(1)(3)); and *e-money tokens* as those that purport "to maintain a stable value by referencing to the value of one official currency" (Article 3(1)(4)). Council of the European Union (2022a)
[165] Financial Action Task Force (2020b), p 6. G7 W.G. on Stablecoins (2019), pp 1-2
[166] G7 W.G. on Stablecoins (2019), p 24
[167] European Central Bank (2019), pp 3-6, and 9
[168] Council of the European Union (2022a), Recital 41b

technology, telecommunications or financial companies.[169] It is primarily the case of the Libra/Diem initiative, first announced by Facebook and the other 27 members of the Libra Association in June 2019. A second whitepaper followed in May 2020, but the project was abandoned in 2022. The initiative was perceived as a controversial monetary revolution from various technical, political and legal angles, and is further addressed in Chapters 4 and 5.

The advent of *global stablecoins* showed the cryptoasset sphere could potentially threaten financial stability due to the exploitation of network effects.[170] Hence, as per MiCA's text, when "significant" *asset-referenced* or *e-money tokens* "could raise specific challenges in terms of financial stability, monetary policy transmission or monetary sovereignty should be subject to more stringent requirements than other asset-referenced tokens or e-money tokens".[171] Accordingly, when within a single currency area an *asset-reference token* becomes widely used as a means of exchange – *i.e.*, number and value of transactions per day is higher than 1,000,000 and EUR 200 million, respectively – its issuer should be required to reduce the activity level".[172] Global stablecoin adoption was also deemed to increase the risks of *anonymity* and ML/TF, but most dangers would arise from arrangements allowing for P2P transactions via unhosted wallets, addressed by Chapter 2. The intensity of these concerns depends on the design of each use case (*e.g.*, *(de)centralisation* degrees of their functions, governance features), but a *centralisation* tendency is foreseeable.[173]

If the launch of Bitcoin marked the beginning of a new digital era, the Libra/Diem initiative revolutionised the ideological perception of the IoM space. The clash between the *disintermediated* (in theory at least) and *decentralised* (supposedly) ecosystems and the evolution of the domain reached a new level with the investigations into digital fiat money known as CBDCs, addressed in Chapter 4. Although one may argue they fall outside the scope of the IoM, the distinction is not clear-cut; seemingly, projects of cryptocurrencies, stablecoins and CBDCs are situated on a spectrum of ideological and architectural design choices. As anticipated, this work employs a broad concept of IoM, to include the entire set of cryptocurrency ecosystems and to refer to them collectively and techno-economically. In this respect, the IoM includes the part of the IoV related to *payment tokens* but also *payment-type cryptoassets* issued on permissioned blockchains that do not share Bitcoin's idea of *disintermediation*.

[169] Financial Action Task Force (2020b), p 6
[170] G7 W.G. on Stablecoins (2019), p 12
[171] Council of the European Union (2022a), Recital 41b
[172] Ibid, Recital 42d
[173] Financial Action Task Force (2020b), pp 11-14

1.5. Looking for Benchmarks: Backing Phenomenology with Conceptual Frameworks

Against the backdrop of such complexity, it is crucial to devise an appropriate global methodology – *e.g.*, for analysis, assessment, research, regulation, and enforcement. From this perspective, it is not enough to acknowledge the aspects that influence a specific network with a cross-disciplinary approach, but there is a need to provide yardsticks different stakeholders (and the present work) can use it to ground analyses, application initiatives, conclusions. The risk is otherwise that any finding could not be re-utilised, as it would not be possible to reconstruct the underlying process and the benchmarks taken as foundations of a specific suggestion. While the structure of this dissertation aims to narrow the gap between legal and technological knowledge to pursue informed regulatory decisions, it seems unfeasible to ask all legal experts to develop a sound contextualised technical expertise. Moreover, cryptoassets are not only constantly evolving, but are also relevant to more and more legal domains, which makes it even more unrealistic to expect a sufficient evolution of all expertise domains involved.

Thus, I argue flexible *and* sound theoretical frameworks can help understand the core elements of these worlds, in compliance with the scope of each action. This is in line with the goal of mitigating the risk that regulatory solutions, and underlying research findings, become technologically outdated soon after they are devised (or even before that): the "risk of overfitting".[174] In this respect, Chapter 6 explores the difference between rules-based and principles-based regulation, where principles-based rules were found to allow for flexibility and avoid never-ending regulatory vicious cycles.[175] I introduce two conceptual benchmarks below.

1.5.1. Regulation and the IoM: reaching beyond the complexity

The advent of the IoM marked a change in the way monetary transactions are envisioned. Distributed ledgers and blockchain introduced not only new mechanisms to handle major drawbacks of traditional means, but also seemingly safe alternatives to *intermediation*. The idea that computer systems, networks and algorithms can replace safeguards provided by trusted and regulated firms and professionals, however, is only a part of the picture. Indeed, the "first wave of cryptocurrencies" seems to have partially failed to deliver on what was promised, and their use has not met the expectations both quantitatively and qualitatively. Although a shift is to be

[174] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), p17
[175] Black J, Hopper M, Band C (2007), p 193

detected in the perception of what monetary transactions should be, urging the setup of systems with less oversight, remarkable side effects have also arisen. Apparently, the price of *disintermediation* is higher than many people are willing to accept.

It was argued above that a major problem of cryptocurrencies is their unstable value. In this context, one can see clearly how technology and ideology can depart, and how similar implementations can address opposite needs. While it would not be possible to present the same argument for all technologies, in DLTs there is a remarkable fluidity in the way they can be shaped and tailored, and their properties exploited. As far as stablecoins and CBDCs are concerned, it is crucial to examine their interdisciplinary impacts, and the attention paid to them by institutions and entities piloting initiatives in this field. The AML/CFT/CPF domain represents a noteworthy benchmark, as many actors engaged in the implementation of these instruments are subject to compliance regimes, as addressed in Chapter 5. In some cases, the deployment of DLTs is just a diversification of traditional monetary activities. Even when this is not the case, consortia are often created with the participation of entities with financial expertise. This leads to understanding how regulatory frameworks can be shaped to suit the needs of traditional cryptocurrency instruments, albeit one should not overlook the fact that the "second wave of cryptocurrencies" features striking differences when compared to the first one.

A partial exception is to be found in retail CBDCs. Although central banks are obviously financial institutions, in some digital cash projects the possibility to engage in P2P transactions outlines the re-emergence of a new way for individuals to dispose of monetary instruments. The following chapters focus on limitations and conceptual issues stemming from this approach, as did most pilot initiatives. Nonetheless, there is a tendency towards giving a greater share of freely disposable transaction power to the public. When it does not originate from institutions, it stems from technology itself, where certain digital skills are required to exploit it. From an AML/CFT/CPF perspective, it is necessary to evaluate regulatory impacts of phenomenological, ideological, and socio-technical distinctions featured by IoM applications.

1.5.2. The IoM as an ecosystem of socio-technical (eco)systems

I introduced above the qualification of cryptocurrency ecosystems as STSs, the elements of which were summarised by arguing that "the blockchain looks purely technical but, […] like the Internet, it is sociotechnical in nature. Humans are essential to its performance: proof of work systems that support major platforms depend on miners, decisions about investing in blockchain hardware and software are made by humans, people are critical to blockchain

operations in a variety of contractor and curator roles, and it is on the basis of human subjectivity that blockchains rise and fall".[176] Meanwhile, wallets linked to the network of nodes, users and miners, exchanges and mixers, were described to be all cooperating "within a complex system of social and informational relationships".[177]

Generally speaking, an STS is an articulated assemblage of technical and social elements in a given environment, interacting with one another in diverse ways and oriented towards a specific goal. Within an STS, various components are connected: *actors*, *technology*, *structure*, *tasks*.[178] In a nutshell, multiple actors with different needs and backgrounds cooperate through an organisational structure to deploy a technology to perform specific tasks. Moreover, the level of abstraction at which an STS can be observed can vary. If – at a general level – cryptocurrency laundering and mobile banking can be viewed as STSs, the same is true for concrete technology implementations in specific socio-geographical and digital contexts.[179] Regardless of its conceptualisation, leveraging the STS notion is key from a methodological perspective. While technical and sociological perspectives view innovation from different angles, the key idea in socio-technical approaches is that "we should study the interactions between technological and social changes to enhance our understanding of innovation and that technology and social environment develop in a process of mutual shaping".[180]

The conceptualisation of cryptocurrency systems as "complex systems" is mirrored by considering them and the IoM as *ecosystems*. Ostensibly "cryptolaundering occurs within a complex sociotechnical system. Such systems are defined as systems comprising human, technological and technical elements working together to achieve a shared goal of some sort […]. To understand the behaviour of complex sociotechnical systems, a so-called systems approach is required, which entails taking the overall system as the unit of analysis and examining the interactions between components (as opposed to only examining the components themselves). As such, a complex systems thinking perspective is required when attempting to understand and prevent cryptolaundering processes".[181] From an architectural standpoint, the IoM can be defined as an ecosystem of *interconnected* STSs, as it is composed of various cryptocurrency ecosystems that may interact with one another. Indeed, the Ethereum platform itself was

[176] Werbach K (2019), pp ix-x
[177] Desmond DB, Lacey D, Salmon P (2019), p 487
[178] Borrás S, Edler J (2020). Kopackova H, Libalova P (2017), citing Leavitt H (1965)
[179] *E.g.*, Desmond DB, Lacey D, Salmon P (2019). Stephen A, Christopher R, Huseyin D et al (2016). Gonsalves T, Vaidyanathan L, Jhunjhunwala A (2012). De Domenico M, Baronchelli A (2019)
[180] Meijer A, Thaens M (2018), p 366
[181] Desmond DB, Lacey D, Salmon P (2019), pp 481-482

described as one element that belongs to an ecosystem of (interconnected) STSs.[182] In practice, the degree of their (direct) interconnection is strongly linked to the issue of blockchain *interoperability*, which is addressed in Chapters 2 and 5.

The regulatory value of the socio-technical concept lies in embracing the elements at play when devising a strategy to approach these ecosystems. The concurrent presence of social and technical components in the qualification of a cryptocurrency transaction as *anonymous* will be explored in Chapters 2 and 3. Without this sensitivity, the risk is to reach conclusions refuted by phenomenology. Accordingly, the socio-technical methodology – *i.e.*, a "systems approach", the consideration of the socio-technical components of IoM ecosystems when evaluating their features – is used throughout this work, and explored in different directions.

1.6. Conclusions

In this Chapter I provided a preliminary outline of the foundations of the ecosystems that form the scope of this analysis. I introduced the traits of the IoM sphere by exploring multi-layered aspects, ranging from the drivers underlying the deployment of the combination of technologies that led to the advent of Bitcoin, to the role played by various stakeholders and architectures. Accordingly, the chapter outlined the background against which the concepts of IoM and IoV were devised, leveraging P2P transfers and *tokenisation*, up to the advent of the "second wave of cryptocurrencies" (*i.e.*, stablecoins) and CBDCs. Relatedly, I accounted for the differences among these initiatives and focused on providing a definition of IoM. In particular, this research embodies a broad concept of it, including the part of the IoV that relates to "payment tokens". Relatedly, in this chapter I highlighted the importance of terminology and disambiguation efforts, and I did so by leveraging definitional remarks on cryptoassets, tokens, and relevant taxonomies, as benchmarks for grounding cross-disciplinary remarks.

The architectural interpretation of IoM ecosystems is mostly token-based, which may suggest they are (purportedly) *anonymous* or *transparent* only due to how tokens are construed. On the contrary, other aspects are to be considered, and actual risks mostly relate to the way the systems that generate and exchange them are construed and governed. Thus, the chapter explored the landscape in which cryptocurrencies are transferred by deploying a teleological and *accountability*-based approach. Moreover, it explored a set of elements portrayed by IoM ecosystems to provide theoretical yardsticks for AML/CFT/CPF measures. I addressed

[182] De Domenico M, Baronchelli A (2019)

different levels of features, underlining the nature of the IoM as an ecosystem of interconnected socio-technical ecosystems, the need to focus on the interplay between the different dimensions, and paying special attention to the concept of *non-centralisation*. Parallelly, I disambiguated the notion of *disintermediation* and outlined new trends while heeding the value of the definition of IoM. Finally, I outlined methodology benchmarks to address IoM ecosystems from a regulatory perspective while heeding conceptual, ideological, and technical evolutions.

Some important threads can be identified in this chapter: (i) the role of terminology in pursuing regulatory clarity, (ii) the development of taxonomies to enable interdisciplinary cooperation, (iii) the selection of yardsticks on which to ground legal reasonings, (iv) the disambiguation of IoM-related misconceptions, (v) the interplay of theoretical schemes and empirical phenomena. Its findings can be seen as the first steps towards avoiding the "streetlight" effect when assessing regulatory solutions for cryptocurrencies in the AML/CFT/CPF domain.

2. Disintermediation and Anonymity: Balancing Privacy and Misuse Risks

"*There is no universal model that could be used to assess the anonymity of different cryptocurrency implementations. Modelling anonymity of cryptocurrencies involves a complex process of studying different notions of anonymity and their relationships and dependencies*".
Amarasinghe N, Boyen X, McKague M (2019)

2.1. Introduction

Chapter 1 introduced the principles underpinning IoM ecosystems, showing how their qualification as the realm of *disintermediation* is not as clear-cut as advertised. Indeed, assessing IoM's *disintermediation* requires the newest developments to be considered. On the one hand, most legal and socio-economic impacts exerted by blockchain technology lie in reducing the role of "trusted" intermediaries – better, replacing "inter-individual" trust with one that is "systemic" and "algorithmic".[183] On the other hand, however, the role played by centralised exchanges (CEXes) and other service providers, and the development of stablecoin and CBDC projects, testify to the significance of intermediation in the cryptocurrency space, and of an increasing interplay between *intermediated* and *disintermediated* scenarios – *e.g.*, between CEXes and DEXes, or service providers intermediating access to DEX platforms.

Indeed, the IoM is populated by a considerable number of intermediaries, consisting of both new types of entities – *e.g.*, cryptocurrency exchanges, brokerage platforms –, and traditional financial and payment institutions offering cryptocurrency-related services. Against this backdrop, most users are still interacting with the IoM through intermediaries, and not in a P2P fashion. Given this "continuing mediation", *disintermediation* was described as a possible myth.[184] Nonetheless, not all entities operating as intermediaries in the cryptocurrency sphere are within the scope (and reach) of regulation, and in principle these entities are not even needed to transact in cryptoassets. On the contrary, although AML/CFT/CPF regulatory guidelines and standardisation efforts have traditionally focused on the "on- and off-ramps" – *i.e.*, gateways between cryptocurrency activities and the traditional financial system – over time the

[183] Quiniou M (2019), pp xiv-xv
[184] Herian R (2019), p 113

domain has evolved significantly towards a variety of innovative products, services, business models, interactions, including virtual-to-virtual transactions.[185]

Although the opportunities offered by DLTs are plentiful, their advent has been channeled into a narrative of pervasive technological change and socio-economic repercussions.[186] The expression "blockchain hype" has come to describe the enthusiasm towards the application to every aspect of life of a technology allegedly able to end dilemmas ranging from governmental corruption to financial exclusion.[187] The main disruption lies in enabling network's participants to agree upon and record information without the need to rely on a trusted central authority. The absence of a "single point of truth" is counterbalanced using encryption and methods to add data to the ledger after the network has agreed on it – *i.e.*, the "consensus mechanisms".[188]

The level of *disintermediation* enabled by DLTs in sectors traditionally grounded on the regulatory and supervisory role of intermediaries challenges laws and regulations.[189] Meanwhile, the advent of Bitcoin showed how encryption also protects the *identity* of users and transactions.[190] Indeed, the idea of enabling *anonymous* and *pseudonymous* transactions seems inherent to the cryptocurrency sphere as a realm of individual freedom, which generated tensions related to the application and enforcement of regulatory regimes against misuses of the financial system. However, the entangled relationship between *anonymous* exchange of information and the digital sphere had been debated well before blockchains, and the reason can be phrased simply: on the one hand *anonymity* is conducive to safeguarding the right to privacy, data protection and other civil liberties, while on the other hand *lack of identification* hampers investigation, enforcement and *accountability*, hence is a fertile ground for illegal behaviour.[191]

It is not straightforward to grasp the meaning of the terms used in the debate. Besides the frequent reference to *privacy*, there is often an equation between *anonymity* and *lack of identification*. But one may wonder: does transacting *anonymously* equate to transacting *privately*? Is a transaction *private* (only) when it is *anonymous*, and in turn is it *anonymous* (only) when there is *no identification*? From parallel perspectives, *transparency* is deemed one of the defining traits of blockchain technologies. Does this originate a paradox?

---

[185] Financial Action Task Force (2021e), p 7
[186] Finck M (2019a), p 211
[187] Walch A (2017), p 13
[188] Schrepel T (2021), pp 18 ss
[189] Nonetheless, even if disintermediation equals to the (partial) elimination of intermediaries, it does not necessarily imply the absence of mediation, that can be automated. A key impact of Internet platforms was indeed the gradual replacement of physical intermediation with a digital one. Quiniou M (2019), p 52
[190] Schrepel T (2021), p 35
[191] Nicoll C, Prins CJEJ, van Dellen MJM (2003), pp 6-8

2.1.1. Encryption, cyberspace anonymity and the IoM

The Bitcoin network was the first large-scale embryonic showcase of an economic system in which to participate directly and *anonymously*, with no need of intermediaries and authorities. Although the extent to which Nakamoto's work embodied an ideologic and financial orientation is up for debate, the idea of exchanging value in an *anonymous* way was addressed throughout the whole history of telecommunication. The transmission of funds by electronic means, first by cable and later over the Internet, was introduced in the second part of the twentieth century, and cryptographic techniques and encryption – *i.e.*, the application of cryptography for a message to be understood only by the intended readers – started to be implemented to safeguard its security.[192] Most importantly, after public-private key encryption was invented, in 1978 the RSA algorithm multiplied its applications and created digital signatures that were highly resistant to forgery.[193] It is the combination of public-private key cryptography and digital signatures that planted the theorical seed for "electronic cash, pseudonymous reputation, and content distribution systems, as well as new forms of digital contracts".[194] Hence, encryption, that can be applied to obtain *anonymity*, played a key role in the development of the IoM.

This line of cryptographic research partially overlaps with a broader cyber-libertarian movement that was underlining surveillance risks arising from the fast development of the Internet in sharing information, if left in the controlling hands of governmental powers.[195] There was a strong belief individuals' privacy rights were under existential threat by the hands of the excessive power exerted by governments and corporations.[196] Trying to find a privacy-preserving solution, in 1988 Timothy C. May, an electronic engineer, argued in his Crypto Anarchist Manifesto that computers could allow *anonymous* communication between individuals and groups.[197] Hence, people could "exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity" of their counterparty. Similarly, he claimed these interactions could be *untraceable*.[198]

---

[192] Geva B (2019), p 24. In cryptography, the status in which only the intended reader can read and process stored or transmitted data is called "secrecy".
[193] De Filippi P, Wright A (2018), pp 14-15. The RSA algorithm generates a mathematically linked set of public and private keys by multiplying two large prime numbers.
[194] Ibid, p 16
[195] Magnuson W (2020), p 17
[196] Ibid, p 34. Cyberpunks argued that "without proper checks and balances, the deployment of modern information technology would narrow the sphere of personal privacy, resulting in pervasive government and corporate surveillance". De Filippi P, Wright A (2018), p 18
[197] May TC (1988)
[198] Ibid

Anonymous cash and *untraceable* payments fitted cyber-libertarian goals perfectly and seemed necessary to attain them.[199] Indeed, encryption does not suffice to save virtual interactions from the monitoring eye of the Government, due to the need to rely on a bank.[200] The work of David Chaum, founder of the International Association of Cryptologic Research, is a great example of early privacy-preserving discussions. In early 1980s, he proposed *pseudonymous* solutions to the pervasiveness of computerisation that was hampering individuals from controlling the use of the information about them.[201] In 1983, Chaum conceived the *anonymous* electronic money system known as Ecash, to be used for micropayments and based on RSA blind signatures, albeit still relying on a centralised operator.[202] Meanwhile, new models for exchanging information were emerging: one-way client-server models were joined by experiments with P2P networks, decentralised infrastructures composed of participants acting as both suppliers and consumers of informational resources.[203] The concept of resilient and decentralised P2P systems resonated well with cyberpunks, while the conjunction with encryption fostered freedom and liberty. Indeed, a decentralised currency seemed a perfect solution.[204] Nonetheless, as described in Chapter 1, the dream only became feasible with Bitcoin.

Anticipating risk assessments by international and (supra)national institutions, in his "Manifesto" May had foreseen the government was going to fight the spread of cryptographic solutions to protect national security – *e.g.*, to avoid the use of these technologies by drug dealers and tax evaders. He acknowledged these concerns and even the possibility of aiding the establishment of an "anonymous computerised market" to deal in assassinations and extortions, apart from national secrets and illicit and stolen materials. He argued, however, this was not going to stop the movement.[205] The link between *anonymity* and illegal activities, which emerged from the early days of the cyberpunk movement, was deemed a minor side effect in comparison to the benefits arising from safeguarding individual *privacy* against the government.[206]

---

[199] De Filippi P, Wright A (2018), p 19
[200] Magnuson W (2020), p 26
[201] Chaum DL (1985), p 1 Chaum, DL (1981) Chaum DL (1983), where he argued "the ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns". The solution relied on an anonymous payments system that could safeguard privacy and mitigate theft risk (Magnuson W (2020), p 28), by enabling transfer of e-cash without providing personal information (De Filippi P, Wright A (2018), p 19)
[202] Introduction to ECash (2017) Chaum DL, Fiat A, Naor M (1990). Nicoll C, Prins CJEJ, van Dellen MJM (2003), pp 34-42. De Filippi P, Wright A (2018), p 20 Micro-payments involve very small sums, usually e-commerce transactions where the good/service is available online (*e.g.*, applications, services, web-based contents).
[203] De Filippi P, Wright A (2018), pp 16-18
[204] Magnuson W (2020), p 34. De Filippi P, Wright A (2018), p 18
[205] May TC (1988)
[206] Magnuson W (2020), p 19. As explored below, *anonymity* and *privacy* are often placed on the same side of the debate, which requires a disambiguation effort.

Nonetheless, the application of advanced cryptography to payments and its impacts on illicit finance did not see the light with DLTs. On the contrary, the debate has a wider scope and the use of other technologies and of a wide variety of tools can be tailored to different goals. The issue of evaluating the impact of *anonymous* transactions on the financial system, and debates on whether and to what extent to allow them, did not originate from cryptocurrencies, nor is it inextricably linked to the Internet or digitisation *per se*. Hence, one may wonder in what terms cryptocurrencies are permeated by concerns about their *anonymity* levels, to the extent that most regulatory activity has targeted the prevention of misuses of the financial system.

2.1.2. Defining the scope of the conundrum

In the early stages of my investigation of *anonymity* and *transparency* in cryptocurrency ecosystems, I noticed the following elements:

- *Anonymity* and *transparency* are pivotal notions in the world of DLTs, and they are both considered inherent features of the IoM. Both *encryption* and ledger *transparency* have played a foundational role in the advent of Bitcoin and development of the IoM.
- *Anonymity* and *transparency* are key notions for AML/CFT/CPF as well, where *anonymity* generates considerable risks of financial systems being misused for illicit purposes. Meanwhile, *transparency* aids compliance, supervision, investigation, and enforcement.
- This twofold perspective is not new and does not relate to the IoM or AML/CFT/CPF exclusively. *Anonymity* and *transparency* have long been pivotal in the spheres of *online communication* and *financial transactions*, as testified by respective lines of literature.
- In the cyberspace, technology can be leveraged to undermine *anonymity* with analytics, but also to *anonymise* or *pseudonymise* activities,[207] which reduces users' *accountability*.
- *Anonymity* is double-edged: it can foster illegality, but the lack of it can violate human rights.[208] This prompted AML/CFT/CPF and privacy concerns, respectively. Cyberlibertarians testify to the tension between safeguarding individuals from surveillance and averting illicit deeds. Cryptocurrencies exemplify how these dimensions concretely play out.
- IoM ecosystems are not mandatorily DLT-based, but the properties of DLTs substantially shaped the IoM. Many regulatory issues of cryptocurrency ecosystems were linked to the properties of DLTs, a neutral tool susceptible to pursue good and illicit purposes.[209]

[207] Nicoll C, Prins CJEJ, van Dellen MJM (2003), p v. Article 19 (2015)
[208] Nicoll C, Prins CJEJ, van Dellen MJM (2003), pp 6-8
[209] ITU-T FG DLT (2019c), p 26

Against this backdrop, during my research I could observe the following:

- IoM discourse generally lacks terminological precision: different notions are (mis)used, within the DLT context and beyond it. The primary cause is the tendency of the "block-chain hype" to generalise – *e.g.*, insufficient distinction between *anonymity* and *privacy*.
- The AML/CFT/CPF framework makes use of notions of *anonymity* and *transparency* anchored to the mitigation of risks generated by unsupervised and *unaccountable* financial transactions. This concept of *anonymity*, crucial to the regulatory system, is not defined.
- Despite the belief there is a world of *anonymity* and *irresponsibility*, and one of *transparency*, *identification*, *accountability*, the dichotomy between *irresponsible anonymity* and *accountable identification* was challenged.[210] Along a spectrum from complete *anonymity* to full *transparency*, at any given point they coexist in a balance.
- The socio-technical nature of IoM ecosystems generates a granularisation of the concepts of *anonymity* and *transparency*. The features of cryptocurrencies are multi-layered, which spills into the dichotomy between *anonymity* and *transparency – i.e.*, the traits of an ecosystem depend on technical and social elements,[211] and on their interaction.
- IoM ecosystems have levels of *anonymity* that vary significantly.[212] When measuring technical *anonymity*, various studies often anchor their assessments to the same metrics, but rely on different interpretations of the attributes, giving different meanings to the benchmarks.[213] Consequently, it was argued that "there is no theoretical model up to now, which could model anonymity across different cryptocurrency schemes in a systematic way".[214] In this context, "modelling anonymity of cryptocurrencies involves a complex process of studying different notions of anonymity and their relationships and dependencies".[215]
- Due to the complex interplay of the IoM and the AML/CFT/CPF dimensions, notions of *anonymity* and *transparency* commonly used in adjacent domains of legal research– *e.g.*, privacy and data protection – are not useful and at times not applicable.
- A disambiguation effort is required when transposing AML/CFT/CPF concepts to the IoM sphere. It is key to clarify which aspects of *anonymity* and *transparency* are important when fighting ML/TF/PF performed within and/or through cryptocurrency ecosystems.

[210] Clarke R (1999). De Koker L (2015)
[211] Rogaway P (2016). Sardá T, Natale S, Sotirakopoulos N, Monaghan M (2019)
[212] Amarasinghe N, Boyen X, McKague M (2019), p 1
[213] Ibid, p 3 *Attribute* describes "an essential, definitional property [of a person] that qualifies it as a member of a given set (or class) [of persons]" (Wang F, De Filippi P (2020), p 2). The same can be argued for IoM ecosystems.
[214] Amarasinghe N, Boyen X, McKague M (2019), p 8
[215] Ibid, p 9

Against this backdrop, after introducing the role of encryption in the IoM, this chapter: (a) investigates the features of *anonymity* and *transparency* in cryptocurrency transactions at the crossroads of the digital world, financial transactions, and AML/CFT/CPF, and (b) outlines the impact on *accountability* of *enhanced disintermediation*. In doing so, it lays the foundations to introduce a holistic perspective in Chapter 3, where the scope of the analysis encompasses socio-technical elements affecting *anonymity* and *transparency* levels of IoM ecosystems.

2.2. Making Sense of Anonymity and Transparency: Two Sides of the Same (Crypto)Coin

The goals of this section are to disambiguate the notion of *anonymity* in the context of the IoM and in the AML/CFT/CPF domain, and to delineate its relationship with that of *transparency*. On the one hand, the relevant regulation does not define *anonymity* as such, but rather how to avert it.[216] On the other hand, the application of the term to IoM ecosystems requires consideration of their features for any conceptualisation of *anonymity* to mirror their reality. I argue the use of a teleological approach, focused on the objective of the definitions, is useful to this end. One may wonder: why is it dangerous that a subject engages in *anonymous* transactions over the Internet? How are AML/CFT/CPF rules challenged by *anonymity*? In what ways does *transparency* mitigate those risks and what can be *transparent* in a cryptocurrency transaction? What is the end-goal of prohibiting or restricting *anonymous* activities?

Well before the IoM, different conceptualisations had emerged in the realm of *online anonymity*. Ever since the issue spilled over to the financial domain and to the blockchain space, it has been increasingly complex for a definition to encompass all influential elements. Indeed, scholars adjusted the theory of *anonymity* in data communication – a topic that grounds diverse theoretical frameworks – to single out attributes to capture the different aspects of the concept of *anonymity* in the IoM sphere.[217] In this respect, it is possible to identify elements deemed as benchmarks to evaluate the *anonymity construction* of a cryptocurrency scheme.[218]

This type of approach shows the granularity of *anonymity*, which emerges as composed of different features whose importance depends on the perspective of the analysis. This notion is often addressed in a "static" way and evaluated using a series of metrics that builds its notion. This approach grounds the foundation of any further analysis, but I argue a "dynamic" methodology is more suitable to the AML/CFT/CPF context. This is chiefly because cryptocurrency

[216] De Koker L (2015)
[217] Amarasinghe N, Boyen X, McKague M (2019), p 2
[218] Ibid, p 3

transactions are performed within (and across) socio-technical ecosystems populated by many stakeholders, services, and technical layers, where the concept of *anonymity* comes into play in different forms. While there are fewer perspectives on the notion of *transparency*, its analysis benefits from a "dynamic" transaction-oriented approach as well. Indeed, the twofold nature of *transparency* outlined below arises from the application of DLTs to financial transactions.

Hence, I begin the analysis from the perspective of a cryptocurrency transaction. Figure 1 displays notions used in literature to describe *anonymity* and *transparency*, showing their different meanings and roles, as well as layers and conceptual differences among them. In the remainder of the section, I address the rectangles showed in the figure, highlighting traits within an AML/CFT/CPF context. According to this reconstruction, *anonymity* emerges as (a) conceptually granular, (b) context-specific, (c) observer-dependent, (d) broader than the ones of other regulatory frameworks. Meanwhile, the notion of *transparency* appears twofold and split by the fact that, as explored below, the concept of *transparency of the ledger* and *ledger operations* appears distant from the constitutive elements of that of *financial transparency*.

2.2.1. Conceptual granularity of anonymity

In my investigation, I focus on the notions typically found in literature, and at times used interchangeably with *anonymity* itself: *(un)traceability*, *(un)linkability*, *(un)identifiability*, *identification (or lack thereof)*, *pseudonymity*, *confidentiality*, *transparency*, *privacy.* The goal is to outline their relationship with *anonymity*, as interpreted for AML/CFT/CPF purposes. It was argued "technical anonymity exists when individuals are untraceable: there is no link between their actions and a singular identifiable and accountable persona",[219] and that "privacy coins" have "revealed that fungibility and anonymity are effectively synonymous".[220] In these statements, we see references to *anonymity*, *untraceability*, *unlinkability*, *unidentifiability, unaccountability* and *fungibility*. While the conveyed message is valuable from the perspective of their authors, it may be argued the mentioned concepts are not appropriately distinguished.

As a preliminary note, the analysis of these properties assumes the transaction is *detectable* and *observable – i.e.*, it is possible for the "attacker/observer" (the subject trying to reach *identification*, as outlined below) to sufficiently distinguish the fact it exists.[221] If not, the transaction is not relevant to my work and no further evaluation is made.

[219] Bancroft A (2020), p 180
[220] Berg A (2019), p 11
[221] Torra V (2017), p 13

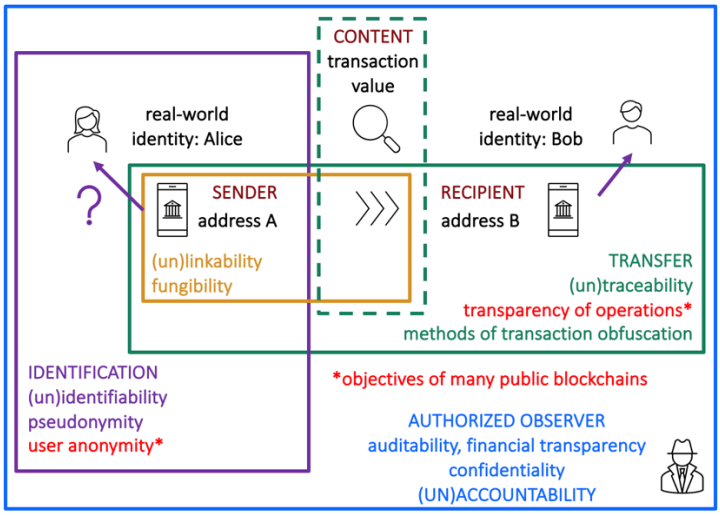

Figure 1: features related to *anonymity* and *transparency* relevant to the various components of a cryptocurrency transaction

A cryptocurrency transaction such as the one in Figure 1 is performed between a sender, with address A, and a recipient, with address B. As explored below, cryptocurrency addresses act as *pseudonyms* for their users. In this context, there are three chief elements to consider: (a) the parties, (b) their addresses, (c) the transfer, with its content. These aspects can be analysed separately to show how different features linked to *anonymity* are presented by literature.

When looking at the transfer of cryptocurrency funds (green rectangle), the notion of *traceability* refers to the possibility to trace the transfer, where methods of *obfuscation*, addressed in Chapter 3, pursue the *untraceability* (or limited *traceability*) of fund flows – *i.e.,* their obfuscation. *Untraceability* is defined as the impossibility to trace transactions back to their senders.[222] As reconstrued in the AML/CFT/CPF domain, the concept of *anonymity* is strongly related to that of *opaqueness* of financial flows, by influencing the possibility to retrieve information on origin of funds, underlying reasons for business/financial operations and identity of beneficial owners. Meanwhile, the possibility to transact *anonymously*,[223] and in general to reduce the *transparency* of fund flows, facilitate collection and laundering of the proceeds of specific (cyber)crimes such as ransomware attacks, often in the headlines in recent years.

Considering the relationship between the transfers and the accounts that originated or received them (yellow rectangle), the notion of *linkability* describes the possibility to link two or more transfers to an address – *i.e.*, given two or more transactions, it is possible to refer them to the same user. In this sense, literature equates *anonymity* with *unlinkability*, and

[222] Amarasinghe N, Boyen X, McKague M (2019), p 3
[223] This chapter and Chapter 3 investigate the extent to which, and the conditions under which, a transaction can correctly be considered *anonymous* and the relationship with other notions.

accountability with *maximum linkability*.[224] In this context, the notion of *recipient anonymity* refers to the impossibility to link transactions to their recipients.[225] Another type of *(un)linkability* is used to define a property between transactions and other type of data, such as transaction metadata. For instance, *metadata (un)linkability* can refer to the *(un)linkability* of IP addresses to transactions and cryptocurrency addresses, which could single out geographical locations and uncover *real world identities*. When looking at the content of the transaction (dotted green rectangle), specific techniques can hide transaction values. In this way, it is harder or impossible to link transactions to addresses through an analysis of transaction flow patterns.[226]

2.2.2. Context-specificity of anonymity: identifiability and identification

In the AML/CFT/CPF field there is a foundational concept that mirrors a necessary step to avoid *anonymity*: *identification*. Reaching *identification*, in turn, depends on the quality of *identifiability – i.e.*, the possibility to link the address to a *real-world identity*. It is self-evident that the address acting as a *pseudonym*, in the absence of any connection to other data, is not enough to hold real-world users *accountable*. From an operational perspective, AML/CFT/CPF provisions regarding customer due diligence (CDD) and know your customer (KYC), analysed in Chapter 4, pivot on two concepts: (a) *identification* of a subject and (b) *verification* or *authentication* of a subject's *identity*. In this context, *identification* means establishing the *real-world identity*, while *verification* entails verifying the authenticity of said *identity* against previously pinpointed identifying information – *i.e.*, an *identifier*/a set of *identifiers*.[227] In other words, verifying that the two details – *i.e.*, the data provided and that used to verify it – relate to the same subject.[228] Indeed, the same existence of financial institutions was linked to *identity*-related regulatory requirements such as KYC in terms of "identity cost economising".[229]

---

[224] Torra V (2017), p 14
[225] Amarasinghe N, Boyen X, McKague M (2019), p 3
[226] Transaction analytics techniques are explored in Chapter 3.
[227] Other authors have described (biometric) identity-based systems starting with the concept of *authentication*, defined as a process that takes place after registration to a specific system, by which the system checks whether the individual has permission to access the service. In this scenario, there are two stages in *authentication*: *identification* and *verification*. While "verification is the process of verifying one's identity" (in the case at hand, by biometric means, a one-to-one matching process), "identification is the process of retrieving the identity of a particular individual, based on an identifier" (a one-to-many matching process). Wang F, De Filippi P (2020),p 8
[228] Grijpink J, Prins C (2001), p 381. The eIDAS framework provides valuable definitions: "person identification data" is "a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established" (Article 3(1)(3)), and "authentication" is "an electronic process that enables the electronic identification of a natural or legal persons, or the origin and integrity of data in electronic form to be confirmed" (Article 3(1)(5)). Regulation (EU) 910/2014.
[229] Berg A (2019), p 2

As mentioned above, it is a mistake to think something is either *identified* or *anonymous*. On the contrary, these traits range on a spectrum. Nonetheless, frameworks such as AML/CFT/CPF provide criteria that impose a degree of *identification* conducive to the prevention (or risk mitigation) of illegal transactions or to ensure *traceability*. Hence, in this context I argue a subject is *identifiable* for a specific purpose when the entity in charge of the *identification* process can access the information required by the framework. Thus, a subject is *identifiable* or *non-identifiable* only with reference to a specific actor. Since the concept of *identifiability* is the negation of *anonymity*, if a subject cannot identify another subject – or identify and verify the identity, if so required –, the latter is *anonymous* with regard to the first one.[230]

It follows that two seemingly opposite goals – (i) for a person to choose if/when to be *identified*, to safeguard fundamental rights,[231] and (ii) to ensure *identifiability* for the sake of *accountability* and enforcement – can be assessed only in light of the specific situation. For this reason, I argue *anonymity* is a context-specific notion. In other words, its definition varies depending on the (regulatory) context. In the case at hand, the applicable AML/CFT/CPF framework lays out the criteria against which it should be evaluated whether *identification* has been reached. In this respect, *anonymity* can be evaluated only with respect to specific requirements.

Taking a further step, one can notice that assessing compliance is not only a question of the regulated entity *being able* to identify and verify an identity – *i.e.*, of the subject being *identifiable*. What is important is *doing it – i.e.*, *identification*. Indeed, a regulated entity may simply not do it even when able to. This explains why in early AML/CFT/CPF initiatives "anonymous funding" was defined as "cash funding or third-party funding through virtual exchangers that do not properly identify the funding source", and an "anonymous transfer" is a situation where "sender and recipient are not adequately identified".[232] In these cases, *anonymity* may not originate from the entity being unable to perform the required *identification* and *verification* but stems from the entity neglecting its duty to perform one or more relevant activities.

When addressing *anonymity* and *identifiability* in the AML/CFT/CPF sphere, one cannot forget they are also at the core of data privacy and data protection law. In this case, the concept of *anonymity* is related to that of "personal data", and the approach resembles the one described above with regard to the importance of *identification* and *identifiability*. The notion of *anonymous information* is not explicitly defined, but refers to the result of the conversion process of personal data to which data protection rules no longer apply – *i.e.*, so-called "anonymisation

[230] Pfitzmann A, Hansen M (2010), p 22
[231] Lindsey LB (1999), p 1
[232] Financial Action Task Force (2014), p 6

techniques" explored below.[233] In other words, "anonymous information is data which does not relate to an identified or identifiable individual (*i.e.*, data that is not personal data)".[234] I argue a similar reasoning, in conjunction with the arguments provided above, can be applied to an AML/CFT/CPF scenario – after all, a transaction is an exchange of information. Accordingly, an *anonymous transaction* is one that cannot be related, or in any case is not related – *i.e.*, it does not relate – to an *identified* (hence, *identifiable*) individual.

2.2.3. User anonymity and ledger transparency

When it comes to assessing ledger *transparency*, the distinction between private and public blockchains is most relevant. As introduced in Chapter 1, blockchains can be *public* or *private*, and *permissioned* or *permissionless*. The first concept concerns reading restrictions, while the latter pertains to writing permissions. In other words, a public blockchain is publicly readable, while a private blockchain can be read only by authorised actors; in a permissionless blockchain all the participants can add transactions to the ledger, while in a permissioned blockchain this is available only to authorised participants. It follows that private ledgers are usually permissioned – *i.e.*, often, if there are reading restrictions there are also writing restrictions.[235] When the network can be freely accessed for reading and viewing purposes, it is public. If not, it is private. In this respect, the (un)restricted access is "to" something, namely to a set of data. These distinctions come into play from two different, albeit related, perspectives.

On the one hand, different ledger types have been related to divergent approaches to *identity* and *identification*. In public permissionless blockchains with no intermediary or centralised authorities, such as Bitcoin and Ethereum, the nodes that maintain the network "operate without association to a particular given identity".[236] In this respect, public blockchains "are structurally designed as devices allowing anonymous transactions between peers. Blockchains are generally intended to provide users with evidence with no disclosure of knowledge".[237] Because in public ledgers all transaction data is publicly available, the *anonymity* of a public ledger could be defined as a situation in which "an outsider cannot link the transaction data to the participants involved in corresponding transactions".[238] Being a public ledger, we assume

[233] ICO (2021)
[234] Ibid
[235] There are specific cases of *private permissionless* systems – *e.g.*, Holochain, LTO Network – where generally anyone can become a node, but information is shared on private sidechains. Daniels, A (2018), LTO Network (2019)
[236] Wang F, De Filippi P (2020), p 4
[237] Quiniou M (2019), p 22
[238] Amarasinghe N, Boyen X, McKague M (2019), p 2

the outsider can see the transaction data, and *anonymity* is then referred to the possibility to connect this data to the parties involved. This is the feature of (*un)linkability* addressed in the previous section. By contrast, in permissioned blockchains, where there is a centralised entity or consortium that identifies the nodes, their key-pair is usually associated with a *real-world identity*. This enables policing and renders unnecessary some security measures employed in permissioned blockchains – *e.g.*, consensus mechanisms PoW or PoS.[239]

On the other hand, allowing individuals to perform transactions directly and without being *identified* was one of the core elements pursued by the monetary application of DLTs. In this context, the goal of many public blockchains like Bitcoin is a combination between *user anonymity* – better, as outlined below, *pseudonymity* – with *transparency of operations*. In other words, the ledger is *transparent,* and the complete transaction history is available for everyone to read. Network participants, however, are not related to their *real-world identities*, but to addresses that act as *pseudonyms*.[240] The combination of *user anonymity* and *transparency of operations* may seem paradoxical. Indeed, part of the "blockchain hype" is centred on the praise of these networks for the *privacy* they seem to offer, where *privacy* is intended as a product of the purported "trustless trust" and lack of centralised control. By contrast, in principle data is published for all participants to see – *i.e.,* the ledger is *transparent*.[241] While the two objectives may appear opposed at a first glance, they are in practice compatible.[242] The combination pursued by public blockchains between *user anonymity* and *transparency of operations* was further developed by AECs, addressed in Chapter 3. In this context, key opportunities to combine these objectives are offered by zero knowledge proofs (ZKPs).

2.2.4. Transparency of operations and financial transparency

Transparency of operations, however, is a type of *transparency* that does not ensure *accountability*, and starkly differs from *financial transparency*, grounded on the connection to *real-world identities – i.e.*, it relies on *identifiability.* Indeed, *transparency* itself is a concept prone to embodying different understandings when related to *accountability* in information networks.[243] This distinction is important because the value of *transparency* is significant in the financial world as well. A long-lived debate has investigated the (in)compatibility of

[239] Wang F, De Filippi P (2020), p 4
[240] Amarasinghe N, Boyen X, McKague M (2019), p 2
[241] Marthews A, Tucker C (2019)
[242] Quiniou M (2019), p 18
[243] Herian R (2019), pp 77-91

financial transparency with the concepts of *financial privacy* and *banking secrecy*, interpreted as the principle of *confidentiality* in financial transactions.[244] In this context, *(financial) confidentiality* also refers to the limited number of actors with access to financial information, as it is also in the context of AML/CFT/CPF-related data.[245] The digitisation of financial services generated new challenges in this regard, and a turning point was identified in 2008, when macroprudential concerns produced by the financial crisis urged regulators to balance core principles such as financial stability, consumer protection, inclusion, growth, and innovation.[246] A prior permissive approach to digitisation known as "deregulation" was replaced by a more structured analysis, which was met by the FinTech revolution and its evolving risks.[247]

Against this backdrop, I argue it is naïve to thrust on cryptocurrencies the burden of having first meddled with the relationship between transacting *privately* and being *accountable* for financial operations. Also in the financial services sector, a situation of "full transparency" would cause significant turmoil, as on a *fully transparent* DLT platform "all information would be disclosed to the public such as the players involved, the pricing and the timing of the transactions along with other relevant information that would reveal much of the investment strategies of the institutions or people involved in the process. Such a level of disclosure would probably greatly affect the competitive advantage that some institutions have over their competitors".[248] The fact that the *transparency* of compliance regimes differs from the one praised in DLTs advocates for applying the teleological approach, focused on context and purpose of the definition of *transparency*, as elaborated below and laid out analytically in Chapter 3.

As introduced above, a situation of *transparency* is often equated to one where there can be *accountability*. From this perspective, the quest for *transparency* to ensure *accountability* has long been a commonplace goal in information networks, frequently challenged by surveillance criticism. In this sense, the interplay between *transparency* and *accountability* does not only transcends the financial sphere – *e.g.*, it also concerns the activity of public administrations – but is also complex.[249] The general understanding of *transparency* was linked to openness and visibility, as opposed to *secrecy*. This, however, proved insufficient in the normative dimension, where it was argued the concept of *transparency* can no longer be limited to *revealing information*, and should address issues of "usage, legitimacy, respect to privacy, accountability,

[244] Lindsey LB (1999), pp 171-172. ABA Bank Compliance (1999), pp 147-158. Le Nguyen C (2018), pp 53-54
[245] Fanti G, Pocher N (2022), p 19
[246] In financial regulation, the "macroprudential/systemic" perspective focuses on the overall impact of interrelationships between financial institutions, thus pinpointing those exerting influence from a systemic perspective.
[247] Zetzsche DA, Buckley RP, Arner DW, Barbaris JN (2017), pp 6-8
[248] ITU-T FG DLT (2019c), p 24
[249] Herian R (2019), p 77

as well as data integrity*"*.[250] For this reason, a modern understanding of *transparency* is based on the *presentation of information* being "open, comprehensive, clear and understandable".[251] Hence, it is not enough to have access to information thanks to *transparency* requirements, it has to be presented in a way qualitatively conducive to establishing *accountability*.

In the AML/CFT/CPF sphere and in related blockchain literature, one may find statements inspired by what I defined as teleological approach. Accordingly, the notion of *transparency* is the one that aims to fight ML/TF/TP, and this understanding of *transparency* is focused on information on the origin of funds and on the *identification* of clients and intermediaries, as provided for by AML/CFT/CPF duties. Although the issue of *transparency* is key in blockchain protocols, the type of *transparency* offered by public blockchains is a type of *transparency* useful for user interaction, not for oversight bodies.[252] Indeed, *non-centralised* systems embody (and leverage) a concept of *transparency* radically opposed to the one useful for regulatory purposes, such as in the AML/CFT/CPF sphere. Hence, there would be a structural incompatibility between blockchain technologies and the rules on *transparency* set by regulators.[253] Indeed, "it is questionable whether this approach to user anonymity and transparency of operations adopted by public blockchains is compatible with regulations".[254] A clear example is that of the GDPR, which pursues the "objective of conferring to the individual control of their own personal data, therefore not allowing it to be fully transparent and open to everyone*"*.[255]

2.2.5. Pseudonymity and monetary fungibility [256]

The accuracy of defining the Bitcoin system as *anonymous* was challenged extensively and there is widespread consensus that, despite its evolutions, it has yet to provide an "acceptable" degree of *anonymity*. This "acceptability" in terms of cyber-libertarian ideals relates to monetary *fungibility – i.e.,* the property of the units of a currency system that are all identical – according to its criteria of "anti-individuation" and "anti-reidentification".[257] If it is possible to trace transactions back to senders/recipients and retrace the history of specific currency units, the currency scheme loses credibility and quality. This is because the history of a specific coin

[250] ITU-T FG DLT (2019c), p 23
[251] Ibid, p 23. The definition is per ISO 16759:2013
[252] Quiniou M (2019), p 20
[253] Ibid, p 20
[254] Ibid, p 18
[255] ITU-T FG DLT (2019c), p 24
[256] *Contents and parts of this subsection have already appeared in the following co-authored publication:* Pocher N, Zichichi M, Ferretti S (2023)
[257] Berg A (2019), p 11

affects its nominal value and actual worth – *i.e.*, it affects the *fungibility* of the units of currency.[258] If the history of currency units can be retraced, the outcome is similar to a banknote bearing on its surface dots representing the types of transactions it was involved in.

In this respect, the concept of "identity of money" refers to the history of the exchanges: when a unit of currency has an *identity*, as a result of regulatory provisions and activities of authorities – *e.g.*, a red dot is drawn on the banknote when it is used to perform an illicit payment –, monetary *fungibility* is threatened.[259] In this case, it is not true any longer that all banknotes are equal, as their identity is defined by the dots drawn over time, and a recipient may reject a specific banknote if a specific dot is present. Accordingly, the banknote loses connection with the nominal value, and the currency scheme loses credibility.

From the perspective of the possibility to link a given transfer – better, the specific coins involved – to a specific address and thus to the previous activities performed by that address and those coins, in Figure 1 the quality of *fungibility* is placed in the yellow rectangle. Indeed, public distributed ledgers were proving tricky in maintaining *user privacy*, due to the possible exploitations of identifiers in terms of *linkability* and *traceability*. Accordingly, Bitcoin itself was found not to possess the properties of *unlinkability* and *untraceability*.[260] Hence, an analysis of the transactions could allow identity-related conclusions to be inferred: "if Account A sends a specific amount at a specific time to Account B it is sometimes possible to triangulate and determine the offline identities of the people associated with the transaction".[261]

The reasons for this depend on the way Bitcoin was designed, and in particular:

- Bitcoin transactions are based on two key concepts: *inputs*, the amounts spent on a transaction, "spent state", and *outputs*, the amounts received, "unspent state". Hence, the balance of a wallet is equal to all the outputs not yet spent – *i.e.*, "unspent transaction outputs (UTXOs)".[262] As depicted in Figure 2 below, each transaction refers to one or many previous UTXOs with their own unique recipient addresses. Since these UTXOs become inputs for new transactions, to know the balance held by a specific user we can add up the UTXOs related to the addresses the person has the private key to unlock. When this type of UTXO-based or address-based data representation is deployed, there are no accounts at the protocol level. Besides Bitcoin and other blockchains such as Litecoin, Zcash, Dash, and Cardano, this is the model used by IOTA's Tangle. Other networks, especially

[258] Ibid, p 1
[259] Ibid, p 6
[260] Van Saberhagen N (2013), cited by Amarasinghe N, Boyen X, McKague M (2019), p 3
[261] Harvey J, Branco-Illodo I (2020), p 109
[262] Silva Ramalho D, Igreja Matos N (2021), p 490. Furneaux N (2018), p 73

blockchains focused on the deployment of smart contracts, primarily Ethereum, use an account-based accounting method, where coins are represented as a balance of a wallet.[263]

- As shown in Figure 2, and contrary to what happens in account-based blockchains, in UTXO-based systems it is not possible to transfer only part of the coins attached to an address. Hence, in a UTXO transaction the entire amount corresponding to an address must be spent when making the transfer. If the amount to be paid is lower than the transferred one, the sender receives the remainder back as change.[264]
- In this context, each transaction is identified through a "transaction ID (TXID)" equipped with details such as time of receipt, relevant block, values of input and output, addresses of sender and recipient. As explored below, this data can be leveraged to "follow" the funds to a wallet managed by a regulated entity, thus identifying at least the (final) recipient.[265] This is not a surprising feature of distributed ledgers. Indeed, although *privacy* was perceived as important, the primary aim of their applications was *decentralisation*, thus generating a "double-headed technical challenge of untraceability and unlinkability".[266]

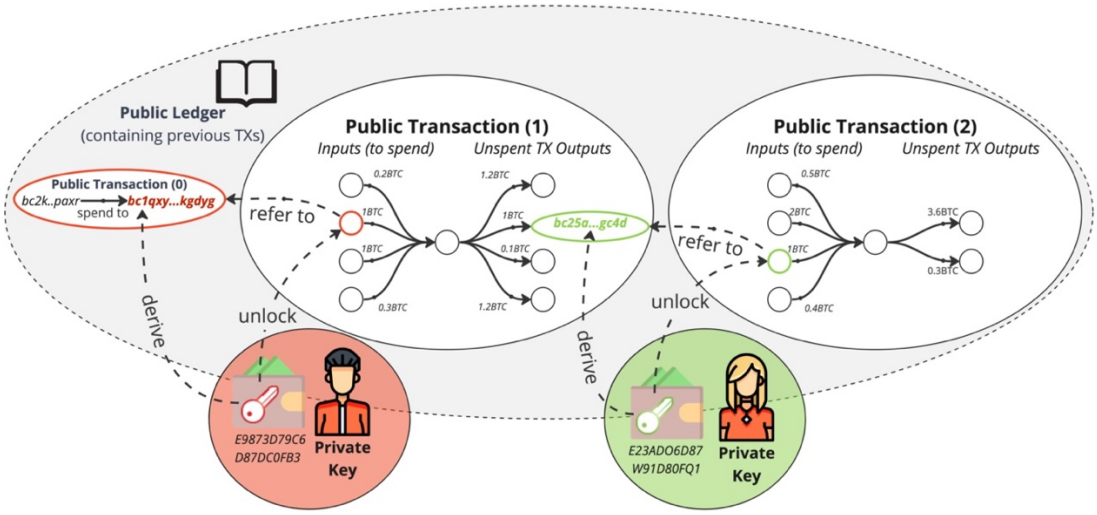

Figure 2: anatomy of a transaction in a UTXO-based system
From: Pocher N, Zichichi M, Ferretti S (2023)

[263] Pocher N, Zichichi M, Ferretti S (2023), p 3. In account-based systems, the accounts are controlled either by a private key or by a smart contract. In Ethereum, this difference originates two types of accounts: externally owned accounts and contract accounts, respectively.
[264] Furneaux N (2018), p 73-74
[265] Silva Ramalho D, Igreja Matos N (2021), p 491. Because Bitcoin is based on *transparency* a significant amount of data on specific transactions and addresses can be obtained from open sources. In this respect, tools such as "wallet explorers" allow addresses tied to gambling platforms, exchanges or mixers to be identified (Ibid, p 493).
[266] Harvey J, Branco-Illodo I (2020), p 130

As mentioned above, however, the property of *anonymity* is paramount for a currency, and in this case the simplest understanding of *anonymity* refers to units being *undistinguishable* from any other.[267] The degree of *fungibility* featured by a currency is closely related to the *anonymity* it offers, while to satisfy *fungibility* it must fail the "*identification* criteria" of *individuation* and *re-identification*.[268] Accordingly, the lack of an acceptable level of *anonymity* brings about the "undesirable consequences of a non-fungible currency, such as the possibility of ostracising participants".[269] Hence, *fungibility* is a key attribute of cryptocurrency *anonymity*, and the claimed insufficiency of Bitcoin in this regard prompted *anonymity*-enhanced coins.

Bitcoin is *pseudonymous*, and the same is true for other cryptocurrencies.[270] *Pseudonymity* is "the use of pseudonyms as identifiers", where a *pseudonym* is an "identifier of a subject other than the subject's real names".[271] A parallel was drawn between public and private keys and the idea of username and password,[272] where cryptocurrency addresses (public keys) act as usernames, a common example of *pseudonyms*. In a cryptocurrency transaction, the sender and/or recipient are *pseudonymous*, and not *anonymous*, when they are identified by their respective addresses. Indeed, the gap between cryptographic keys and human identities was one of the elements leading to the establishment of intermediaries in the cryptocurrency sphere – *e.g.*, centralised exchanges and related businesses.[273] The concept of *pseudonymity* primarily relates to the case in which it is possible to link public addresses (*pseudonyms*) to *real-world identities.* Hence, the purple rectangle in Figure 1. *Pseudonymity*, however, can also be interpreted in a broader sense. Generally, a *pseudonymous* trait can be conceived even in those networks with no access requirements such as *identification*. This is because the linkage to a *real-world identity* can exploit data that is external to the ecosystem at hand.[274]

A blockchain system generally manages *identifiers* through pairs of public/private keys that identify the wallet holder uniquely.[275] In Bitcoin "the complete history of the transactions is transparent to the network participants, yet they are not related to specific identities, but

[267] Amarasinghe N, Boyen X, McKague M (2019), p 1
[268] Berg A (2019), p 1-3
[269] Amarasinghe N, Boyen X, McKague M (2019), p 1
[270] Biryukov A, Tikhomirov S (2019). Li Y, Susilo W, Yang G, Yu Y, Du X, Liu D, Guizani N (2019). Wachsman (2019)
[271] Pfitzmann A, Hansen M (2010), pp 21-22. In a more ambiguous fashion, *pseudonymity* was equated with the use of a false name (Weber R, Heinrich U (2012), p 1), where "false" assumes the chosen identifier is also a name.
[272] Sun Y, Yi YZ (2018a)
[273] Allen S, Capkun S, Eyal I, Fanti G, Ford B, Grimmelmann J, Juels A, et al (2020), p 26. Blockchain scholars explored *identity* using different methodologies. It was underlined how it is inherently "digital", encompassing four elements: "registration information", "transactional identity", "transaction history", and "digital history" (Marthews A, Tucker C (2019), p 246). For AML/CFT/CPF purposes, it shall be a verifiable "legal identity"
[274] This can be done through blockchain forensic strategies, as outlined in Chapter 3.
[275] Wang F, De Filippi P (2020), p 3

addresses".[276] Bitcoin's *pseudonymity* means that even if identifiers "do not communicate any personal identifying information about the person, unless additional information is associated with them",[277] they can be used to connect transactions to their history. In other words, although Bitcoin seemed to fit cyberlibertarian goals of a monetary system supporting ideals of *unaccountability*, its actual *anonymity* level proved insufficient. In line with the socio-technical nature of the IoM, there are several elements to consider. A significant influence in the evolution of the *anonymity* levels was exerted by forensics. This is because the deployment of advanced investigative techniques, and certain transactions being trackable, generated significant distrust of the *privacy* degree of DLT ecosystems, while undermining *fungibility*.[278] Against this backdrop, other authors investigated parameters such as *k-anonymity* and *taint resistance*,[279] whose relevance emerged in the context of intelligence techniques addressed in Chapter 3.

2.2.6. Observer-dependency and broadness of the notion of anonymity

Because *identifiers* alone "do not communicate any personal identifying information about the person, unless additional information is associated with them",[280] the quality of being *pseudonymous* does not necessarily imply *identifiability*. A *pseudonymous* subject is *identifiable* only if from the point of view of the actor trying to identify the subject – *e.g.*, providers of exchange or forensic services, LEAs, authorities –, it is possible to discover its *real-world identity*. At this point, the literature accounts for the interplay between *identifiability* and *traceability*. In this sense, however, the meaning of *traceability* is referred to the *identity* of the parties, not to the transaction itself, as outlined above and displayed in the green rectangle of Figure 1. Indeed, from this additional perspective the link been *identifiability* and *traceability* emerges from four "forms of *identification*" – that could be better defined, perhaps, as degrees of *identifiability* – described in 1995 with regard to email communication:

[276] Amarasinghe N, Boyen X, McKague M (2019), p 2
[277] Wang F, De Filippi P (2020), p 3
[278] Casey M, Crane J, Gensler G, Johnson S, Narula N (2018). Berg A (2019)
[279] K-anonymity was explained by stating that "in a system of k users, for any given user in the system, if the actions of any of the remaining k-1 users cannot be differentiated from said user, then that user is regarded as k - anonymous. K represents the size of the anonymity set and a larger k value corresponds to a higher level of anonymity". Amarasinghe N, Boyen X, McKague M (2019), p 3. Taint resistance was defined as a "measure of the identifiability of the ownership of a Bitcoin by analysing its past transactions and hence is related to the properties of traceability and fungibility". In particular, the analysis is of the "relationships among Bitcoin addresses based on the transaction history corresponding to those addresses". Meiklejohn S, Orlandi C (2015), cited by Amarasinghe N, Boyen X, McKague M (2019), p 3
[280] Wang F, De Filippi P (2020), p 3

i. *traceable anonymity*: the originator sends no identity data, but this information can be retrieved by contacting the intermediary;
ii. *untraceable anonymity*: the sender is *unidentifiable;*
iii. *traceable pseudonymity*: the *pseudonym* can be traced back to the sender;
iv. *untraceable pseudonymity*: the originator uses a false and *untraceable* identity.[281]

These concepts explain why *pseudonyms* can be used to "cover the range between *anonymity* (no *linkability*) to *accountability* (maximum *linkability*)",[282] and to pursue *anonymity*.[283]

Against this backdrop, I argue the concept of *anonymity* is observer-dependent: it can be assessed only with respect to a specific actor trying to reach *identification*. Indeed, the *anonymity of an entity* was defined in the literature as the situation in which an outsider is unable to adequately identify it within a group of entities, where the latter is its "anonymity set". In the context of data privacy, the cybersecurity perspective is that of an "attacker" engaged in a de-anonymisation attack, where this is a negative concept – *i.e.*, an attempt to compromise the integrity of a system to pursue illegal goals such as data protection violations. Nevertheless, the same techniques are deployed by LEAs to "follow the money" and uncover illicit schemes, as explored in Chapter 3. Evidently, when transferred amounts and other metadata are permanently and publicly stored on the ledger it is easier to gather information. Similarly, some networks leak information that can be used for de-anonymisation purposes.[284]

As suggested above, when speaking of *anonymity* in AML/CFT/CPF literature there is less terminological precision than in other fields such as data protection. It is also noticeable, however, that in the AML/CFT/CPF domain the meaning of the concept of *anonymity* is broader. Indeed, consistently with the purpose of the framework (*i.e.*, teleological approach) AML/CFT/CPF provisions lean towards an understanding of *anonymity* that does not distinguish between *anonymisation* and *strong pseudonymisation*. Hence, in AML/CFT/CPF *anonymity* encompasses both "(i) the impossibility or near impossibility of linking data on a ledger with an identified person(s), and also (ii) a situation when such a linking is 'only' significantly hampered".[285] Thus, methodologically this work builds on a broad understanding of a*nonymous data* and *anonymisation technologies*. Accordingly, it acknowledges that the "same data could be qualified as pseudonymous under the GDPR and as anonymous under AML policies".[286]

[281] Froomkin AM (1995), p 1
[282] Torra V (2017), p 14
[283] Pfitzmann A, Hansen M (2010), p 22
[284] Airfoil (2019)
[285] Karasek-Wojciechowicz I (2021), p 3
[286] Ibid, p 3

The literature on the *anonymity* of cryptocurrency does not usually enshrine an AML/CFT/CPF-oriented methodology, nor it features the perspective to strictly identify *anonymity* metrics relevant for AML/CFT/CPF compliance purposes. However, intelligence strategies and AECs show how the two perspectives may be closer than one would think. Hence, it can be argued the increasing complexity of new cryptocurrency applications, networks, or service providers, is making a broad technical understanding of their *anonymity* levels – and relevant metrics – more relevant also from an investigative and enforcement viewpoint. Indeed, there is an important connection between *anonymity* in cryptocurrencies and *anonymisation techniques* applied in data privacy. Their application to personal data happens in the context of frameworks such as the GDPR in the EU. When these techniques are applied to personal data, this is no longer considered personal, thus making the relevant regime not applicable. As per Recital 26 GDPR, the principles of data protection are not applicable to *anonymous information*, defined as information that is not related "to an identified or identifiable natural person", nor to personal data "rendered anonymous in such a manner that the data subject is not or no longer identifiable". Although *anonymisation techniques* have been supported for many years, their limitations have been recently underlined, such as that their effectiveness requires irreversibility.[287]

It goes beyond the scope of this work to dive into *anonymisation techniques* and their historical background. However, some have a strong IoM connection from an AML/CFT/CPF perspective, especially considering AECs. A special role is played by *pseudonymisation*, an *anonymisation technique* in data privacy, although controversially,[288] and crucial in data protection and valuable for controllers and processors. It is defined by Article 4(5) GDPR as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

Further, *anonymisation techniques* encompass concepts such as *k-anonymity*, *l-diversity* and *t-closeness*,[289] as well as approaches of data perturbation or noise addiction such as *differential privacy*. Meanwhile, other methodologies employ synthetic/artificial datasets or apply *homomorphic encryption*, which allow encrypted data to be used without decrypting it. Although these concepts prove useful to assess *anonymity* levels in IoM ecosystems, in recent

[287] Capraz S, Ozsoy A (2021), p 110
[288] See, for instance, Article 29 Data Protection Working Party (2014)
[289] *L-diversity* was described with reference to the idea of generating and using a diverse enough set of possible values to represent data. *T-closeness* uses distributed systems to parse and distribute sensitive data (Capraz S, Ozsoy A (2021), p 110)

times these techniques were replaced by the application of distributed systems and blockchains. Indeed, centralised and trust-based systems are argued to be possibly insufficient to provide users with control over their personal data.[290] Albeit the compatibility of blockchain technology with data protection frameworks is debated,[291] its use to implement data protection systems is also investigated. To date, it has largely relied on ZKPs, as detailed in Chapters 3 and 4.

2.2.7. Contextualisation: privacy and anonymity

Often, in cryptocurrency discourse the terms *anonymity* and *privacy* are used in a way that may seem interchangeable. A typical example is to say that the *anonymity* of cryptocurrency is dangerous but can safeguard individual *privacy* against governmental surveillance practices. This is not incorrect, but it is important to specify that in data privacy, *anonymity* – better, *anonymisation* – is only one of the available techniques to enhance *privacy*. In particular, *anonymity* requires the absence of *identifiers*. If there are *identifiers*, there is *pseudonymity*. Hence, both *anonymity* and *pseudonymity* relate to *identity*. By contrast, *privacy* is a much broader concept and can also be safeguarded in ways other than *anonymity*, and to different extents. Hence, the two terms, although possibly at the same side of the debate involving *surveillance* vs. *privacy*, are not synonyms. From this perspective, it was argued that a correct conceptualisation of *anonymity* does not define it as a subset of *privacy*, but as its perfect realisation or product.[292] To clarify, the context of a transaction such as the one depicted in Figure 1, from the perspective of data *privacy* the scope of the concept of *anonymity* only relates to the address – that acts as a *pseudonym* – and to the *real-world identity* – *identifiability* and *identification*.

The same interchangeable use of terms can be detected in *privacy*-enhancing techniques (PETs) and their implementation in *anonymity*-enhanced currencies (AECs), also known as "privacy coins". AECs and the application of PETs in the IoM are addressed in Chapters 3 and 5, respectively. From the perspective that is relevant here, "privacy coin" projects are focused on enhancing their *privacy* level, and they do so by enhancing (also) their *anonymity* level. Nonetheless, there is no single way to assess the *privacy* level of a given application, and three different aspects of *privacy* have been explored when looking at a blockchain architecture:

(i) *privacy of identity* or *user-identity privacy*: it follows from what was argued before that this the type of *privacy* relates to *anonymity* and *pseudonymity*. At times, this concept is

[290] Capraz S, Ozsoy A (2021), pp 110-111
[291] Finck M (2019b)
[292] Helms SC (2001). The concept is most relevant to current debates on CBDC designs, explored in Chapter 5.

labelled *user anonymity*. Indeed *user-identity privacy* concerns the link between *identity-related* data stored on the blockchain, and a *real-world identity.* From this perspective, scholars explored the structural difference between *anonymity* and *privacy* in respect to *identification*, namelessness, and new technologies.[293] Relatedly, enhancing *privacy* does not necessarily impact on *identification*, as exemplified by the use of *pseudonymity* to protect *privacy* in the cyberspace long before the advent of Bitcoin;

(ii) *privacy of information* or, in the financial context, also *privacy of transaction data*: it refers to the green rectangle in Figure 1 above. In this sense, *privacy* is a mutable concept, as data is represented differently in the different blockchain types, various elements may be *public* or *private* from different third-party observers (the observer-dependency argued above), and different types of information can be *private* to different extents;

(iii) *privacy of the total blockchain state*: this is a separate aspect that pertains to the total ledger state. In this context, specific attributes can be *private* to different extents.[294] Although more frequently mentioned use cases are blockchain-based, *privacy* assessments have been carried out for other distributed ledgers. In this respect, a notable example concerns the directed acyclic graph known as "the Tangle", implemented by IOTA.[295]

Against this backdrop, it can be argued that the concepts of *anonymity* and *user privacy* are overlapping, and most studies investigate "privacy and anonymity in conjunction and find an intrinsic relationship between the two terms".[296] Indeed, some of the metrics mentioned in this section in relation to *anonymity* have been leveraged to calculate the level of *user privacy* of different networks. For instance, the level of *user privacy* offered by Bitcoin was assessed through the metrics of *unlinkability of activities* and *indistinguishability of user profiles*.[297]

2.2.8. Anonymity and transparency: a paradox or a combination?

As outlined above, public blockchains tend to enshrine an alleged "paradox" in which "while the information on the ledger is transparent for everyone to see or read, it is also private, thus ensuring the anonymity of the players involved. The balance between transparency and privacy is paramount for DLTs to comply with norms and regulations".[298] In a *distributed* and

[293] Skopek JM (2015), pp 717-723
[294] Sun Y, Yi YZ (2018a)
[295] Tennant L (2017), pp 14-15
[296] De Haro-Olmo FJ, Varela-Vaca AJ, Álvarez-Bermejo JA (2020), p 11
[297] Androulaki E, Karame GO, Roeschlin M et al (2013)
[298] ITU-T FG DLT (2019c), p 24

non-centralised environment, *transparency* is used to generate or bypass "trust", avoiding the need of a trusted third party. To some extent, *transparency* enables the kind of *privacy* that follows the absence of a central authority. Nonetheless, *transparency* has a twofold impact, since it fosters *accountability* and allows surveillance and *traceability*. This is not a surprising feature of distributed ledgers: although *privacy* was politically important, the primary aim of their applications was *decentralisation*, which generated a "double-headed technical challenge of untraceability and unlinkability".[299] Hence, reaching higher levels of *anonymity* required specific techniques known as PETs, addressed in Chapters 3 and 5. While PETs can be used to "design" *privacy*, their application to DLTs generates regulatory problems: while in *intermediated* systems there is a gateway that "has no technical restraints in providing access to the information and in deciding when to delete it", the use of PETs may produce considerable challenges when there is a change in compliance rules, or the requirements entail "a differentiation of disclosure of the information".[300] As explored in Chapter 5, PETs display different features, and are often implemented in a joint fashion to mitigate their respective shortcomings.

Against this backdrop, cryptocurrencies' networks offering architectural *transparency* and (some) transactions being *anonymous* does not seem paradoxical, but a combination of multi-faceted elements. The combination does not exclusively concern the IoM, as these concepts have long coexisted in the areas of online communication and financial transactions. Still, one shall not forget two aspects. On the one hand, the impact exerted on DLT-based monetary ecosystems by techno-libertarian views is debated; the topic should neither be ignored nor overestimated. On the other hand, the IoM has long overcome Bitcoin, and the possible contrast between ideology and architecture is not mirrored in the same way by the variety of current use cases. While more than 10,000 cryptoassets have been deployed to this day,[301] the term IoM was created with regard to one, which perhaps blurred some beliefs concerning its traits.

Indeed, I argue nowadays one may distinguish between two types of IoM ecosystems:

i. The ones actively rejecting any intervention of the law and authorities, and only regulating themselves (if so) through code, a topic addressed in Chapter 6.
ii. The ones yielding to *accountability* needs, mainly to interact with the traditional financial system. In this context, research is investigating whether it is feasible for cryptocurrencies and CBDCs to comply with both *privacy* and *accountability* requirements.[302]

[299] Harvey J, Branco-Illodo I (2020), p 130
[300] ITU-T FG DLT (2019c), p 24
[301] CoinMarketCap (2022). European Central Bank (2022). UK Government (2022)
[302] *E.g.*, Goodell G, Aste T (2019). European Central Bank, Bank of Japan (2020). European Central Bank (2019). Berberich M, Steiner M (2016). Finck M (2019b). Karasek-Wojciechowicz I (2021)

2.3. The Uptake of Enhanced Disintermediation, Atomicity and Impacts on Accountability

Many new intermediaries are involved in cryptocurrency transactions, while enticing business prospects prompt also traditional financial intermediaries to offer related services. From a regulatory perspective, both categories of players can be reached by compliance measures. As suggested in Chapter 1, however, the IoM is witnessing new trends in *non-centralisation* and *disintermediation*. I describe them as cases of *enhanced disintermediation* as opposed to the more traditional *disintermediation* cherished by the "blockchain hype". These innovations are generating *anonymity* concerns and show how the fluid nature of the IoM alters the cryptocurrency landscape in terms of *(un)accountability* and transaction *opaqueness*. In this respect, since 2019 the FATF has been voicing a downward trend.[303] In particular, these solutions are challenging *identifiability*, *linkability*, and *traceability* as depicted above in Figure 1. While Chapter 3 addresses reduced *transparency* and increased *obfuscation* of cryptocurrency flows, this section focuses on key developments in techniques and tools of *enhanced disintermediation*. In doing so, it attempts a typology of these trends, by identifying four major breakthroughs fostering a new era for cryptocurrency transfers: (1) *atomic cross-chain swaps*; (2) *multi-layered* applications; (3) unhosted or self-hosted wallets; (4) decentralised exchanges (DEXes).[304]

These developments have a profound impact on the *anonymity* level of IoM ecosystems and leverage specific technologies to be analysed in terms of their concrete implementations. From a basic perspective, the degree of actual *disintermediation* featured by the IoM depends on the technical capacity to support *interoperability* between different blockchains and DLTs. Indeed, *(intra-blockchain) interoperability* is needed to allow the transfer of the increasing number of assets, platforms, and projects from an ecosystem to another.[305] As an example, trading bitcoins with ether without relying on conversion services offered by a third party – *e.g.*, a *centralised* cryptocurrency exchange (CEX). While providers of cryptoasset portfolios can manage ledgers compatible with multiple systems, *intra-blockchain interoperability* still poses technical issues.[306] Notwithstanding multi-blockchain compatibility schemes, the result

[303] Financial Action Task Force (2019). Financial Action Task Force (2020d). Financial Action Task Force (2020b). Financial Action Task Force (2020a)
[304] The order of these instances of *enhanced disintermediation* mirrors the one used in this section and serves a narrative purpose only. Nonetheless, *atomic cross-chain swaps* play a key role in obtaining disintermediation.
[305] *Interoperability* can be described as the feature of a system able "to provide services to and accept services from other systems and to use the services so exchanged to enable them to operate efficiently together". ISO (2017) ISO/IEC 30182:2017(en), cited by Zuech K, Wöhnert K H, Skwarek V (2019), p 155
[306] Quiniou M (2019), pp 62-64. While *intra-blockchain interoperability* defines the "overall capacity of blockchains to exchange information with other blockchains", *inter-operability* refers more broadly to the "capability of blockchains to exchange information with other systems, outside of blockchains" Tasca P, Tessone CJ (2018)

is still not the same as direct, *disintermediated*, and *non-centralised* exchanges. The four mentioned breakthroughs above aim to change this paradigm and raise regulatory concerns.

2.3.1. Atomic cross-chain swaps and multi-layered protocols

Atomic swaps are key to true *disintermediation*, as they feature a smart contract technology that enables P2P cryptocurrency exchanges without third-party intervention. In particular, the notion of *atomic cross-chain swap* or *on-chain atomic swap* defines the case in which the protocol is embedded in a distributed ledger. In this case, the mechanism works as a "distributed coordination task where multiple parties exchange assets across multiple blockchains, for example, trading bitcoin for ether".[307] The model consists of a directed graph, where vertexes and arcs represent parties and proposed asset transfers, respectively.[308] Transactions are instant, and are either both finalised or cancelled. Indeed, the *atomicity* of a series of database operations refers to their indivisibility and irreducibility, and their sequence is called a *distributed atomic transaction*.[309] Evidently, the lack of third-party intervention implies lack of monitoring.

The disruptive idea underlying atomic swaps is that they provide a way to engage in these transactions even if there is no trust among participants. The protocol guarantees not only that all swaps shall take place, but also that for it to happen they must all conform to the system – if not, no transfer occurs. This means no participant can end up in advantageous circumstances by breaking the rules, and everyone is incentivised to adhere to the protocol.[310] This explains another definition of an *atomic swap protocol* as a "trust-free Byzantine-hardened form of distributed commitment".[311] Clearly, there is an important distinction between transacting cryptoassets through centralised platforms – *i.e.*, "gatekeepers" addressed by regulation – and the situation in which users can do so while remaining in control of their cryptoassets.[312] Hence, P2P trading causes a remarkable operational and architectural shift.

---

[307] Herlihy M (2018), p 245
[308] Ibid, p 247
[309] Ibid, p 246
[310] The goal is achieved through *hash timelocked contracts*, which are deployed by the transacting parties and take temporary control over the assets until the finalisation of the transaction is triggered by the contract receiving *matching secrets*. If not, a refund takes place (Herlihy M (2018), p 249. Satoshi (2019)) With *atomic swaps* the cryptoasset exchange "will initially be locked and can only be retrieved by the relevant counterparty using a cryptographic hash function. Thereby, a time-lock function ensures the refund of the two crypto-assets to the original counterparty in the case that one of the counterparties did not retrieve the crypto-asset within a predefined time period". European Securities and Markets Authority (2019), p 15
[311] Herlihy M (2018), p 246
[312] European Securities and Markets Authority (2019), p 15

Atomic swaps are useful to grasp the relationship between *multi-layered* protocols and *enhanced disintermediation*. Indeed, besides (i) *on-chain atomic swaps – e.g.*, the 2017 on-chain swap between Dacred and Litecoin – the cryptocurrency space houses *atomic swaps* that take place (ii) *off-chain*, and (iii) on the second layer of a blockchain.[313] This last category enables exchanges between selected currencies that take place on a secondary layer of nodes,[314] and suggests there is communication between different layers. Indeed, *decentralisation* can be enhanced by adding new "layers" of application protocols and often "interdependent forces shape the degree of centralisation in often more than one layers of DLTs".[315] Common examples are known as *layer-2 solutions*, such as the Lightning Network, used for the first off-chain atomic swap between Bitcoin and Litecoin.[316] As already argued, *decentralisation* is not a siloed trait and impacts on other features of a cryptocurrency ecosystem such as *anonymity*. Hence, *anonymity* is influenced by the presence of a multi-layered structure. While a network architecture can comprise multiple on-chain and off-chain layers for diverse reasons, this mechanism can be exploited to add one or more *anonymity*-enhancing layer(s) on top of an existing network.

2.3.2. Peer-to-peer (P2P) transactions and the FATF

Atomic cross-chain swaps enable P2P transfers across different blockchains or DLT networks without the intervention of a central entity. As mentioned in Chapter 1, P2P systems are networks of peers sharing information with each other directly and without relying on a third-party service.[317] Although the "blockchain hype" pivots around *disintermediation*, the IoM turns out to be more *centralised* and *intermediated* than expected, at least until *enhanced disintermediation* started to arise. In a truly *disintermediated* transaction, no monitoring activity can take place, nor it is possible to regulate an intermediary. Depending on the circumstances it may not even be feasible to know the transfers are taking place, let alone to identify senders, recipients, amounts, or to trace them. Although the "visibility of P2P transactions on public ledgers might support financial analysis and law enforcement investigations, especially when combined with other information sources", these techniques can be hampered by *anonymity*-enhancing technologies, as outlined in Chapter 3.[318]

[313] Choo H (2019)
[314] European Securities and Markets Authority (2019), p 45. Choo H (2019)
[315] Bodó B, Giannopoulou A (2019), p 5
[316] Choo H (2019)
[317] ITU-T FG DLT (2019c), p 4
[318] Financial Action Task Force (2021e), p 18

From an AML/CFT/CPF perspective, the FATF defines P2P cryptocurrency transactions as transfers performed without the involvement of a regulated entity.[319] When cryptocurrency users perform this type of transfers, they do not rely on the services of third parties. As outlined in Chapter 4, current AML/CFT/CPF frameworks are intermediary-based and P2P transactions fall outside their scope. Nonetheless, the FATF stressed the risk they can be used to bypass controls, as P2P transfers can be both used for legitimate activities and exploited to for criminal purposes, which is rendered even more worrisome given the rapid evolution of the sector.[320]

Data provided by analytics companies on P2P transfers is significant, but there is no consensus on the size of the sector. The difficulty in obtaining precise data mirrors "the challenges and limitations inherent in this kind of research with blockchain analytics, in terms of coverage, timeliness, accuracy and reliability, even if P2P transactions are recorded on public ledgers".[321] If it were to become mainstream for a significant portion of cryptocurrency activity to take place P2P, the effectiveness of AML/CFT/CPF measures would be challenged radically.

2.3.3. Self-hosted cryptocurrency wallets and decentralised custody

As mentioned above, despite *enhanced disintermediation* to this day the world of cryptocurrencies is still more *intermediated* and *centralised* than the hype would suggest. In this respect, although a blockchain system is *decentralised* when the history of transactions is recorded and maintained immutably by a *distributed* network of nodes, the "decentralised nature of a blockchain network does not, however, apply to the custody and secure storage of the keys that control the individual wallets on that network".[322] Indeed, most cryptocurrency users hold their coins in so-called custodial wallets, also known as hosted wallets. The value of cryptocurrencies never leaves the network, and they are stored in wallets that resemble more keychains than traditional wallets. It is well-known there are different types of cryptocurrency wallets, whose function is to help manage addresses and private keys.[323] The choice among the different options depends on individual preferences and expertise. A user accesses and spends the coins associated with a given address through the corresponding private key, as outlined in

[319] "VA transfers conducted without the use or involvement of a VASP or other obliged entity" (Ibid, p 18)
[320] The FATF urges jurisdictions and service providers to single out those P2P transfers that pose higher and lower risk, and to understand the different risk profiles, where "relevant factors that could, depending on the design of the VA, potentially impact the extent to which users engage in P2P transactions include the VA's accessibility and protocols that control the VA's privacy, transparency, security and associated transaction fees" (Ibid, p 18)
[321] Ibid, p 18
[322] Wang F, De Filippi P (2020), p 6
[323] Whitehouse-Levine M, Kelleher L (2020), p 5

Chapter 1. Because private keys act as an authentication code that grants access to funds, the different options come with strings attached in terms of privacy and security.[324]

From a first perspective, wallets are "hardware" when they consist of devices like USB pen drives (*e.g.*, Ledger Nano, Trezor), or "software". In turn, "software" wallets can be "desktop", "mobile" or "web" wallets.[325] "Desktop" and "mobile" wallets are applications installed on a computer (*e.g.*, Bitcoin Core, Electrum) or on a smartphone (*e.g.*, Mycelium, Coinomi), respectively. They do not involve the services of an intermediary, and the software is executed only on the device. On the contrary, "web" wallets are accessed through Internet browsers or apps, and can be either "hosted" (*e.g.*, Coinbase) or "non hosted" (*e.g.*, MetaMask). This means the wallet can be "custodial", where a third party offers storage services and has custody of users' private keys, or "non-custodial", when users retain custody of their private keys. Given the differences among "software" wallets, the fact that users interact with their wallet through an app does not mean the wallet is "hosted" – *i.e.*, that a third-party entity is storing their private keys. Lastly, wallets can be classified as "hot", when they are connected to the Internet, or "cold", when private keys are stored offline.[326] The decision to make use of a "hot" or "cold" wallet is significant in terms of privacy and security, as "cold" solutions are not constantly exposed to the dangers stemming from connectivity to the Internet (*e.g.*, cyberattacks, thefts).

Hence, custodial wallets are not the only available means to store and use cryptocurrency funds. On the contrary, a type of P2P transaction that is currently worrying AML/CFT/CPF regulators and enforcement agencies relates to "VA transfers between two unhosted wallets whose users are acting on their own behalf".[327] These wallets are known as self-hosted or unhosted or private and are non-custodial, which means users are the sole holders of their private keys and have full control of their cryptocurrency funds. In this way they can perform P2P transactions, which achieves the *disintermediation* goal. To explain the importance of users retaining full custody it was argued that "from a purely technical perspective (notwithstanding legal and contractual obligations), ownership of assets on the blockchain is equated with control of the assets, which is managed through the private keys associated with a wallet that contains the assets". It follows that when exchanges control the private keys associated with the wallets of their customers, they also control their funds, given that "custody of these keys

[324] Pocher N (2021b)
[325] Another subcategory of "software" wallets is that of "paper" wallets, although this type is argued to be obsolete. It consists of a printed QR code or a hand-written piece of paper.
[326] Sharma TK (2022)
[327] Financial Action Task Force (2021e), p 18

ultimately implies full control of the funds stored in that account".[328] From an AML/CFT/CPF perspective, in P2P transactions there is clearly no third party to hold *accountable* for monitoring, as no regulated intermediary is involved. Evidently, the traditional intermediary-based "active cooperation" approach, outlined in Chapter 4, ends up empty-handed, which leaves a gap where illicit activities can thrive avoiding the scrutiny of regulators and supervisors.

These considerations prompted the FATF, the EU, and other authorities such as FinCEN to take a stand against such instruments, especially because of possible combinations with obfuscation methods outlined in Chapter 3 – *e.g.*, "privacy coins" and advanced services that reduce transaction *transparency*.[329] The topic of self-hosted wallets from a compliance perspective will be addressed Chapter 4, also with reference to the impacts on the "crypto travel rule" debate.[330] Nonetheless, it can be anticipated the regulatory issue is twofold. On the one hand, self-hosted wallets ordinarily interact with regulated providers of cryptocurrency-related services. Indeed, cryptocurrency funds can originate from a self-hosted wallet and be sent to a hosted wallet, or vice versa. In these cases, when regulated entities receive a cryptocurrency transfer from a self-hosted wallet, they are required to comply with AML/CFT/CPF rules, hence they "should obtain the required originator information from their customer".[331] On the other hand, true P2P transactions, taking place between two self-hosted wallets, are equally possible.

Against this backdrop, regulators are considering restrictions on the use of non-custodial wallets, in the form of bans or threshold limits. These initiatives are starkly criticised by some cryptocurrency communities and by defenders of anti-surveillance. In their view, a restrictive attitude would be detrimental to values such as individual freedom, privacy, autonomy, and financial inclusivity, as well as it would hamper the use of self-hosted wallets as non-monetary value holders and the use of cryptocurrencies as true digital cash.[332] Also in this case, data on the share of cryptocurrency activity that goes through self-hosted wallets is provided by

[328] Wang F, De Filippi P (2020), pp 6-7. The impact is not limited to the financial sphere. It more generally relates to individuals exerting *control* on their digital IDs, which is pivotal in the "self-sovereign identity" debate. While the topic falls outside the scope of this work, digital ID systems are strongly linked to AML/CFT/CPF – *e.g.*, from the KYC perspective. The related "principle of control" is that per which "individuals must control their identities, they should always be able to refer to it, update it, or even hide it – even if others can make claims about these identities". Ibid, p 10. The private law impacts of different types of wallets on ownership and custody of cryptocurrencies, and considerations on the legal treatments of these instruments, are not addressed in this work. An overview of the importance of self-storage and self-custody is provided by Barresi RG, Zatti F (2020). Key issues related to the ownership of DLT-based cryptoassets are addressed by Siena J (2022).

[329] The Financial Crimes Enforcement Network (FinCEN) belongs to the US Department of the Treasury and is responsible for collecting and analysing information about financial transactions to combat money laundering, terrorism financing and other types of financial crimes.

[330] Pocher N (2021a)

[331] Financial Action Task Force (2019), p 30

[332] Pocher N (2021b). Whitehouse-Levine M, Kelleher L (2020)

analytics companies, but it is difficult to obtain accuracy. According to a recent report, in 2020 52% of Bitcoin's payment volume was sent to exchanges, while 40% to self-hosted wallets.[333]

2.3.4. Decentralised exchanges (DEXes) and decentralised finance (DeFi)

The most common ways to buy and exchange cryptoassets still relies on centralised trading venues, known as *centralised exchanges* (CEXes). The use of this type of intermediary services is at odds with the description of the IoM as an ecosystem for people to dispose of their own money directly.[334] In recent times, however, the field has witnessed the emergence of a new type of trading venues with no central authority, free from regulatory constraints – known as *decentralised exchanges* (DEXes) – and of so-called *decentralised protocols*. These projects fall within the domain of DeFi applications, which include stablecoin projects (*e.g.*, DAI), lending platforms (*e.g.*, Aave, Compound), cryptoasset DEXes (*e.g.*, Bancor, Kyber, Uniswap, Sushiswap, Pancakeswap), derivative services/DEXes (*e.g.*, Synthetix, dYdx).[335]

To date, DeFi has largely developed on the Ethereum blockchain, although specific projects were implemented on other networks such as EOS, TRON, and Cosmos.[336] DeFi represents "a whole ecosystem of financial services realised through smart contracts deployed on public distributed ledgers",[337] where "the role of the financial intermediary is taken over by the self-executing computer code".[338] The composability of the space warranted the label "financial Lego" or "money Lego" – *i.e.*, the various protocols and applications can interact with each other and be combined to reach the optimal transaction experience for the users.[339] The total value of DeFi projects reportedly amounted to USD 1 billion in January 2020, USD 27 billion in January 2021, USD 60 billion in April 2021, and USD 40 billion in November 2022.[340]

DEXes, among the primary DeFi applications, are governed by online communities of anonymous stakeholders,[341] and offer marketplaces of cryptocurrency and/or other tokens built directly on DLT networks. The opposite happens with CEXes, which are centrally operated by

[333] CipherTrace (2021), p 6
[334] Choo H (2019)
[335] Amler H, Eckey L, Faust S, Kaiser M, Sandner P, Schlosser B (2021), p 182. Aramonte S, Huang W, Schrimpf A (2021), p 23
[336] Katona T (2021), p 78
[337] Amler H, Eckey L, Faust S, Kaiser M, Sandner P, Schlosser B (2021), p 181. A related definition describes DeFi as "an ecosystem of decentralised applications which is built on top of permissionless smart contract platforms to mimic and extend traditional financial services" (Eikmanns BC, Mehrwald P, Sandner PG, Welpe IM (2023), p 1)
[338] Katona T (2021), p 78
[339] Amler H, Eckey L, Faust S, Kaiser M, Sandner P, Schlosser B (2021), p 181. Katona T (2021), p 81
[340] Chainalysis (2022)
[341] Barbereau T, Smethurst R, Papageorgiou O, Rieger A, Fridgen G (2022), p 6043

(for-profit) entities – *e.g.*, Coinbase, Binance, Kucoin, FTX, CEX.io, OKEx, Kraken.[342] The basic concept in DEXes is that trading on them only requires an unhosted wallet.[343] The service is non-custodial and transactions are not *intermediated* in any way, but rather governed by smart contracts,[344] which serve the purpose of depositing the assets users want to exchange.[345] While they present a series of advantages, their use undoubtedly requires specific skills.[346]

According to data provided by analytics companies, the transaction volumes of DEXes are increasing at a considerable speed. Because there is no intermediary governing them, an attractive element is that fees and commissions tend to be minimal or even non-existent.[347] The world of DEXes, however, is populated by different species of platforms. From a first perspective, the specific setup of a DEX impacts the type of cryptoassets it can offer. In this respect, they can be currency-centric or currency-neutral. To date, they can offer only crypto-to-crypto exchanges, and most of them trade only Ethereum-based tokens. In other words, DEXes do not currently support cross-chain transfers,[348] and cannot access the market of fiat money. Cross-chain experiments, however, are underway. Meanwhile, while users can usually trade a wider variety of assets on a DEX than on a CEX – in DEXes there is no preliminary verification of the safety of listed assets – CEXes are still offering more options of trading and investment.[349]

Secondly, while some projects pursue the creation of platforms for a *decentralised token exchange* – *e.g.*, Uniswap, Airswap –, others pursue the combination of multiple models of DEX swaps – *e.g.*, MetaMask.[350] Parallelly, DEXes such as Bancor and Kyber are "simplified", while other projects are not. More specifically, the architecture of DEXes can feature either (i) an off-chain order book and order matching with on-chain settlement – by smart contracts or by relayers/miners –, such as IDEX and EtherDelta, or (ii) an on-chain order book, order matching, and settlement by miners, such as OasisDEX. This means DEXes can vary substantially in their decentralisation levels. When the order book is held off-chain, in the architecture of a

[342] A CEX operates like any other exchange. There is a matchmaking algorithm that regulate supply and demand, and an order book that stores the users' orders. Wiesflecker L (2021)
[343] Yazdanparast E (2021). Choo H (2019). Wiesflecker L (2021)
[344] European Securities and Markets Authority (2019), p 44. Indeed, DEXes offer the key functions of CEXes, including "order books (or Automated Market Maker (AMM)), a trading venue, a matching system, and security functions. The difference to centralised exchanges is that all these functions are decentralised. To this end, a DEX is not based on internal servers and its own IT infrastructure but acts as a decentralised application (dApp) on a blockchain" (Wiesflecker L (2021))
[345] Ibid
[346] Choo H (2019). DEXes make use of atomic swaps. Real-time on-chain trading is currently hampered by transactions being processed by miners.
[347] Yazdanparast E (2021)
[348] Choo H (2019). Lin L (2019).
[349] Yazdanparast E (2021)
[350] WEF (2020), pp 18 and 28

DEX there is a centralisation point. In these cases, they might be within regulatory reach.[351] In this respect, it was noted how often DEXes "don't collect KYC information on their users and have no way of freezing funds like a centralised exchange; sometimes, this power lies with the individual DeFi projects themselves".[352] A new generation of DEXes, however, no longer makes use of order books but of "liquidity pools" – in brief, "smart contracts that hold balances of two unique tokens and enforce rules around depositing and withdrawing them".[353]

In light of their activities, DEXes would in theory fall within the FATF's and the EU understanding of providers of cryptocurrency services. Because they are not single entities, however, it can be argued it is considerably challenging to impose compliance on them. That is, at least, through traditional gatekeeper-based models and despite the considerations regarding their actual degree of *centralisation* and power re-concentration put forward in Chapter 1. In this respect, notwithstanding the conceptual value of *embedded regulation* explored extensively in Chapter 6, in the context of DeFi communities and stakeholders its implementation could indeed prove difficult.[354] Additionally, to use the services offered by a DEX there is no need to undergo a registration procedure, the possession of a *self-hosted* wallet is enough. It is for this reason they are usually described as *anonymous*,[355] and indeed *anonymity* in the form of absence of authentication and KYC is described as one of the core reasons to trade on a DEX, together with a claimed higher security when compared to CEXes.[356]

Analytics companies provide insights into the use of these platforms for money laundering. A 2021 report highlights that, while there is an increase in legitimate use, the percentage of transactions related to criminal activity goes down: "2020 crypto crime was $1.9 billion in 2020, down 57% from 2019's $4.5 billion".[357] The same report, however, argues DeFi is becoming "the next major threat vector for fraud and money laundering: half of all thefts in 2020, totalling $129 million, were DeFi-related hacks", while some CEXes are transforming into DEXes to avoid regulation.[358] Moreover, DEXes are vulnerable to be used as money mixers, introduced in Chapter 3, as it happened with Uniswap in the 2020 hack to KuCoin.[359]

---

[351] EtherDelta was charged by the US SEC for exchanging unregistered securities. Choo H (2019)
[352] CipherTrace (2021), pp 11-12
[353] On liquidity pools and role of liquidity providers: Dex & Cex (2021)
[354] Barbereau T, Smethurst R, Papageorgiou O, Rieger A, Fridgen G (2022), p 6050
[355] Choo H (2019)
[356] Wiesflecker L (2021)
[357] Ibid, p 6
[358] Ibid, p 6
[359] Ibid, p 45. In this respect, regarding the risk of illicit abuses it was reported that "even 2020's largest theft, the $281 million hack of the centralised exchange KuCoin, ultimately involved DeFi as criminals attempted to launder the stolen funds through one of the largest decentralised exchanges in the world—Uniswap" (Ibid, pp 11-12)

2.4. Conclusions

Leveraging the overview of the socio-technical nature, foundations and development of IoM ecosystems provided in Chapter 1, in this Chapter I presented a first part of considerations on the concepts of *anonymity* and *transparency* in the IoM. In Chapter 3, the analysis will focus on *obfuscation* and *traceability*. In particular, I addressed in this chapter the role of encryption in the early stages of the IoM against the backdrop of the cyber-libertarian movement and introduced the relation between *anonymity* and the impacts of allowing transactions that cannot be monitored. After singling out the scope of this analysis, I explored the multifold concepts of *anonymity* and *transparency* in the IoM and related transactions, attempting disambiguation efforts at the crossroads between different conceptual levels pertaining to the cyberspace, IoM ecosystems, financial transactions. In this chapter I focused primarily on achieving a higher level of conceptual clarity about constitutive elements of the domain, on which to ground the following investigation and the final conclusions. In doing so, the analysis pivoted around the notion of *accountability* and on how it is affected by *enhanced disintermediation*.

Through an exploration of the characteristics featured by cryptocurrency-related *anonymity* and *transparency* within an AML/CFT/CPF context, I differentiated *anonymity* from *privacy*, and I defined IoM *anonymity* as: (a) "conceptually granular", compounding the technical metrics of *traceability*, *linkability*, *identifiability*, *identification, pseudonymity*, *confidentiality*, *privacy,* (b) "context-specific", on the grounds of the role played by *identifiability* in AML/CFT/CPF frameworks, (c) "observer-dependent", as it can be assessed only with respect to a specific actor trying to reach identification, (d) presenting a broader meaning than the understandings of *anonymity* that are featured by other regulatory frameworks (*e.g.*, data protection), since it does not distinguish between *anonymisation* and *strong pseudonymisation.* Meanwhile, the IoM notion of *transparency* emerged as twofold and torn by the fact that the concept of *transparency of the ledger* and *ledger operations* is constitutively distant from the notion of *financial transparency.* Thus, I reframed the alleged paradox of blockchains featuring *anonymity* and *transparency* traits into a combination of features whose interplay can be explored and measured by using a teleological methodology. Finally, I addressed the part of the IoM world that pursues *enhanced disintermediation*, in terms of P2P transfers, major techniques such as atomic cross-chain swaps and multi-layered protocols (*e.g.*, layer 2 solutions), self-hosted wallets and DEXs, showing the impact on *accountability* from an AML/CFT/CPF standpoint.

Some threads can be identified in Chapter 2: (i) IoM *anonymity* is situated at the crossroads of *online anonymity* and *financial confidentiality*, (ii) the issue of *anonymous* exchange of

information precedes the “blockchain hype”; (iii) cryptocurrencies are not the first instance of tension between private transactions and *accountability*; (iv) the quest for *transparency* to ensure *accountability* is common in information networks; (v) the *transparency* of compliance regimes differs from the one of public blockchains; (vi) the issue of cyberspace and IoM *anonymity* is of socio-technical nature; (vii) AML/CFT/CPF provisions pivot around the concepts of *identification* and *verification* of an *identity*; (viii) a subject or an item is not *identified* or *anonymous*: these traits range on a spectrum; (ix) *anonymity* is a concept dependent on the observer; (x) a subject is *identifiable* if the entity in charge of *identification* can access the information required by the applicable framework; (xi) *anonymity* and *transparency* can be reconciled by using benchmarked trade-offs and a teleological methodology; (xii) in AML/CFT/CPF, an *anonymous* transaction is one that cannot be related to an *identified* or *identifiable* individual; (xiii) AML/CFT/CPF and data protection embody different understandings of *anonymity*; (xiv) the IoM is more intermediated than expected, but disruptive new trends of *enhanced disintermediation* pose substantial *anonymity* risks.

3. Obfuscation and Traceability: an Accountability-Based Approach to Anonymity

"*It turns out that the very notion of anonymity itself, in such complex multi-party systems as decentralised cryptocurrencies, has been until now very poorly understood, and is anything but clear-cut*".
Amarasinghe N, Boyen X, McKague M (2021)

3.1. Introduction

The unsatisfactory level of Bitcoin's *anonymity* prompted the implementation of new techniques both within the same network and to design other ecosystems. In this way, developer communities pursued *fungibility* and user *unaccountability* for cyberspace transactions, thus bypassing regulatory constraints and governmental surveillance. The advent of complex and *anonymity*-oriented models was accompanied by an increasing interest of institutional and corporate stakeholders in the IoM space, which transformed into projects of stablecoins and CBDCs, addressed in Chapter 5. In this context, the array of *privacy* concerns grew wider and generated new sensitivities to the possible exploitation of financial data by a vast range of actors – *e.g.*, if transactions are not performed *anonymously*, "a malicious merchant may sell customers' transaction information to third parties for financial benefit".[360]

The onset of *anonymity*-enhanced trends is also linked to the intelligence techniques applied to the blockchain space. As Bitcoin transactions became popular and AECs were developed, experts and law enforcement professionals devised specific investigative strategies to trace these transfers. Later, analytics solutions were requested by newly regulated entities – *e.g.*, exchanges and custodian wallet providers, as outlined in Chapter 4. As it often happens with innovation, new opportunities gave rise to a race where "in response to a new technological shift, criminals and consumers alike are increasingly finding new ways to evolve".[361]

This evolution of the IoM caused an overall enhancement of the *obfuscation* level of cryptocurrency transactions, which challenges the AML/CFT/CPF framework. The FATF frequently reported this, noting how the IoM is increasingly populated by AECs, "mixers and tumblers,

[360] Li Y, Yang G, Susilo W, Yu Y, Ho Au M, Liu D (2021), p 679
[361] Reynolds P, Irwin ASM (2017), p 1

decentralised platforms and exchanges, privacy wallets, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows", as well as innovative "business models or activities such as initial coin offerings (ICOs) that present ML/TF, fraud and market manipulation risks". In this context, there is a worrying rise of new typologies of illicit financing such as "virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner".[362]

The laundering process provides benchmarks to understand the debate on the degree of *obfuscation* and *traceability* of cryptocurrency transfers. Hence, in the following sections I will provide an overview that contextualises the regulatory analysis of Chapter 4. Indeed, the link between *obfuscation*, *traceability* and money laundering is clearly enshrined by the literature and legal initiatives. This is not surprising, since cryptocurrency *anonymity* has been mostly addressed in terms of possible misuses of the financial system. Meanwhile, forensic activities are a major source of insights into IoM *anonymity* from a socio-technical perspective.

3.1.1. Transaction obfuscation and the money laundering process

From an objective-oriented standpoint, the goal of AML/CFT/CPF measures is to prevent criminals from enjoying and profiting from ill-gotten proceeds, hindering their capacity to benefit from the revenues of illicit activities. The strategy is to thwart the capacity to "wash" these proceeds, thus making it difficult to provide them with a legitimate appearance. This explains why the first prevention and repression measures originated from enforcement operations against crimes that produce substantial returns – *e.g.*, organised crime, trafficking in drugs and firearms, corruption.[363] In the 1970s and 1980s, in the U.S. investigators started considering "follow the money" techniques as a key part of their effort to unravel criminal organisations.

In the IoM, the relationship between money laundering, *obfuscation* and *anonymity* pivots on two aspects: (i) money laundering is a "process", and (ii) the regulatory response consists of two complementary approaches. From the first perspective, money laundering does not consist of a single act, but of a "process". For the sake of clarity, the latter is usually described as composed of three phases depicting the steps illicit profits go through to be "laundered" and come out "clean": *placement*, *layering* and *integration*. Briefly put, in the (i) *placement* phase ill-gotten proceeds are introduced into the financial system, if needed (*i.e.*, if not already there);

[362] Financial Action Task Force (2021e), p 7
[363] Gelemerova L (2009), pp 34-36

in the (ii) *layering* stage their origin is concealed through as many complex transactions as possible; and finally (iii) *integration* sees cleansed funds being (re)integrated into the system.[364] Evidently, this threefold layout is a simplification, and in real-life scenarios these stages are not siloed. Laundering methods are often complex – *e.g.*, they may involve the use of different corporate vehicles and be performed at a global scale. Because it is difficult to find a clear separation between these phases, and the actions pursuing the three different goals tend to overlap, nowadays they are not considered a comprehensive representation of laundering dynamics. Nonetheless, they can play a benchmarking role when analysing the risks tainting the IoM.

The added value of using cryptocurrencies reportedly stems from three elements that enable the exploitation of blind corners of the prevention system and allow these funds to covertly go through the laundering stages.[365] They are: (a) *decentralisation*, in terms of operating (partially, at least) outside the regulated financial system; (b) *pseudonymity*, that provides opportunities to conceal *real-world identities*; (c) *instant* conclusion of transactions and *speed* of payment, that challenge the effectiveness of due diligence checks.[366] I previously outlined the differences between IoM ecosystems and the actors involved, focusing on *enhanced disintermediation*, cross-blockchain exchanges and DeFi. Hence, the three elements mentioned above sub (a), (b) and (c) should be interpreted flexibly; the same arguments do not apply in the same way to all IoM transactions. As exemplified below, different ecosystems feature various levels of vulnerabilities to illegal exploitation. On top of this, significant concerns affect areas currently unregulated and/or where effective compliance, implementation and/or enforcement are harder to attain – *e.g.*, DEXes, self-hosted wallets (Chapter 2), the "crypto-travel rule" (Chapter 4).

Cryptocurrencies seem to be most useful in the *layering* phase, where their use is more frequent. *Layering* is a key component in all studies on the criminal use of cryptocurrencies and is facilitated by the cross-border nature of their ecosystems and the growing variety of options in terms of service providers.[367] In this respect, in schemes of *virtual-to-virtual layering* illicit actors engage in multiple exchanges from/to different cryptocurrencies to conceal the

[364] Ecorys, CEPS (2017), p 57
[365] Silva Ramalho D, Igreja Matos N (2021), p 501
[366] Ibid, p 501. The most recent version of the recast proposal of the Fund Transfers Regulation, addressed in chapter 4, reads as follows. Council of the European Union (2022b). Recital 22a: "Compared to funds transfers, transfers in crypto-assets can be carried out across multiple jurisdictions at larger scale and higher speed due to their global reach and technological characteristics. In addition to the pseudo-anonymity of crypto assets, this offers criminals the opportunity to carry out at high speed large illicit transfers while circumventing traceability obligations and avoiding detection, by structuring a large transaction into smaller amounts, using multiple seemingly unrelated DLT addresses, including one-time use DLT addresses, and automated processes".
[367] In trade-based laundering, the complexity of international trade and the interconnection of supply chains are exploited to transfer value – *e.g.*, false invoices (*e.g.*, over-/under-invoicing) or representations of goods (*e.g.*, over-/under-shipment or false descriptions) – and violate customs and tax regulations (*i.e.*, smuggling and fraud).

origin and transaction history of their funds, making use of manifold service providers. Nonetheless, cryptocurrencies can be exploited effectively throughout the whole laundering cycle.[368] Indeed, also for *placement* and *integration* launderers can leverage the almost instantaneous and cross-border nature of these transfers to avert the time-consuming and regulated traditional financial paths. From a *placement* perspective, they may exploit the low-risk opportunity to swiftly open and access cryptocurrency accounts, which allows them to convert and consolidate their profits easily and *(pseudo)anonymously*. Indeed, *pseudonymity* allows flagged or blacklisted actors – *i.e.*, people or entities that cannot enjoy the services of regulated entities because of previous flagging or blacklisting (*e.g.*, sanctioned entities or individuals) – to bypass restrictions posed by authorities to their operations.[369] Finally, in the *integration* phase they can be used to buy an increasing variety of goods and/or services, options bound to increase in the future. Reportedly, "privacy coins" are increasingly adopted in darknet markets and by ransomware actors, while for *settlement* bitcoins or fiat currencies are usually chosen.[370]

From a second point of view, the regulatory response to the money laundering risk encompasses two complementary approaches. On the one hand, criminal sanctions are imposed on launderers – *i.e.*, money laundering is a crime in most jurisdictions.[371] In this respect, an important evolution affected predicate offences – *i.e.*, crimes that generate the proceeds whose "washing" is deemed by law as money laundering.[372] By expanding the list of predicate offences, regulators widen the scope of application of the AML/CFT/CPF framework itself. On the other hand, a set of AML/CFT/CPF provisions are included in civil/administrative regulatory frameworks, depending on the legal system.[373] These norms thrust compliance duties on specific entities, thus partially decentralising oversight – *i.e.*, as explored in Chapter 4, regulated entities cooperate with authorities by monitoring financial activities. What these entities have in common is a substantial involvement in financial and business operations, in various

[368] Irwin ASM, Slay J, Kwang Raymond Choo K, Lui L (2014). Fanusie YJ (2020). Mabunda S (2018). CipherTrace (2021). Desmond DB, Lacey D, Salmon P (2019)
[369] Silva Ramalho D, Igreja Matos N (2021), p 501
[370] Financial Action Task Force (2021d), p 23. Reportedly, while cybercriminals usually want to be paid in bitcoin, at times ransomware operators offer discounts to victims willing to pay in "privacy coins" to reduce *transparency*.
[371] The issue concerning the definition of "money laundering" and the role of international and EU initiatives in respect to criminal law efforts – with specific reference to Directive (EU) 2018/1673 – is addressed in Chapter 4.
[372] "Predicate offences" are components of a larger crime, the latter in this case being money laundering or terrorist financing. While initial actions focused on drugs-related offences, the scope was later expanded to a plethora of serious crimes. Today, as per Directive (EU) 2018/1673, "any kind of criminal involvement in the commission of any offence punishable, in accordance with national law, by 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" can be a "predicate offence" for ML. A list of crimes is included *per se* (Article 2(1)(1)).
[373] Boundaries between civil, administrative and criminal frameworks may not be as explicit. Frequently, the same piece of legislation provides for different kinds of sanctions for violations of different norms.

ways and to different extents, and their "active cooperation" is deemed conducive to alerting authorities if suspicions arise. Hence, businesses such as banks, law firms, notaries or casinos are tasked to follow the measures addressed in Chapter 4 – *e.g.*, KYC and CDD. The publications released by the FATF and supervisory organisations often address these entities to help them fulfil their role. Moreover, these "active co-operators" and law enforcement bodies are the actors that benefit the most from improvements in the services of analytics companies. This has contributed to the development of new strategies and technologies, striving to make it easier for regulated stakeholders to comply with the ever-expanding AML/CFT/CPF regime.

Besides considering cryptocurrencies as one of the possible means to the laundering end – *i.e.*, focusing on their use within this process – it is also possible to look at how they can be laundered themselves. This means considering cases in which criminals are not (only) trying to cleanse fiat money by means of cryptocurrencies, but (also) want to conceal the illegal origin of their crypto funds – *i.e.*, cryptocurrencies themselves are proceeds of the predicate offence. This dynamic is called "cryptocurrency laundering" or "crypto-cleansing", and originated from the uptake of "mixing/tumbling" techniques, initially labelled "Bitcoin mixing".

Instances of laundering of cryptocurrencies can take place within a process initiated with fiat proceeds, for instance in the *layering* phase, or independently. Laundering "of" and "through" cryptocurrencies often happen in a conjoined fashion – *e.g.*, proceeds originally in fiat money can be converted into cryptocurrencies that are later "crypto-cleansed" in the *layering* phase. This testifies to the intricate interlinks between the three stages. It is in this context the FATF highlighted the risks posed by *virtual-to-virtual* operations performed by/through unregulated providers.[374] Nonetheless, both in laundering "through" and "of" cryptocurrencies the goal is to obfuscate the chain of transactions and hinder investigations and enforcement.

3.1.2. Anonymity as a red flag indicator

Chapter 2 introduced the socio-technical nature of IoM's *anonymity* and *transparency*, and the value of applying a teleological approach to their definition. As noted there, the AML/CFT/CPF framework does not provide a definition of *anonymity*. Nonetheless, insights can be drawn from the understanding of *anonymity* that emerges from the FATF's report on "red flag indicators". In this context, the organisation outlines benchmarks to signal regulated entities and

[374] Fruth, J (2018)

authorities to proceed with care in certain situations.[375] The goal is to help identify *risky* and *suspicious* operations and/or customers based on a list of circumstances.[376]

The FATF published a comprehensive list of indicators related to activities in virtual assets in 2020, with a subsection on *anonymity*, complementary risk factors in 2021.[377] These risks are vulnerabilities inherent to the technology or generated by the ecosystem. However, the FATF does not consider *anonymity* itself as an automatic suggestion that a transaction is illicit. Indeed, legitimate reasons can drive behaviours in abstract *suspicious* – *e.g.*, hardware wallets increase the *anonymity* level of an operation but are also means of protection against thefts –, but in these cases further scrutiny is. Hence, in compliance with the RBA, addressed in Chapter 4, the risk must be assessed considering the specific customer and business relationship.

In Table 1 below I list FATF's risk factors, with a summary of the suspicious elements and the type of *anonymity* that comes into play – *e.g.*, what is the aspect that grounds FATF's risk evaluation. In particular, I assess whether each case of *anonymity* is linked to the type of cryptocurrency (*e.g.*, privacy coins, coins linked to fraud), service (*e.g.,* DEXes, mixing services), communication (*e.g.,* VPNs, proxies), wallet (*e.g.,* self-hosted), wallet use (*e.g.,* shell wallets). In turn, I provide an evaluation of whether the case of *anonymity* is an example of *obfuscation* (grey shading), *enhanced disintermediation* (green shading), or is of another *specific* kind. As outlined in Chapter 2, these categories can be tied to *untraceability* and/or *unidentifiability* and/or *unlinkability*, depending on the specifics. In principle, more *anonymity* types can co-exist in a single risk indicator. However, I argue in each case one comes across as more evident.

	Text of the Risk Indicators [378]	**It is suspicious when:**	***Anonymity* is tied to:**
1	"*Transactions by a customer involving more than one type of VA,[379] despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins*"	a customer transacts in more than one type of cryptoasset and AECs, even if doing so requires the payment of additional transaction fees	*Type of Cryptocurrency (obfuscation):* Privacy Coins

[375] "Red flag indicators" are typical of frameworks grounded on the RBA, as outlined in Chapter 4. At the national level, self-regulating authorities issue indicators for their supervisees – *e.g.*, Central Banks and FIUs.
[376] Accordingly, regulated entities are required to apply enhanced CDD, submit an STR or even refuse to perform an operation. The different phases of AML/CFT/CPF compliance are outlined in Chapter 4.
[377] Financial Action Task Force (2020d), pp 9-10. Financial Action Task Force (2021e)
[378] Financial Action Task Force (2020d), pp 9-10
[379] As addressed in Chapter 1, in FATF's wording VA stands for "virtual asset", defined as "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". This work addresses the "cryptocurrency" subset.

2	"*Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin*"	a customer moves assets from a public and transparent blockchain to a CEX and then exchanges it with AECs	*Type of Cryptocurrency (obfuscation)*: Privacy Coins	
3	"*Customers that operate as an unregistered/unlicensed VASP[380] on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions*"	a customer operates on P2P platforms as an unregistered service provider, especially when there are concerns the customer handles a significant number of transfers and charges high fees	*Type of Service (disintermediation)*: P2P exchanges / DEXes	
4	"*Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation*"	there is abnormal activity in terms of level and volume of transactions, cashed out from wallets tied to P2P platforms	*Type of Service (disintermediation)*: P2P exchanges / DEXes	
5	"*VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms*"	cryptoassets are transferred to/from wallets tied to mixing services or P2P platforms	*Type of Service*	*(disinterm.)*: P2P exchanges/ DEXes
				(obfuscation): Mixing services
6	"*Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces*"	mixing services are used, suggesting the goal of obfuscating the flow between wallet addresses and darknet markets	*Type of Service (obfuscation)*: Mixing services	
7	"*Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet market-places, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports*"	funds are deposited or withdrawn to/from an address/wallet directly or indirectly exposed to sources known as suspicious, *e.g.*, darknet marketplaces, mixing services	*Type of Service (obfuscation)*: Mixing services	
8	"*The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders*"	funds are moved across borders through decentralised/unhosted, hardware/paper wallets	*Type of Wallet (disintermediation)*: Self-hosted wallets	

[380] In the FATF's wording, a VASP is a "virtual asset service provider". The notion is addressed in Chapter 4.

9	"*Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that sup-press or redact the owners of the domain names*"	users use proxies or DNS suppressing/redacting their owners	*Type of Communication (obfuscation)*: Anonymisers / proxies
10	"*Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP*"	users use an IP address associated with a darknet or a software enabling *anonymous* communication or transactions take place between users communicating through encrypted methods instead of regulated providers	*Type of Communication (obfuscation)*: Anonymizers / proxies
11	"*A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other*"	there are many wallets, seemingly unrelated, controlled from the same IP or MAC address	*Type of wallet use (obfuscation)*: Shell wallets
12	"*Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes*"	schemes whose design is not properly documented or is linked to fraudulent mechanisms such as Ponzi schemes [381]	*Type of Cryptocurrency (specific)*: New Asset / Ties to fraud
13	"*Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent*"	transfers from/to providers whose CDD/KYC is weak or non-existent	*Type of Service (specific)*: Non-compliant providers
14	"*Using VA ATMs/kiosks despite the higher transaction fees and including those commonly used by mules or scam victims; or in high-risk locations where increased criminal activities occur. A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the*	repeated use of cryptocurrency ATMs/kiosks for small transactions, even if fees are high and they are used by mules or scam victims, or in locations at	*Type of Service (obfuscation)*: ATMs / kiosks

[381] Ponzi schemes, prohibited in many countries, are a "fraudulent investment operation where the operator generates return for older investors through revenue paid by new investors, rather than from legitimate business activities or profits of financial trading. In a Ponzi scheme, many participants, especially those posteriors, are doomed to lose most of their invested money". The blockchain-based form exploits the lack of specific knowledge of users and investors. Chen W, Zheng Z, Ngai E, Zheng P, Zhou Y (2016)

	machine being in a high-risk area, or was used for repeated small transactions (or other additional factors)"	high-risk for criminal activities [382]	

Table 1: FATF's VA Red Flag Indicators related to *anonymity*

Against the backdrop of these benchmarks provided in 2020, the "market for anonymity-enhancing tools and methods is in rapid flux" and keeps posing considerable concerns.[383] In 2021 the FATF referred to other *obfuscation* techniques such as the use of chain-hopping and dusting (*i.e.*, transfer of small amounts of cryptoassets to random wallets), cases of *enhanced disintermediation* linked to *decentralised* applications, atomic swapping exchanges, and reported an increase in "privacy wallets" transfers that combine into a single transaction those of multiple people – *e.g.*, CoinJoin. In this context, the FATF identified two sets of actions to mitigate enhanced *anonymity*: (i) enforcement initiatives to close mixing platforms for operating as unregistered providers, (ii) registered providers delisting products such as AECs.[384]

Against this backdrop, to avoid or mitigate the risk of overfitting, introduced in Chapter 1, I heed the socio-technical and ever-evolving nature of the traits of *anonymity* and *transparency* of IoM ecosystems. To structure the analysis accordingly, I focus on the concepts of *obfuscation* and *traceability*, defined in Chapter 2. These notions are the key to explore:

- the interaction and possible combinations between the types of *anonymity* risks and the difference between laundering "of" and "through" cryptocurrencies;
- the "social" elements contributing to the *anonymity* and *transparency* level of an IoM ecosystem, with reference to the impacts exerted by (i) techniques pursuing the *obfuscation* of cryptocurrency flows and, (ii) intelligence strategies such as blockchain analysis;
- their repercussions of the specific methods deployed sub (i) and (ii) on the *accountability* level of the actors involved in cryptocurrency transactions.

Hence, the remainder of this chapter: (a) addresses the multi-layered nature of *obfuscation* techniques in their relationship with money laundering, where a key role is played by AECs, PETs and mixing, (b) contextualises their action vis-à-vis intelligence strategies, (c) provides a socio-technical framework to define an AML/CFT/CPF-specific concept of IoM *anonymity*.

[382] The risk of crypto ATMs emerges in the proposal to recast the Fund Transfers Regulation (see Chapter 4): "Crypto-ATMs can enable users to perform transfers of crypto-assets to a crypto-asset address by depositing cash, often without any form of customer identification and verification. Crypto-ATMs are particularly exposed to money laundering risks because the anonymity they provide and the possibility of operating with cash of unknown origin make them an ideal vehicle for illicit activities" (Council of the European Union (2022b). Recital 19b)
[383] Financial Action Task Force (2021d), p 23
[384] Ibid, p 23

3.2. Multi-Layered Methods to Obfuscate Financial Flows and the Role of Traceability

When it comes to the ways in which *obfuscation* and *traceability* come into play in the IoM from an AML/CFT/CPF perspective, it is important to consider the phenomenological interaction between the types of *anonymity* risks emerging from FATF's guidelines, and the difference between laundering "of" and "through" cryptocurrencies. Methods to obfuscate the flow can be combined in many ways, and it is useful to visualise a process composed of different stages, each of them corresponding to the activities performed by a launderer. In our example, Alice.

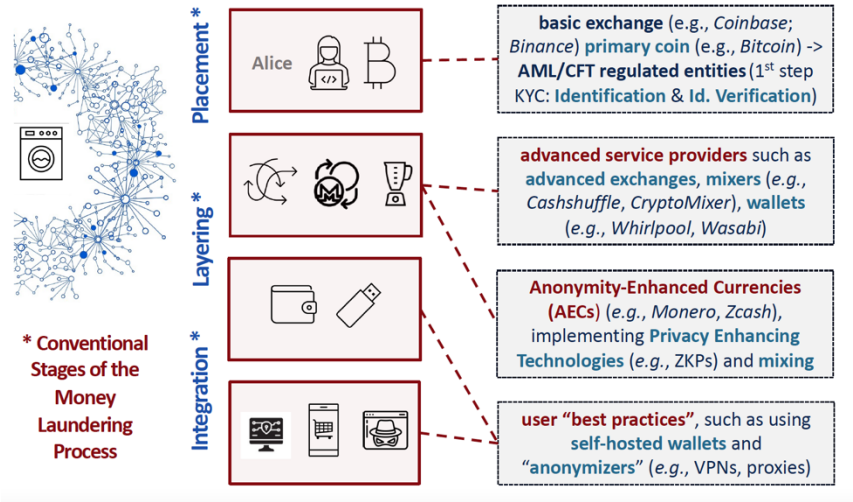

Figure 3: obfuscation of cryptocurrency flows

The laundering process could involve the steps taken by Alice in Figure 3, where the proceeds are originally in fiat money.[385] As mentioned above, a key step is *layering*. In particular:

1. *Placement/Layering*. Alices exchanges ill-gotten funds from fiat currency to a "primary" type of cryptocurrency through a "provider of basic exchange services". A "primary coin" is a coin that is not *anonymity*-enhanced (*i.e.*, a coin other than an AECs), and a "provider of basic exchange services" is a regulated provider that does not make use of *anonymity*-enhancing tools. In principle, in this example the first step consists either of a *placement* activity, if funds are not already in the financial system – in this case, they could be converted into a "primary coin" from a cash-based cryptocurrency ATMs (hence the evaluation of crypto-ATMs as suspicious) – or already of a *layering* activity, with the fiat money

[385] This is not always the case. When cryptocurrency funds are stolen from a DeFi project or a cryptocurrency exchange, the proceeds of the crime are already in the form of cryptocurrency. Later the hackers engage in laundering activities to prevent/hinder LEAs and intelligence companies from tracing the stolen coins back to the hack.

to convert originating from bank accounts or accounts held at non-bank PSPs. If we assume Alice is a money launderer, the issue with this first stage is that the entities that perform fiat-to-crypto exchanges are usually regulated, as outlined in Chapter 4. This means they will perform *identification* and *verification* of her identity before she will be able to access their services. Hence, at this point her *real-world identity* is likely linked to the funds.

2. *Layering*. Given the circumstances, as a next step Alice wishes to sever her *real-world identity* from her cryptocurrencies. With this goal in mind, the "primary coins" previously obtained are mixed and exchanged for AECs. As explored below, the properties of AECs are conducive to Alice's objective. The conversion is performed through a "provider of advanced exchange services", which is a provider that deploys on top of its protocol and/or embeds *obfuscation* techniques. Given the FATF's stance on AECs and the link to *mixing* techniques, these providers may not be regulated.
3. *Layering*. To further *obfuscate* the trail, in this phase Alice can exchange her funds, already *anonymity*-enhanced, with other combinations of AECs, through *layering* techniques that can rely on multiple exchanges and addresses (*i.e.*, *virtual-to-virtual layering*). In addition, she can try to *disintermediate* the trail, by making use of DEXes and P2P platforms. Leveraging recent developments, she can perform cross-blockchain exchanges, and/or make use of DeFi solutions to combine the *disintermediation* and *obfuscation* goal.
4. *Integration*. Alice's funds are now cleansed from their criminal origin, insofar as she can trust the chain of *obfuscated* transactions not to unveil their history.[386] As a further step, they may be withdrawn from the IoM (but compliant crypto-to-fiat exchanges will ask information on the funds' origin) or spent directly to buy goods and services from sellers that accept cryptocurrencies. Meanwhile, the funds may be held on self-hosted wallets.

This process is far from rigid. Besides the overlapping of the different phases, the monetary flow may also proceed in the opposite way, starting with Alice holding cryptocurrency funds on a self-hosted wallet, passing through various *anonymity*-enhancements, and finally being converted into "primary coins" and fiat currency through "basic exchanges". This is, however, hampered by the duties of regulated entities, as outlined in Chapter 4. Nevertheless, the goal of this section is to show how the different phases of the process can be interlinked in manifold ways. The interplays are a clear emblem of the threats posed by intricate *layering* schemes.

By retracing the possible phases of this illicit journey, certain steps appear crucial not only in *disintermediating*, but also in *obfuscating*, the trail, in terms of reducing *traceability* and

[386] Fruth, J (2018)

accountability. These loopholes can be specific cryptocurrencies such as AECs, or service providers such as "advanced exchanges" or "mixers". In early regulatory initiatives, the compound of these instruments was addressed as *anonymisers*, broadly described as "tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity".[387] They emerged in the analysis of the FATF's "red flag indicators", but over time experts taxonomised the main methods to obfuscate IoM flows: (1) mixing; (2) zero-knowledge proofs (ZKPs) and other *privacy*-enhancing cryptographic techniques; (3) user best practices.[388] In this work, I add remarks on (4) network-level *anonymity*-enhancements.

3.2.1. Anonymity enhanced currencies

Bitcoin paved the way for an array of cryptocurrencies labelled "altcoins", shortened form for "alternative coins", where "alternative" is meant in respect to Bitcoin.[389] The main driver of a subset of these systems – known as AECs or "privacy coins" – was the desire to safeguard *privacy*. As reported in a comprehensive review of their whitepapers, many AECs share the ambition to be used as general-purpose money, although the political positions and justifications underlying the initiatives vary significantly.[390] As explored in Chapter 2, their *privacy* motive pivots around the concept of *fungibility*. Because money can be (mis)used for criminal purposes, throughout its history of transfers its owners' actions can taint it. This concerns both transactions that involve drugs, weapons, or laundering, but also those associated to activities in breach of rules posed by dictatorial regimes. From this perspective, *obfuscating* the transaction history aims at *true fungibility*, where "all coins are equally valued regardless of their historical trajectories and associated owners", a quality of physical coins and banknotes.[391]

Nonetheless, currency *fungibility* was not the only AEC driver. *Privacy* has also been pursued for personal security, consumer protection, safe acquisition/transaction, and compliance. Bitcoin's *pseudonymity* is equal to the publication of account numbers or credit card statements while keeping originators and beneficiaries' names hidden, and *anonymity*-enhancements are tasked to mitigate the relevant dangers.[392] While in AEC projects *privacy* is generally seen as

[387] Financial Action Task Force (2014), p 6
[388] Sun Y, Yi YZ (2018a). Sun Y, Yi YZ (2018b). Zhang Y, Sun Y (2019)
[389] The first "altcoin" was released in 2011 and was called Namecoin (Orr DA, Lancaster DM (2018), p 422)
[390] The motives behind "privacy coin" projects have never ceased to develop. Arguably, they moved past anti-governmental and anti-establishment goals. Successful cryptocurrencies, in terms of the value creation, are now "explicitly branded and positioned to aid hegemonic political interests" (Harvey J, Branco-Illodo I (2020), p 108).
[391] Ibid, p 122
[392] Silva Ramalho D, Igreja Matos N (2021), p 503

"as end in itself" and there is no consensus on its specifics, promoters agree on one aspect: the pursuit of *anonymity*. Reportedly, "the state of privacy which privacy coins aim to protect … is, almost always, anonymity", and most whitepapers explicitly refer to it explicitly.[393] As explored in Chapter 2, the link between *privacy* and *anonymity* is clear in the literature.

Against this backdrop, AEC-related risks challenge the AML/CFT/CPF framework considerably, and in 2021 the FATF specified they fall within the scope of the regulatory regime. The major *obfuscation* concern lies in the evolution of the underlying technologies, which hampers effective monitoring on the types of transfers they enable. As suggested in Chapter 2, despite extensive research on the *anonymity* of cryptocurrencies, a standardised mean to assess its levels has yet to be achieved. By contrast, the efforts to identify *anonymity* in a unified manner across different implementations suggest "claims for anonymity cannot be made lightly in the presence of such granularity".[394] While the most basic type of *privacy*-enhancement is the use of a new address for every transaction – *i.e.*, stealth addresses –, most AECs implement a combination of PETs, whose role is significant in terms of both safeguarding *privacy* and fostering *anonymity*-oriented set-ups.[395] Indeed, as explored above and in Chapter 2, *anonymity* is one of the methods to pursue *privacy*. Accordingly, on the one hand PETs can be implemented to safeguard *privacy* against intrusions and for the sake of data protection (*e.g.*, as per the GDPR), and on the other hand they can be exploited to cripple the *traceability* of funds.[396]

ZKPs, among the most complex and used PETs, are a perfect example of this twofold nature. *User privacy* is preserved by enabling a party to prove the possession of certain data without the need to disclose it, thanks to a cryptographic technique that allows a transaction to be validated while masking the content, preventing users not participating in it from accessing its original content.[397] The value of ZKPs lies in bridging the two objectives of public blockchains underlined in Chapter 2: *user anonymity* and *transaction transparency*.[398] Accordingly, research is exploring how to use ZKPs to reach a desirable level of *user privacy*, in the form of *confidentiality*, without thwarting *accountability*, measured in terms of *auditability*.[399]

The application of ZKPs entails data *obfuscation – i.e.*, to mask/hide data. According to their specifics, and on the grounds of the effects on data *confidentiality* and *auditability,* PETs

[393] Harvey J, Branco-Illodo I (2020), p 121
[394] Amarasinghe N, Boyen X, McKague M (2021), pp 206 and 219
[395] Torra V (2017)
[396] Pocher N, Veneris A (2022b), p 7
[397] De Haro-Olmo FJ, Varela-Vaca AJ, Álvarez-Bermejo JA (2020), p 14
[398] Quiniou M (2019).
[399] European Central Bank, Bank of Japan (2020). Yuen TH (2020). Dashkevich N, Counsell S, Destefanis G (2020). Puzis R, Barshap G, Zilberman P, Leiba O (2019). Tian H, Luo P, Su Y (2020). Barbereau T, Sedlmeir J, Smethurst R, Fridgen G, Rieger A (2022). Gross J, Sedlmeir J, Babel M, Bechtel A, Schellinger B (2021)

were classified as *segregating*, *hiding*, or *unlinking*.[400] Accordingly, their effects were ranked from *effective auditability* to *weak auditability*, showing how some techniques may safeguard *privacy* but still enable oversight, while others do not leave room for effective *auditing*. In this respect, the level of *auditability* can be construed as the result of the degrees of: (a) accessibility to necessary information; (b) reliability of information; (c) efficiency of the process.[401]

To imagine an extreme scenario, if a specific technique leads to some data not being stored on the ledger in any form, this cannot be retrieved later. In particular, it was argued "segregating PETs", "Quorum's private transaction", "Pedersen commitment" and "centralised mixing" may allow for effective *auditability*, which means they can be applied to reach a suitable balance between *privacy* and *transparency* for AML/CFT/CPF. On the contrary, "ZKP", "one-time address" and "multi/ring-signatures" make transaction information thoroughly inaccessible.[402] Chapter 5 addresses this distinction and the AML/CFT/CPF impacts within a more comprehensive analysis of trade-offs in PETs. By contrast, the following subsection takes a broader approach in heeding the elements at play when pinpointing *anonymity* benchmarks in "privacy coins" that embed different techniques. To do so, it outlines four use cases of AECs – Zcash, Monero, Dash, Mimblewimble –, and their cryptographic mechanisms. Although these use-cases are blockchain-based, *privacy* has been enhanced in non-blockchain scenarios as well.[403]

3.2.2. Four AEC use-cases

Zcash was created drawing from two previous systems: Zerocoin and ZeroCash. On the one hand, Zerocoin relied on "one-way accumulators" for value storage and on ZKPs for spending coins while breaking ties between transactions. On the other hand, ZeroCash introduced a type of ZKP known zero-knowledge succinct non-interactive argument of knowledge (zk-SNARKs) for transaction verification, and schemes of "decentralised anonymous payment" to pay directly and privately (*i.e.*, concealing senders, recipients and amounts). Both systems presented serious drawbacks: they were not compatible with the Bitcoin network, their functioning relied on heavy cryptographic computation, they did not hide the IP addresses of their users.[404]

[400] European Central Bank, Bank of Japan (2020). Pocher N, Veneris A (2022b), p 8. *Stealth addresses*, *one-time address* and *ring signatures* based on *homomorphic encryption* are *unlinking* PETs. *Homomorphic encryption* is used in e-voting, "where each vote cast must not be related to the identity of its issuer, who must be anonymous. This is achieved by using ring signatures" De Haro-Olmo FJ, Varela-Vaca AJ, Álvarez-Bermejo JA (2020), p 14
[401] European Central Bank, Bank of Japan (2020), p 15
[402] Ibid, pp 18-22
[403] Tennant L (2017), pp 6-8. Ince P, Liu JK, Zhang P (2018), pp 32-45
[404] Amarasinghe N, Boyen X, McKague M (2019), pp 5-6

Zcash was developed on top of the ZeroCash model, to improve its level of *confidentiality* and the size of its *anonymity* set, while also using Bitcoin's transaction type.[405] The main *anonymity* feature of Zcash is the "shielded pool", and also in this case the goal of the underlying ZKP protocol is to hide transaction data while allowing its verification. However, in Zcash *privacy* is enhanced selectively, which enables to preserve *confidentiality* of a subset of data. When coins are placed into the "pool", senders are revealed but recipients are hidden by using "z-addresses" to identify them. By contrast, when coins are withdrawn from the "pool", senders are hidden, and recipients are revealed. Hence, complete *privacy* can only be provided when transactions take place *within* the "shielded pool". In this case, senders, recipients and transferred value are all hidden.[406] Because zk-SNARKs are computationally expensive, only a minority of Zcash's addresses is shielded. The other ones are *transparent* (*i.e.*, not *anonymity*-enhanced). The use of *transparent* addresses has the same outcome of Bitcoin transactions, described in terms of "t-addresses". Hence, the Zcash model is not "private-by-default",[407] and the *unlinkability* of its transactions is not complete due to the concurrent presence of *transparent* and *shielded* transactions, which means the system vulnerable to *de-anonymisation*.[408]

The cryptocurrency Monero, on its part, was initially deploying the CryptoNote protocol to achieve *untraceability* and *unlinkability* counterbalancing blockchain's *transparency*. The goal was pursued using "one-time ring signatures" with non-interactive ZKPs, similar to "non-interactive mixing".[409] The expression "ring signatures" refers to the presence of a "ring of users", within which a user signs a message on behalf of the whole group without revealing the individual identity – *i.e.*, the signature is verified using all the public keys of the group. This technique is considered less performant than zk-SNARKs, but was tested more intensely.[410] Nonetheless, it was vulnerable to *de-anonymisation* because some features made transactions partially *linkable*, values were not hidden, and cryptographic keys increased transaction size.[411]

---

[405] Ibid, p 6

[406] Yousaf H, Kappos G, Meiklejohn S (2019), p 13. In "shielded" transactions, each address is equipped with a private spending key that enables the owner to spend the coins (notes) sent to that address. For each note, a unique nullifier is created using the spending key and a note commitment, made public upon creation of the note. The private key allows the note commitment to be linked to its nullifier. Hence, a Zcash unspent note is a note whose commitment is revealed and whose nullifier is hidden. The creation of a "shielded" transaction entails the disclosure of (i) nullifiers of input notes and (ii) commitments of output notes. Values are also hidden, as they are revealed through value commitments related to inputs and output notes, whose balancing is performed as homomorphic operations. Zk-SNARKS primitives are deployed to prove the notes' ownership and to verify and validate transactions (Amarasinghe N, Boyen X, McKague M (2021), p 214)

[407] Biryukov A, Tikhmirov S (2019), pp 1-2. Yousaf H, Kappos G, Meiklejohn S (2019), p 13

[408] Amarasinghe N, Boyen X, McKague M (2019), p 6. Amarasinghe N, Boyen X, McKague M (2021), p 208

[409] Altcoins such as ByteCoin and Aeon deploy CryptoNote. Amarasinghe N, Boyen X, McKague M (2019), p 6

[410] Maupin JA (2017), p 7

[411] Amarasinghe N, Boyen X, McKague M (2019), p 6

Indeed, the *anonymity* of Monero has evolved over time, and the cryptocurrency is claimed to be one of the most *anonymous* given the deployed combination of PETs. Currently, it uses "ring signatures" to hide senders' details and allows coins to be "mixed" with so-called "mix-ins". Transaction values are hidden through "ring confidential transactions", that allow verification through value commitments, to improve CryptoNote. Meanwhile, "one-time addresses" or "stealth addresses" are deployed to hide recipients, and "linkable ring signatures" attain senders' *privacy* and avoid double spending.[412] In principle, transactions can still be *de-anonymised* because the "mixing" sampling strategy allows *linkability*, and *untraceability* can be breached.[413] However, Monero deploys Dandelion++ to obscure the IP address of the device broadcasting the transaction. This protocol makes use of "randomised routing algorithms" and "graph topologies", and consists of a broadcast propagation method where new transactions pass through a Monero's node, and later a probabilistic method decides whether the transaction is sent to one node or broadcasted to many.[414] Further, the ongoing project Kovri aims to further increase *anonymity* by encrypting the traffic and routing it through nodes of the Invisible Internet Project (I2P), whose nodes transfer messages without having visibility over them.

Thirdly, Dash embeds as its main *anonymity* feature a type of CoinJoin known as "PrivateSend transactions". It allows multiple users to make more transfers through a single transaction, in line with the "mixing" concept outlined below. When a group of senders send the same number of coins to the respective recipients, it becomes difficult to link input addresses to the corresponding outputs, which severs the link between individual senders and recipients. If CoinJoin methods usually require users to find each other, Dash finds users automatically and chains multiple mixers together. The actual level of *anonymity* depends on the number of transactions mixed in any given case,[415] and to hamper users from sending identifiable values the system restricts "PrivateSend transactions" to specific denominations.[416] As in Zcash, the *privacy* of senders and recipients is achieved in the same way.[417] Dash deploys a secondary

[412] Yuen TH (2019), pp 225-227. Each Monero user has two pairs of private/public keys acting as spend/view keys. For each output, senders create a "one-time public key/stealth address" using the recipients' public key. To generate the inputs' ring signature the input is mixed with random public keys (*i.e.*, mixins). Outsiders can only see the ring's public keys, each of them having the same probability of being the input (Amarasinghe N, Boyen X, McKague M (2021), p 216)
[413] Amarasinghe N, Boyen X, McKague M (2019), p 7. Amarasinghe N, Boyen X, McKague M (2021), p 208
[414] Amarasinghe N, Boyen X, McKague M (2019), p 7. Fanti G, Venkatakrishnan SB, Bakshi S, Denby B, Bhargava S, Miller A, Viswanath P (2018), pp 1-35
[415] Yuen TH (2019), p 225
[416] Yousaf H, Kappos G, Meiklejohn S (2019), p 14. PrivateSend is an extension of the CoinJoin protocol and improves *decentralisation* and denominations. Remaining limitations are the need of at least three participants and the *centralisation* caused by the Masternode network (Amarasinghe N, Boyen X, McKague M (2019), p 5).
[417] Yuen TH (2019), p 227

network of full nodes (*i.e.*, Dash Masternode Network) on top of the Bitcoin network, therefore its *privacy* level is influenced by the presence of both regular nodes and "masternodes".[418]

Finally, Mimblewimble is a protocol that deploys a system of "confidential transactions" and "transaction aggregation".[419] Its cryptographic method, named "elliptic curve cryptography" is based on logarithms and allows the verification of transactions' amounts and involved parties without revealing any information. On top of this, other cryptographic protocols are deployed, such as the mentioned CTs and CoinJoin – to conceal transaction values and make transactions *untraceable*, respectively –, but also Dandelion and Cut-Through, where the first one hides the identity of senders and users and the second one improves "scalability".[420] Arguably, Mimblewimble is the only cryptocurrency scheme to truly achieve the property of *fungibility*. Nonetheless, proposed corrections to enhance security turned out to lower *fungibility* insofar as the amount of preserved data increases.[421]

3.2.3. Crypto-mixing: the first type of crypto-cleansing

Since mixing was the first attempt to solve Bitcoin's lack of *fungibility*, in the early stages of the IoM "crypto-laundering" and "Bitcoin mixing" were considered synonyms. The mixing process consists of combining inputs and outputs of different transactions into a larger one, to sever the links between the addresses of senders and recipients.[422] Transactions are made *unlinkable* by shuffling them, which means the level of *confidentiality* depends on the amount of mixed data (the "anonymity set") and the similarity of transfers' values.[423] From a related perspective, due to the fact that transaction amounts are usually stored in the clear on the blockchain mixing methods are often combined with *hiding* techniques.

The resulting degree of *confidentiality* is also influenced by whether the model is custodial – *i.e.*, the mixing service is operated by a *centralised* service provider – or not.[424] Indeed, if the service is offered by a *centralised* provider, users must entrust it with their original information.

---

[418] Biryukov A, Tikhmirov S (2019), p 2. Amarasinghe N, Boyen X, McKague M (2019), p 5
[419] Senders send input coins to recipients through an authenticated channel that adds commitments to output coins that include individual private keys, and a partial transaction's signature generated using a random nonce. This is sent back to the sender, who validates the signature, adds his/her portion of it, and broadcasts the transaction to the network. The transaction is verified and minted by the nodes, and the transaction graph is hidden through "transaction aggregation". Amarasinghe N, Boyen X, McKague M (2021), p 217
[420] Shilina S (2021)
[421] Amarasinghe N, Boyen X, McKague M (2021), p 208
[422] Sun Y, Yi YZ (2018). Chapter 5 will heed the classification of "mixing" as an "unlinking" PET (European Central Bank, Bank of Japan (2020). Pocher N, Veneris A (2022b), p 8)
[423] Pocher N, Veneris A (2022b), p 8. Amarasinghe N, Boyen X, McKague M (2019), p 4
[424] Nadler M, Schär F (2023), p 3

In other words, the level of *confidentiality* depends on the way in which the provider disposes of the identifying data after the mixing operation.[425] New P2P schemes of non-custodial cryptoasset mixers allow the *centralisation* point to be removed, but in *non-centralised* and non-custodial scenarios users need to timely find others willing to mix their data.[426] An example of mixing method that does not rely on a third party is the CoinJoin protocol implemented by Dash, while significant turmoil was generated in very recent times by Tornado Cash, arguably the most used non-custodial mixer on Ethereum.[427] It consists of a set of smart contracts and was proposed as a zkSNARK-based ERC-20 solution to the user privacy challenges in account-based blockchains.[428] Similarly, a method that provides trustless *unlinkability* deploys "ring signatures with elliptic curve digital signature algorithm" and can be integrated into Bitcoin to generate and verify signatures. However, if mixing operations are constructed by a server, the overall decentralisation level decreases.[429] Although mixing is neutral in principle, there is a negative aura surrounding these services, as they strongly inhibit detection of criminal revenues. Nonetheless, it was argued that even if they are usually used to dilute and disguise criminal proceeds, they can also serve legitimate purposes of self-protection.[430]

From an operational perspective, mixing can take various forms, and can be automatic or voluntary. Indeed, it can be offered as a service by *centralised* entities – *i.e.*, as an external service, by providers such as the early BitLaundry and MixCoin, or Cashshuffle, Blender and CryptoMixer –, or it can be embedded into: (i) the currency design, implemented on top of the original protocol – *e.g.*, the "layer-2 solutions" mentioned in Chapter 2; (ii) a wallet – *e.g.*, Whirlpool, Wasabi; (iii) an exchange platform. Overall, mixing services are often linked to the activities of custodian wallet providers.[431] Crypto-wallets with embedded mixing are dubbed *privacy wallets* or *mixing-enabled wallets* and perform transfers where multiple transactions are combined into a single transfer.[432] The FATF considers all these possible mixing strategies as tools that increase *anonymity* in the IoM.[433] Indeed, while these methods belong to different

[425] Ibid, p 3
[426] Pocher N, Veneris A (2022b), p 8
[427] Wu M, McTighe W, Wang K, Seres IA, Bax N, Puebla M, Mendez M (2022), p 2. Nadler M, Schär F (2023)
[428] Béres F, Seres IA, Benczúr AA, Quintyne-Collins M (2021), pp 72 and 76. Wu M, McTighe W, Wang K, Seres IA, Bax N, Puebla M, Mendez M (2022), pp 2-3. Users make deposits of equal amounts (of Ether and a few Ethereum-based tokens) to a Tornado Cash smart contract, and later they withdraw the funds to a "fresh" account by proving with a ZKP they were among the depositors. The new account is *unlinkable* to any unique depositor, albeit the level of confidentiality varies according to the size of the "anonymity set", as outlined above.
[429] Amarasinghe N, Boyen X, McKague M (2019), pp 4-7
[430] Silva Ramalho D, Igreja Matos N (2021), pp 497 and 503
[431] Ibid, pp 497 and 500
[432] Financial Action Task Force (2021e), p 7
[433] Financial Action Task Force (2021d), p 23

categories of *anonymity*-enhancements, the intermediary-based AML/CFT/ CPF framework applies to regulated entities regardless of the specific embedded *obfuscation* techniques.[434]

3.2.4. Users and a diversified bundle of "best" practices

"Red flag indicators" do not only refer to the use of cryptocurrencies or services embedding or employing *anonymity*-enhancing methods or increasing *disintermediation*. While mixing and PETs are applied at a protocol level, a set of *anonymity* enhancements originate from user behaviour. In 2021 the FATF underlined the risk posed by "exposure to Internet Protocol (IP) anonymiser such as The Onion Router (Tor), the Invisible Internet Project (I2P) and other anonymising software or anonymity enhancements".[435] Indeed, users can deploy *obfuscation* strategies defined as "best practices" – *e.g.*, making use of *anonymisers* such as Virtual Private Networks (VPNs), and other strategies such as using new addresses for every payment.[436]

To conceal their IP address, users may access the Internet through a VPN, which generates an encrypted tunnel between the user and a remote server before accessing the Internet.[437] TOR, on its part, is the most popular *anonymous* communication network and it enables server-side *anonymity* through hidden "onion services". In this way, "a hidden service client and operator establish a communication tunnel, known as a circuit, between each other over multiple intermediate routers. Anonymity is maintained as long as the intermediate routers at the two ends of the tunnel are not controlled by an adversary who can use time or traffic analysis to link the source to the destination".[438] On top of more common solutions, such as VPNs but also TOR, other sophisticated methods can be deployed by a specific type of skilled users, active on dark-net markets, to avert any investigative and/or enforcement intervention from the authorities.[439] The need to deploy these strategies has emerged above: even if AEC schemes have reached *anonymity* levels that are considered "acceptable" in terms of *unlinkability* and *untraceability*, complete *unlinkability* has yet to be attained with regard to IP addresses.[440]

---

[434] The framework applies to "covered VA activities and VASPs, regardless of the type of VA involved in the financial activity (e.g., a VASP that uses or offers AECs to another person for various financial transactions), the underlying technology (e.g., whether it uses the mainnet or the use of embedded layering or other scaling solutions), or the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation)". Financial Action Task Force (2021d), p 23. Chapter 4 addresses the concepts of "covered VA activity" and the definition of "VASP".
[435] Financial Action Task Force (2021e), p 20
[436] Furneaux N (2018). Sun Y, Yi YZ (2018a)
[437] Furneaux N (2018), pp 229-230
[438] Al Jawaheri H, Al Sabah M, Boshmaf Y, Erbad A (2019), p 3
[439] Maupin JA (2017), p 5
[440] Amarasinghe N, Boyen X, McKague M (2019), p 7

3.2.5. Network-level anonymity-enhancements: on-chain and off-chain layers

As introduced in Chapter 2, the *decentralisation* level of a DLT application can be affected by the addition of one or more on-chain or off-chain "layers" to the protocol – *e.g.*, the Lightning Network in Bitcoin. Accordingly, the properties of *privacy* and *anonymity* can be altered by the specifics of a multi-layered structure – *i.e.*, by the design of the network. In particular, one or more layers can be added to an existing network, or introduced in the design of a new project, to the end of enhancing its *privacy* and/or its *anonymity*. The Dash Masternode Network, mentioned above, consists of a secondary network of full nodes deployed on top of the Bitcoin network that influences the overall *privacy* level of Dash transactions.[441]

As argued for "best practices", the need to develop additional methodologies is linked to other techniques not having achieved full *unlinkability* of IP addresses – *i.e.,* lack of *metadata unlinkability*. In this context, the creation of overlaying *anonymous* "payment channels" was suggested to guarantee transaction *anonymity* by storing some transaction data off-chain, leveraging smart contracts. "Payment channel networks (PCNs)" are also known as "second layer" or "layer-2" solutions, where "layer-1" is the primary blockchain architecture (the "mainnet" or "root blockchain"). "Second layer" solutions can consist of "sidechains", "state channels", or "off-chain transaction networks", allowing instant off-chain transactions with minimal fees, which enhances efficiency and scalability. For this reason, they are used to experiment with (automatic) micro-payments,[442] for which traditional consensus mechanisms are unsuitable. The "layer-2" can deploy specific *anonymity* enhancements, such as a mixing mechanism. From this perspective, the *anonymity* and *transparency* of the resulting network may be altered by the specifics of the tools deployed on overlaying networks or off-chain services.

Whenever a pair of users wishes to transact through a PCN, they can perform a funding transaction that locks funds on-chain, that are then to be used in the specific PCN opened between them. After this, PCN transactions do not involve (*i.e.*, they are not recorded on) the blockchain, and consists only of exchanging a signed message containing the balance between the users. In addition, two users that do not have an open direct PCN can still transact with each other if a path of payment channels connects them – *e.g.*, if Alice has a channel open with Bob, and Bob has a channel open with Charlie, Alice and Charlie can transact with each other through this path. This typically requires the payment of a fee (in this case, to Bob) for having

[441] Biryukov A, Tikhmirov S (2019), p 2. Amarasinghe N, Boyen X, McKague M (2019), p 5
[442] Pocher N, Zichichi M (2022) addresses the value of micro-payments in device-to-device transactions

the transaction forwarded, anticipating both the transaction amount and all the required fees for routing the payment. *Atomicity*, introduced in Chapter 2, is used as a guarantee: either all users along the path update their balances, or none of the balances is updated.[443] An example of the basics of the PCN technique can be found in Blind Off-chain Light-weight Transactions. Besides the Lightning Network in Bitcoin, examples of "second layer solutions" can be found in Ethereum's Raiden for intra-chain operations, and InterLedger or Atomic CrossChain for inter-blockchain transactions.[444] Another network-level solution is the one implemented by Dandelion ++, described above, using randomised routing algorithms and graph topologies.[445]

3.3. Intelligence Strategies: Following Crypto Money across the Ecosystems [446]

Chapter 2 introduced IoM ecosystems as socio-technical, which affects the evaluation of their *anonymity* and *transparency*. Accordingly, among influential elements one should not only consider the technical ones – *e.g.*, PETs, governance, architecture –, but also the social factors. As underlined when exploring *fungibility*, from a social perspective the essence of IoM *anonymity* comprises the impacts exerted by investigative activities. In this context, forensic techniques are to be weighed against users' skills to limit *traceability*. The overall *transparent* nature of (public) blockchains makes them vulnerable to insufficient data privacy, *de-anonymisation* attacks and possible application of surveillance techniques. However, while *de-anonymisation* is a concept that is often perceived negatively, it is the same mechanism that can be applied to "follow the money" and comply with rules that aim to mitigate specific risks. In this respect, the combination of data that is accessible due to the nature of (certain types of) blockchain and the extracts of a given cryptocurrency wallet offers great material for investigative purposes – *e.g.*, Bitcoin transactions generally associate more input addresses to an output address, and an analysis of these links provides useful insights in terms of tracking.[447]

Although in a public blockchain it is not difficult to retrieve information such as TXIDs, with details attached (*e.g.*, time of receipt, input/output values, sender/recipient addresses), specific operative knowledge is needed to interpret it. Indeed, some traits of Bitcoin's inputs and outputs (*e.g.*, transaction fees, transfers between addresses belonging to the same wallet)

[443] Avarikioti Z, Pietrzak K, Salem I, Schmid S, Tiwari S, Yeo M (2021), pp 1 and 3
[444] Amarasinghe N, Boyen X, McKague M (2019), p 7. Pocher N, Zichichi M (2022), p 5
[445] Fanti G, Venkatakrishnan SB, Bakshi S, Denby B, Bhargava S, Miller A, Viswanath P (2018), pp 1-35. Amarasinghe N, Boyen X, McKague M (2019), p 7
[446] *Contents and parts of this section have already appeared in the following co-authored publications:* Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022). Pocher N, Zichichi M, Ferretti S (2023)
[447] Wu Y, Tao F, Liu L, Panneerselvam J, Zhu R, Shahzad MN (2020), p 1231

may be misleading.[448] Further, the trustworthiness of the retrieved data for what concerns the association between addresses and *real-world identities* should always be doublechecked. In this sense, the private sector has been crucial in providing the technology to gather intelligence.

This offer of "visibility" into the IoM space is the business of companies such as CipherTrace, Chainalysis, Elliptic, but also Coin Metrics, Elementus, ScoreChain, Blockseer, Neutrino, Crystal Blockchain, Blockchain Intel, TRM Labs. In broad terms, their activities consist of developing strategies of "blockchain analytics", to be sold as a service to governments, supervisory authorities, LEAs, and entities regulated under compliance regimes. Because they analyse the different ecosystems and their relationships, these companies can provide insights to "bridge the gaps between regulation and the world of cryptocurrencies and blockchain".[449] Further, they can help supervisory authorities identify unlicensed entities operating as service providers,[450] or regulated entities in assessing exposure to specific risks.[451]

3.3.1. Blockchain forensics: the unfolding of different techniques

As they benchmark the level of *traceability*, forensic techniques can be addressed as the *trait d'union* between *pseudonymity* and *accountability*. Their role lies in defining the possibility and/or likelihood to link a *real-world identity* to a specific (set of) IoM transaction(s). This, in turn, depends on the efficacy of the given techniques vis-à-vis *privacy*-enhancing methods. At the same time, the efficacy of "follow the money" strategies influence the evolution of *anonymity* enhancements, because they prompt the development of new means of *obfuscation*.

Forensic techniques started to be deployed in the IoM as "blockchain analysis", informed by the specificities of blockchain technology. Accordingly, "blockchain forensics" was defined as a "use of science and technology to investigate and establish facts in criminal or civil courts of law" that "deals primarily with the recovery and analysis of latent evidence left on the blockchain digital ledger as the results of transaction activities on a blockchain".[452] Although an analysis of cryptocurrency transactions mainly focuses on data recorded on blockchains, and

[448] Silva Ramalho D, Igreja Matos N (2021), p 491
[449] CipherTrace (2021), pp 2 and 6
[450] Financial Action Task Force (2021e), p 45
[451] Ibid, p 71. Enhanced CDD and risk assessment procedures are addressed in Chapter 4
[452] Phan T (2021). The criminal and/or procedural aspects of IoM analytics fall outside the scope of this work. The analysis is limited to *traceability* and socio-technical impact on *anonymity*, *privacy*, and *transparency*.

techniques were mostly tested on the Bitcoin network, data-exploitation strategies were deployed on Ethereum as well,[453] and debates are ongoing for non-blockchain-based DLTs.[454]

In addition, IoM transactional data is usually analysed through a combination of on-chain and off-chain techniques – *i.e.*, targeting also information that is not recorded on blockchains. In other words, although data generated by on-chain activity, related to the transactions cleared and settled on a blockchain layer, is a primary source of insights on illicit activities, it is necessary to turn to off-chain data to gather data on transactions performed outside the blockchain layer – *e.g.*, transactions between two traders on an exchange's order-book, trading volumes or market data of exchanges, volumes of P2P platforms.[455] Off-chain information may also consist of data that is linked to on-chain activity but is not stored on-chain and is retrieved elsewhere – *i.e.*, everywhere but on the given blockchain (hence, also on another blockchain).

The analysis of transactions is the main method to *trace* transfers in the IoM.[456] Before delving into existing approaches, a disclaimer is needed. In the overview provided below, the use of cryptocurrencies is an assumption, but in real-world investigations this may not be clear from the start. Hence, preliminary strategies encompass acquisition or extraction of private keys, public addresses and crypto-wallets files pertaining to a given subject, analysis of recovered addresses and wallets, to gather data on which to build "follow the money" operations.[457]

In this context, the final goal of intelligence methods is to match users to transactions performed by "cryptocurrency IDs" – in other words, as outlined in Chapter 2, to connect users' *pseudonyms* (*i.e.*, addresses) *to real-world identities* –, leveraging the presence of unique *identifiers* to specific individuals.[458] The structure of the IoM allows many sources of information to be exploited to this end – *e.g.*, data extracted from a transaction can be leveraged to retrieve the transaction history of an address. Different techniques have been refined over time, according to the parallel development of *anonymity* enhancements, and methods based on Artificial Intelligence (AI) and machine learning, addressed below, are now broadly deployed.[459]

---

[453] Chen W, Zheng Z, Ngai ECH, Zheng P, Zhou Y (2019), p 1. Bartoletti M, Carta S, Cimoli T, Saia R (2020). Li Y, Yang G, Susilo W, Yu Y, Ho Au M, Liu D (2021). Moreno-Sanchez P, Zafar MB, Kate A (2016), pp 436–453. Ferretti S, D'Angelo G (2019). Wu M, McTighe W, Wang K, Seres IA, Bax N, Puebla M, Mendez M (2022)
[454] Tennant L (2017), pp 6-8. Ince P, Liu JK, Zhang P (2018), pp 32-45
[455] Blandin A, Pieters G, Wu Y, Eisermann T, Dek A, Taylor S, Njoki D (2020), p 36
[456] Other methods rely on a "central party" or on "cryptographic tools", generally embedding certain features into an AEC to ensure its *traceability* by design. Li Y, Yang G, Susilo W, Yu Y, Ho Au M, Liu D (2021), pp 680-681
[457] Furneaux N (2018), pp 119-145, 147-173 and 175-197
[458] Airfoil (2019). The Cryptocurrency Consultant (2019b). Paesano F (2019), pp 2-8
[459] Yin HHS, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019), pp 37-73. Serena L, Ferretti S, D'Angelo G (2022). Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022)

3.3.2. Analysis of the transaction network and the role of clustering

A considerable portion of forensic techniques deploy statistical approaches to collection and transaction analysis. Notably, they focus on the re-use of the same account for more transactions, or the co-use of more accounts for a single transaction, as well as their topologies, are elements that can be leveraged to match accounts to the same user.[460] Among these methods, several strategies try to link (pools of) addresses and transactions to specific users. They deploy techniques of "address clustering" to cluster addresses owned by the same user,[461] and visualisation analytics such as "transaction graphs".[462] Some of these methods aim to identify "idioms of use" in the network that can erode user *anonymity*.[463] In principle, these techniques do not (try to) *de-anonymise* an address or transaction (*i.e.*, to link a given address or transaction to a *real-world identity*), but in case one of them is *de-anonymised* (in other ways) they allow the whole cluster to be *de-anonymised*. Likewise, the function of these strategies is not to identify and analyse transaction patterns, but to allow that "once an address is suspected in a cluster, other addresses are also suspected because they are very likely to belong to the same user or group".[464] However, "transaction flow analysis" can be implemented to define patterns based on transaction features, to pinpoint suspected addresses.[465]

Clustering methodologies are grounded on heuristic models.[466] The concept behind "clustering heuristics" is that users may be associated with addresses through two heuristic models: (1) "if two (or more) addresses are used as inputs to the same transaction, then they are controlled by the same user".[467] Indeed, one can assume that if a user owns the private keys to sign the transaction – *i.e.*, all the private keys matching the public keys of the different inputs – then the same user owns all the addresses; (2) a "one-time change address – if one exists – is controlled by the same user as the input addresses".[468] The second heuristic is built on the concept

[460] Li Y, Yang G, Susilo W, Yu Y, Ho Au M, Liu D (2021), p 680
[461] Neudecker T, Hartenstein H (2017), pp 1-12. Ince P, Liu JK, Zhang P (2018), p 37. Wu Y, Tao F, Liu L, Panneerselvam J, Zhu R, Shahzad MN (2020), p 1231
[462] Fleder M, Kester MS, Pillai S (2015), pp 1-7. Ober M, Katzenbeisser S, Hamacher K (2013), pp 237-249. Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T (2019)
[463] Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S (2016), p 87
[464] Wu Y, Tao F, Liu L, Panneerselvam J, Zhu R, Shahzad MN (2020), p 1231
[465] Ibid, pp 1231-1232
[466] Lischke M, Fabian B (2016) Analyzing the Bitcoin Network: The First Four Years. Future Internet 8 (1), p 4. Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S (2013) Evaluating User Privacy in Bitcoin. LNCS 7859: 34–51, pp 8-10. Reid F, Harrigan M (2013), pp 8-11. A "heuristic method" is a problem-solving approach deployed when an "exhaustive search" methodology proves impractical. It is based on intuition, reasoning, problem context and past experiences. Although "heuristics" pursues solutions not guaranteed to be optimal, they provide sufficient accuracy for the immediate goal.
[467] Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S (2016), p 89
[468] Ibid, p 90

of "one-time change addresses", where a "change address" is created for the sender to receive the excess from the input address. As outlined above, in a transaction a "change address" is created to receive the remaining funds unless the user owns the exact amount in one UTXO. Hence, at least one of a transaction's outputs is the "change address". Since a related "idiom of use" is that the "change address" is created internally and never re-used, if a transaction has a single output, this address usually has the same owner as the input address.[469] This approach is named "wallet-closure analysis" and aims to establish a "unique many-one mapping between addresses and an identity".[470] Another technique is known as "behaviour-based clustering".[471]

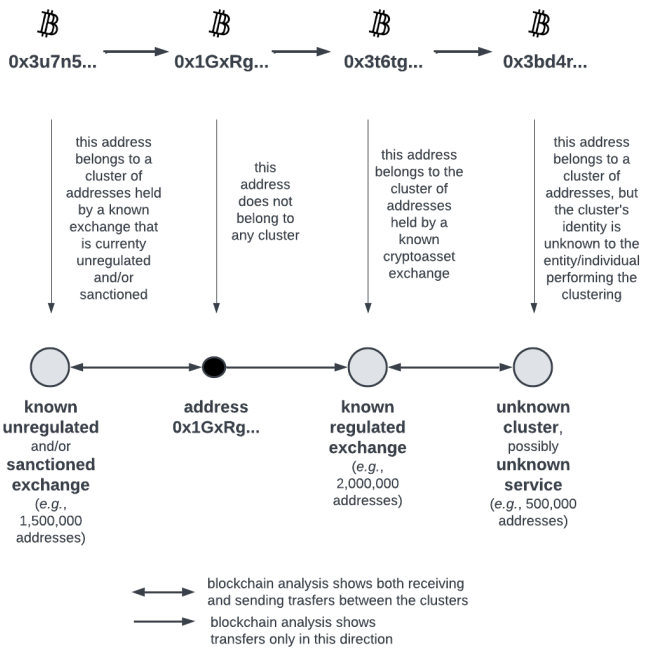

Figure 4: an example of the value of clustering in blockchain analysis

One of the practical examples of the value of clustering is displayed in Figure 4 above. Given a series of cryptocurrency (in this case, bitcoin) transactions between four addresses, through the deployment of clustering algorithms – that are often proprietary and owned by the analytic companies offering RegTech applications – each of the addresses is pinpointed as either (i) belonging to a specific identified cluster (*e.g.*, a service provider such as an exchange),

[469] Ibid, p 90. Borreguero Belntrán A (2019), p 29
[470] Al Jawaheri H, Al Sabah M, Boshmaf Y, Erbad A (2019), p 5
[471] Amarasinghe N, Boyen X, McKague M (2019), p 3. "Behaviour-based clustering" is defined as the "grouping of Bitcoin addresses with similar behavior patterns based on characteristics such as transaction values". Other clustering methods are "co-spend clustering", when more addresses contribute inputs to a single transaction, or "intelligence-based clustering" when information is gathered from sources external to the transaction history, as outlined below (Yin HHS, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019), pp 37-73)

(ii) belonging to a (yet) unidentified cluster (*e.g.*, a possible service provider given the amount of addresses and relevant transactions), or as (iii) not belonging to any cluster (at least as far as the specific clustering algorithm is concerned). These findings allow the fund flow between the identified entities/clusters to be visualised, thus unveiling (a part of) the transaction history. Since forensic companies perform this process on as many cryptocurrency transactions as possible, the overall outcome shows the degree of receiving/sending relationships between the clusters. Although the example focuses on bitcoin transactions, the same approach is deployed on other blockchains and cross-chain (*i.e.,* across different blockchains).

On the application level, other analytic methods exploit the information that leaks when it is possible to establish a correlation between transactions and the users' public profiles on social networks. Indeed, users do not only often post their cryptocurrency addresses (*e.g.*, to receive donations, offer services) on social media, but also personal information related to their online identities (*e.g.*, contact information, age, gender, location).[472] In this respect, there are methods of "transaction fingerprinting" pegged on "publicly available information",[473] or on "off-network information",[474] and techniques involving web-scraping and OSINT tools.[475] Parallelly, a more proactive approach is "illicit transactions mapping and prediction".[476]

In light of the *obfuscating* role of mixing techniques, another forensic method analyses mixing services.[477] As introduced above, a "coin-mixer" *obfuscates* funds by sending them to other addresses and shuffling them with those of other users. Clearly, users of mixing services are harder to trace if the number of inputs and outputs involved in a given process is larger.[478] Although intermediated third-party mixing services still tend to act as *centralisation* points also for *traceability* purposes, other disintermediated methods pursue a similar shuffling goal through more sophisticated approaches – *e.g.*, the mentioned P2P mixing protocol CoinJoin. Against the backdrop of the *enhanced disintermediation* evolution outlined in Chapter 2, an important role is played by the performance of *disintermediated* transactions between cryptoassets based on different blockchains, and hence also by the related platforms. In this context, a new subset of blockchain analytics research efforts targets the analysis of cross-currency transactions and their *traceability* through exchanges such as ShapeShift.[479]

---

[472] Ibid, pp 1 and 5
[473] Fleder M, Kester MS, Pillai S (2015), p 2
[474] Lischke M, Fabian B (2016), p 4. Reid F Harrigan M (2013), pp 15-17
[475] Airfoil (2019). The Cryptocurrency Consultant (2019b). Paesano F (2019)
[476] The Cryptocurrency Consultant (2019b). Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T, Leiserson CE (2019). Koshy P, Koshy D, McDaniel P (2014)
[477] Wu J, Liu J, Chen W, Huang H, Zheng Z, Zhang Y (2020)
[478] Borreguero Belntrán A (2019), p 30
[479] Al Jawaheri H, Al Sabah M, Boshmaf Y, Erbad A (2019), p 6

3.3.3. Machine learning-based approaches to anomaly detection

Nowadays, tools of blockchain forensics are ordinarily deployed in specific RegTech solutions that support regulated entities in their compliance activities by providing alerts when unusual patterns are identified – *e.g.*, when a transaction meets predefined standards of suspicion. In this context, "anomaly detection" consists of processing data to detect patterns that suggest a change in system operations, thus pinpointing events that are significantly different from the dataset.[480] The important interplay between anomaly detection solutions and the red flag indicators mentioned above will be introduced in Chapter 4 and explored more extensively in Chapter 6. In this section, the goal is to complement the overview of IoM-related analytic approaches by accounting for strategies based on AI and machine learning. Consistently, Table 2 below lists and compares forensic methods applied in IoM scenarios for anomaly detection.

Work	Methodology	Algorithms	Results
Reid and Harrigan (2013)	Network Analysis	flow analysis + off-network information	associate addresses with each other and with external identifying information
Fleder et al. (2015)	Network Analysis	flow analysis + web scraping	link illicit activities to online identities
Y. Wu et al. (2021)	Network Analysis	safe Petri Net-based cluster analysis	find suspected addresses
Al Jawaheri et al. (2020)	Network Analysis	wallet-closure analysis	infer links between Bitcoin users and hidden services
Harrigan and Fretter (2016)	Network Analysis	address-clustering analysis	identify super-clusters
Sun et al. (2021)	Graph Analysis	flow-based graphs analysis with coupled tensors	anomalous transactions detection FAUC metric 0.94
X. Li et al. (2020)	Graph Analysis	theoretical flow-based multipartite graphs analysis	anomalous transactions detection FAUC metric 0.96
Yin et al. (2019)	Machine Learning	supervised learning-based (baseline)	predict type of yet-unidentified entity F1score 0.796 (GradientBoosting)
Weber et al. (2019)	Machine Learning + Graph Analysis	supervised learning-based (baseline + GCN)	predict illicit transactions F1score 0.796 (Random Forest)
Eddin et al. (2021)	Machine Learning + Graph Analysis	supervised learning-based (baseline + triage model)	reduce the number of false positives by 80%
Oliveira et al. (2021)	Machine Learning + Graph Analysis	supervised learning-based (baseline + GuiltyWalker)	predict illicit transactions F1score 0.85 (Random Forest)
Ours	Machine Learning + Graph Analysis	supervised learning-based (baseline + GCN + GAT)	predict illicit transactions F1score 0.844 (GCN)

Table 2: selected overview of methods of blockchain analytics and anomaly detection.
From: Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022)

As introduced above, AI-based solutions are increasingly deployed in transaction analytics, and a line of research specifically focuses on machine learning-based forensics.[481] In machine

[480] Kamišalić A, Kramberger R, Fister I (2021)
[481] Machine learning is a part of AI "that exploits data and algorithms to imitate human learning processes, with gradual accuracy improvements […] in the most diverse contexts, it provides tools that can learn and improve automatically leveraging the vast amount of data available in our age" (Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022), ref. to Kamišalić A, Kramberger R, Fister I (2021)). As explored in other parts of the work,

learning, a key distinction is between unsupervised and supervised methods.[482] Unsupervised techniques are usually deployed when there is a lack of real-world labelled (*i.e.*, tagged, annotated) datasets,[483] but the latter arguably guarantee better results when it comes to prediction – *e.g.*, transaction classification. In the AML/CFT/CPF domain, there is an overall shortage of large-scale annotated blockchain transaction datasets, due to both the scale of the relevant phenomena but also to specificities and the timing of relevant investigations.[484] Hence, the role of analytic companies has emerged as crucial in labelling IoM transaction data.

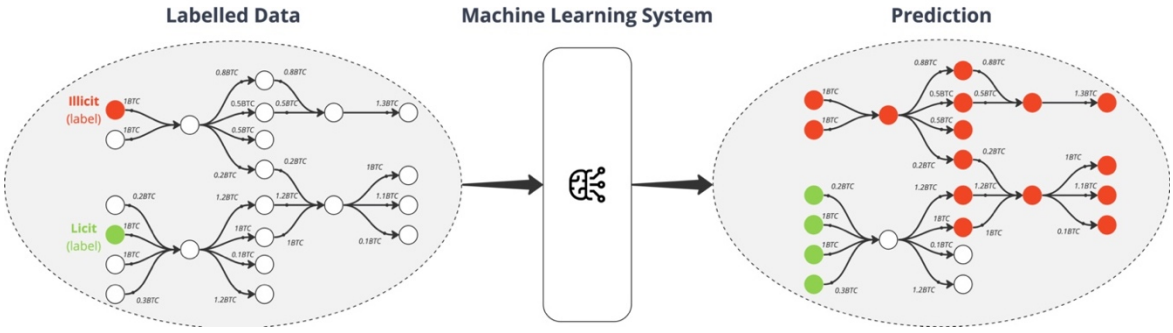

Figure 5: example of the application of supervised learning for transaction classification
From: Pocher N, Zichichi M, Ferretti S (2023)

For instance, providers of RegTech services can annotate a transaction dataset tagging different transactions as licit or illicit based on previous investigations, public information (*e.g.*, scandals, scams) or their own proprietary data and methods – e.g., clustering algorithms. The resulting set of labelled transactions can be used to train machine learning algorithms to identify other transactions as licit or illicit – *i.e.*, as depicted in Figure 5 above, to perform transaction classification where the model provides a prediction output starting from an annotated dataset. Indeed, recent tools deploy supervised machine learning to detect anomalies based on rules of association to pinpoint suspicions. Since in AML/CFT/CPF-oriented applications the label of a transaction usually indicates whether it was identified as illicit,[485] a primary challenge

these algorithms show promising results when applied in AML/CFT/CPF RegTech solutions, especially in terms of mitigating the shortcomings of rule-based systems, increasing detection rates and limiting false positives

[482] In the first case, the learning model pursues the discovery of data and patterns previously undetected. In the second case, algorithms are trained using labelled datasets, which means the initial training data must be tagged and annotated by experts. Pocher N, Zichichi M, Ferretti S (2023), p 9

[483] To address lack of data, various strategies were proposed – *e.g.*, fully synthetic data or simulating unusual accounts within a real-world dataset (Eddin AN, Bono J, Aparício D, Polido D, Ascensão JT, Bizarro P, Ripeiro P (2021). Meanwhile, the shortage of real-life datasets led to the deployment of methods of unsupervised and active learning (Lorenz J, Silva IS, Aparício D, Ascensão JT, Bizarro P (2021)).

[484] Ibid, p 1

[485] Yin HHS, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019). Lorenz J, Silva IS, Aparício D, Ascensão JT, Bizarro P (2021)

is to identify proper classification criteria – *e.g.*, defining how to reach the conclusion that if a transaction is illicit its neighbour transactions also are. Examples of supervised techniques are Decision Trees, Random Forests, Boosting Algorithms, Logistic Regression, Support Vector Classification, k-Nearest Neighbours.[486]

In this context, since every cryptocurrency transfer inherently involves a relationship between entities that can be represented using a graph structure, "transaction graph analysis" emerged as key in blockchain forensic and focused on leveraging the structure of these graphs to identify illicit transactions.[487] Meanwhile, the broader field of machine learning has been increasingly experimenting with real-world structured datasets that take the form of graphs or networks – *e.g.*, social networks and knowledge graphs.[488] Hence, some solutions focused on the possibility to create multiple graph types from blockchain data. A set of approaches are based on a variant of neural networks that operates directly on graphs – *i.e.*, graph neural networks.[489] Convolutional neural networks, for instance, extract statistical patterns from large-scale and high-dimensional datasets and can be generalised to graphs.[490] In particular, graph convolutional networks (GCN) aim to learn a function of features on a dataset structured as a graph, and graph attention networks (GAT) can give different importance to each node's edge.

In this context, a supervised learning approach was deployed on the Bitcoin blockchain to predict the type of entities yet not identified.[491] Relatedly, studies benchmarked GCN against various supervised methods,[492] and leveraged random walks on a cryptocurrency graph to characterise distances to previous suspicious activity.[493] Parallelly, a set of works focused on graph-based scores of suspicion based on a detection system leveraging business knowledge on

[486] For an overview of the techniques: Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022), pp 12-13
[487] Because blockchain transactions are linked by nature, it is possible to create "a graph of transactions that can be of help in the classification process. Given a transaction t, it is possible to collect all the connected transactions and recursively search for other ones up to a certain depth level. Given such a connected graph centred at t, an inspection of the neighbouring transactions and their classified value can aid the classification of t. Each node of the graph (transaction) thus has a set of neighbours that will influence its classification" (Ibid, p 15). See also Serena L, Ferretti S, D'Angelo G (2022)
[488] Pocher N, Zichichi M, Ferretti S (2023), p 10
[489] Jiaxuan Y, Ying R, Jeskovec J (2020). Kipf TN, Welling M (2016)
[490] Defferrard M, Bresson X, Vandergheynst P (2016). Kipf TN, Welling M (2016)
[491] Yin HHS, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019). The analytic company Chainalysis provided the dataset and had previously clustered, identified, and categorized a considerable number of addresses manually or through clustering techniques. The authors concluded it is possible to predict if a cluster belongs to predefined categories – *e.g.*, exchange, gambling, mining pool, mixing, ransomware, scam.
[492] Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T (2019). Eddin AN, Bono J, Aparício D, Polido D, Ascensão JT, Bizarro P, Ripeiro P (2021)
[493] Oliveira C, Torres J, Silva MI, Aparício D, Ascensão JT, Bizarro P (2021). In mathematics and computer science, a "random walk" is a frequently deployed "random process which describes a path including a succession of random steps in the mathematical space" (Xia F, Liu J, Nie H, Fu Y, Wan L, Kong X (2020), p 95)

financial flows, without the use of any learning algorithm.[494] Against this backdrop, in my co-authored publication referenced in Table 2, the goal was to improve the performance of classifier methods through a combination of machine learning and transaction graph analysis. Notably, this was pursued through the deployment of a GAT-based scheme for transaction classification and an innovative GCN implementation.[495]

3.4. An Accountability-Based Approach to a Socio-Technical Conundrum

As introduced in Chapter 2, cyber-libertarians want a cyberspace free from regulatory constraints, where everyone operates *anonymously*, and nobody is held *accountable* for their actions. Although the idea of transposing the *anonymity* of cash to the online world was appealing, they were not able to create a currency system that could underpin a cashless society, chiefly because Bitcoin's *pseudonymity* houses "an inherent tension between the two extremes of anonymity and accountability".[496] In all means of payment – more generally, in all means of information exchange – there is a trade-off between *privacy* (of which *anonymity* is one aspect) and *transparency.* Likewise, *anonymity* and *transparency* do not only ordinarily coexist, but also embody internal ambivalences. As outlined in Chapter 2, *transparency* can bypass trust, but also aid *de-anonymisation*, and fosters both *accountability* and surveillance.[497]

Even before Bitcoin, new technologies allowed to pursue monitoring and *anonymisation* to be pursued at the same time. Technology can be used to reach opposing goals, and this chapter displays how innovative techniques can generate new pathways to both *accountability (e.g.*, forensics) and *unaccountability* (*e.g.*, anonymity-enhancing methods). The evolution of the IoM helps single out the trade-offs featured by the Internet and develop an analytical framework to assess them.[498] Not all cryptocurrency ecosystems within the *anonymity*-oriented subset are *equally anonymous*. However, it is possible to assess the impact of a given implemented technology on the risk of *anonymity* and the degree of *accountability* (or lack thereof). Relatedly, the technological solution underlying an application can embed a specific balance, which in turn is influenced also by aspects related to the ecosystem itself and stakeholder dynamics.

In this respect, as argued in Chapters 2 and 3, the levels of *anonymity* and *transparency* are influenced by: (i) the technical side – *i.e.*, privacy tools such as PETs, governance (*e.g.*,

[494] Li Z, Xiang Z, Gong W, Wang H (2022) Sun X, Zhang J, Zhao Q, Liu S, Chen J, Zhuang R, Cheng X (2021)
[495] Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022), pp 20-23
[496] Yin HHS, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019), p 64
[497] Herian R (2019), p 77
[498] Magnuson W (2020), p 19

centralised vs. *decentralised* systems), broader architecture of the system (*e.g.*, relationship with other on/off-chain layers); and (ii) the social side – *i.e.*, forensic techniques against the backdrop of users' skills to hinder their efficacy. It is difficult to apply such a detailed and layered account of *anonymity* and *transparency* to devise a compliance or regulatory approach. For this reason, it is useful to apply a teleological approach, referring to AML/CFT/CPF goals and to its benchmarks when evaluating different systems. After all, in AML/CFT/CPF the functional approach plays an important role in accommodating technological evolutions.[499]

3.4.1. Obfuscation red flags and cryptocurrency forensics

From a phenomenological perspective, transaction *obfuscation* in the IoM is the outcome of the interplay between (i) the combination between laundering "through" or "of" cryptocurrencies, and (ii) forensic techniques. The two types of cryptocurrency(-enabled) laundering pursue a similar end-goal: to *obfuscate* the flow and confuse the *traceability* chain. In this way, criminals strive to thwart investigative efforts and elude enforcement. Laundering "through" cryptocurrencies often encompasses multiple layers of "crypto-cleansing" because the transition from fiat money to the IoM alone does not ensure *anonymity* in terms of lack of *identifiability* and *traceability*, and further steps are necessary to reach *obfuscation*.

To clarify this argument, reference can be made to the example of the illicit journey of the funds laundered by Alice. Indeed, in that circumstance the following may have happened:

1. Assuming the proceeds of crime were originally in fiat money, Alice may have bought her bitcoins (a "primary" cryptocurrency, that is not *anonymity*-enhanced, and thus does not feature *unlinkability* and *untraceability*) with her credit card or via a wire transfer on a "basic exchange platform", such as Coinbase. At this point, the regulated entity acquired information on her *identity*, verified it, and possibly inquired about the origin of her funds.
2. Later she could have exchanged Bitcoins for Monero through an "advanced/high risk exchange service", such as CryptMixer, that embeds a mixing service. The transaction that moves Bitcoins to the other exchange or to a self-hosted wallet (to then convert it, if the "basic exchange platform" does not exchange to AECs or Monero specifically), performed from a Coinbase account to CryptMixer, is traced and evaluated by the regulated entity.
3. Most likely, now Alice was holding her Monero on a self-hosted wallet or at an entity offering services of cryptocurrency custody implementing *anonymity*-enhanced wallets

[499] Financial Action Task Force (2021e), p 22

such as Wasabi. Then she could have exchanged her Monero for combinations of Zcash and Dash, by making use of other "advanced exchanges" and by creating multiple/stealth addresses. She could have also focused on DeFi products and/or made use of DEXes. The operations performed at this point increase the *obfuscation* of Alice's transaction trail substantially, to avert techniques such as graph analysis and be outside the monitoring eye of regulated entities or LEAs that implement RegTech tools implementing these solutions.

4. Finally, she could have user her funds, stored in a self-hosted wallet, to buy goods and services online. In this respect, Alice could have either made her online purchases on legitimate websites, if retailers accept cryptocurrencies or buy both legal and illegal goods and services on darknet marketplaces. In the latter case, possible purchases include–drugs, weapons, human organs, counterfeited currency, cybercrime-as-a-service.
5. Along this journey, she could have likely deployed the array of mechanisms addressed as "best practices", such as the basic measure to connect to the Internet through a VPN.

The steps taken by Alice aim to sever the links between her transactions and any association to her. She wants neither to be identified as the person making the transfers, nor for her transactions to be linked to one another. Further, her goal is that none of the activities can be traced back to her computer or to off-network information that may be available and possibly linked to her. To sum up, her actions strive to elude forensic methodologies of data-exploitation devised to *de-anonymise* IoM transactions. Notably, these strategies are among the ones listed within FATF's *anonymity*-related "red flag indicators" outlined above,[500] which testifies how Alice is trying to heighten the degree of *anonymity* of her operations, in the form of both *obfuscation* and *enhanced disintermediation*. Indeed, Alice

i. transacts in multiple cryptoassets, especially in AECs,
ii. changes bitcoins through a centralised exchange and then into AECs,
iii. makes use of mixing services,
iv. keeps her funds on a self-hosted wallet,
v. deploys *anonymous* encrypted communication methods (*i.e.*, a VPN service),
vi. interacts with questionable service providers – *e.g.*, "advanced/high risk exchanges",
vii. transacts on/through DEXes,
viii. operates on DeFi platforms and/or buys DeFi products.

Alice's actions show how the teleological approach to the meaning of *anonymity* (and *transparency*) – *i.e.*, one that focuses on the purpose, context and end-goal of a concept when

[500] Financial Action Task Force (2020d)

defining it – may prove useful when it comes to identifying those elements that are more conducive to illicit activities. To this end, a primary reference can be made to FATF's "risk indicators" themselves. Given the dangers posed by *anonymity*-enhanced applications countries, through their regulatory and supervisory activities, must ensure regulated entities are able to manage and mitigate the risks arising from performing "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". Alternatively, should they not be found able to manage and mitigate (or should they not be able to give sufficient assurances that they are indeed able to manage and mitigate) the risks that arise from performing or being exposed to these *anonymity*-enhanced activities, these providers should not be permitted to engage in them.[501]

While the IoM challenges existing measures to mitigate and/or prevent the risk of abuse for illicit purposes, techniques of forensic investigation engage in a race to disrupt dangerous dynamics. Because these opponents do not seem to be bound to outrun one another once and for all, any regulatory instrument needs to be constantly updated. Thus, they need to be conceived and drafted in a way that allows it. As the FATF suggests, money laundering is not a victimless crime, and the possibility to cleanse great amount of funds and/or to gather finances through *anonymous* and *untraceable* solutions poses a great threat to the international community and financial system. This is not to say cryptocurrencies ought to be collectively marked as shady or illegal. On the contrary, most stakeholders and ecosystems are less *anonymous* and more *traceable* than what could be expected. However, while lawmakers and LEAs deploy their forces to include these transactions in the scope of AML/CFT/CPF compliance, the online world reaches new heights of *unaccountability*. While it could be argued that *anonymity*-enhanced tools are not easy to use by individuals lacking specific expertise, the history of the Internet shows how the evolution of new solutions has over time the potential to provide a great variety of users with opportunities originally in the exclusive hands of experts.

3.4.2. The multi-layered nature of accountability in the IoM

Because in the IoM the techno-legal trade-off between *complete anonymity* and *full transparency* is socio-technical in nature, the evaluation of these traits may generate confusion from an operational perspective. For instance, although the IoM may seem impenetrable because of

[501] Financial Action Task Force (2021e), p 55

darknet operations, a cryptocurrency and its network should not be confused with what users or developers do on top of/beside it to increase the *anonymity* level of a transaction. Physical cash is always *anonymous*, not only when used in the black market or hidden in a briefcase. Bitcoin is *pseudonymous* even if it is used in the dark web, and even if the degree of *anonymity* may be altered socially, through users' actions to hinder *traceability* vis-à-vis forensics.

Indeed, in any given use case that presents features of *anonymity* (or *transparency*) the trait can be referred to different aspects, such as the payment instrument, some specific elements of it, the whole system. The feature could then be influenced by the application of *obfuscation* techniques, hindering *traceability* and *linkability*, or by tools of *enhanced disintermediation* that deceive traditional intermediary-based regimes. Moreover, the *anonymous* trait may stem from embedded technologies (within layer 1), from processes that are implemented on top of it (as a layer 2 or as a component of layer 2) and/or from additional behaviours (*e.g.*, user best practices). Accordingly, when evaluating cryptocurrency ecosystems or also specific transactions, it is possible to assess their levels of *anonymity* and *transparency* from different perspectives. It is possible to focus on the concept of online exchange of information, and/or on their position within the financial services domain and/or on the specific implemented technologies such as DLTs and/or the given governance aspects displayed by a specific use-case. Indeed, traits such as *anonymity*, *transparency* and *privacy* present diversified meanings and degrees in the IoM, and they can pertain to conceptual, ideological, or structural levels of reasoning.

The interplay between the ambivalent principles informing online communication and the financial domain, coupled with the non-binary nature of traits such as *anonymity* and *transparency*, testify to the need to set appropriate balances policy-wise. The IoM does not make any difference: the only way to overcome a tension between the traits of *anonymity* and *transparency* is to agree on a desirable trade-off. When setting or evaluating these trade-offs, there are elements that resemble issues arising in general from innovative products and services, and other aspects more closely linked to DLTs and cryptocurrency specifics, such as cryptography. From this perspective, *anonymity* and *transparency* are coexistent values that shaped the IoM. DLTs, when applied in certain ways and in some contexts, exacerbate such traits.

As explored in Chapter 2, DLTs retain ambivalent features, depending on the different perspectives. They have been analysed and implemented as solutions to reach seemingly conflicting goals, attempting to leverage their multifold properties to different ends. In addition, the debate between *financial privacy* and *transparency* shows how *financial confidentiality* was discussed before digital technologies. DLTs heightened an existing complexity more linked to the need to reach suitable trade-offs between opposing interests than to the technology. Hence,

the regulatory urgency to agree on acceptable balances between non-binary states such as *anonymity* and *transparency* does not originate from DLTs. The latter, however, provide insights on the dynamics informing these values – *i.e.*, the IoM shows how these technologies can unlock opportunities for both lawlessness and *accountability* – and ways to combine them.

In this context, I argue *accountability* emerges as the conceptual *trait d'union* between the different developments. Both *obfuscation* and *disintermediation* generate a situation where users are not *accountable* for their transactions. Likewise, the socio-technical perspective accounts for players and techniques that pursue to increase or decrease *accountability* for IoM transactions. Indeed, some actors are trying to (provide ways to) avoid regulatory constraints, and some others are trying to re-establish it, thus engaging in a race that is not likely to end soon. On the ground of the socio-technical nature of IoM ecosystems, the activities performed by this plethora of actors influence the overall character of the domain. Hence, I believe the added challenge brought by the IoM when addressing trade-offs between *privacy* and *transparency* is not their presence, but rather their composition of its socio-technical elements.

3.5. Conclusions

After the deep dive of Chapter 2 into the notions of *anonymity* and *transparency* in the IoM from an AML/CFT/CPF standpoint, this chapter addressed the impact of (a) available methods to *obfuscate* IoM transactions and, by contrast, (b) forensic techniques deployed to *trace* these fund flows. To do so, the analysis started from how the unsatisfactory level of *anonymity* of the Bitcoin network fostered the evolution of (i) *anonymity*-enhancing strategies applied by different actors at various levels (*e.g.*, application, network), and (ii) methods of transaction analytics to "follow the money" across the IoM for investigation and compliance. Most of these elements consist of activities performed by IoM stakeholders. Hence, they affect *anonymity-transparency* trade-offs of relevant IoM socio-technical ecosystems from a "social" standpoint.

In this chapter I furthered the application of the teleological approach when evaluating the meaning of features such as *anonymity* and *transparency* in the domain at hand. Accordingly, various types of *anonymity* enhancements were outlined with respect to the traditional phases of the laundering process. This highlighted not only the growing relevance of virtual-to-virtual *layering* schemes, but also the difference between laundering "of" and "through" cryptocurrencies. Relatedly, I outlined the understanding of *anonymity* that emerges from the risk indicators published by the FATF. Since various aspects are reported without a clear classification of the ways in which *anonymity* can be enhanced, I addressed the relevant risk factors

individually and performed an assessment of whether their *anonymous* character pertains to *obfuscation* (*e.g.*, AECs, mixing, PETs), *enhanced disintermediation* (DEXes, DeFi), or is related to other specific circumstances. Moreover, I argued that in different scenarios the *anonymous* trait may stem from embedded technologies, processes that are implemented on top of it and/or also additional behaviours (*e.g.*, user best practices). Parallelly, I overviewed the main deployed forensic approaches, from the chief standpoint of the techniques of transaction network analysis, that usually leverage graph visualisation tools, underlining the role of clustering. Further, I introduced recent applications of AI for anomaly detection, outlining the value of the combination between machine learning-based approaches and graph analysis.

This investigation displays how *anonymity* enhancements and forensic techniques are engaging in a likely never-ending race. It follows that any regulatory instrument needs either to be constantly updated or conceived and drafted in a way that grants the flexibility to adapt to continuous evolutions. In this respect, I suggested the identification of specific benchmarks to differentiate between the various degrees of *anonymity* enshrined by IoM ecosystems without running into the risk of overfitting. It is in this context that the concept of *accountability*, ensured by the *auditability* of relevant transactions, emerges as pivotal. Indeed, both *obfuscation* and *disintermediation* generate a situation where users are not *accountable* for their activity (in this case, for their transactions). Likewise, the socio-technical perspective accounts for players and techniques that pursue to increase or decrease *accountability* for IoM activities.

In this scenario, the feature of *auditability* assumes access to a given type of information is allowed in certain circumstances, by specific actors and for a specific purpose, in a way that does not breach *confidentiality*. Indeed, *confidentiality* and *auditability,* in the same way as *anonymity/privacy* and *transparency*, are not a zero-sum game, but generate different trade-offs that can be balanced depending on the intended objective. To this end, I argue cryptocurrency schemes and transactions can be assessed in term of their *privacy-transparency* and *confidentiality-auditability* trade-offs by referring to specific benchmarks such as the implementation of certain PETs. Chapter 5 elaborates on how these yardsticks can play out in the concrete evaluation of CBDC use-cases, and on how taxonomies can be built on top of it.

4. AML/CFT Regulation of Cryptocurrency Ecosystems in the EU and the Role of Global Standards

"*Cybercriminals dealing in cryptocurrency share one common goal: Move their ill-gotten funds to a service where they can be kept safe from the authorities and eventually converted to cash. That's why money laundering underpins all other forms of cryptocurrency-based crime. If there's no way to access the funds, there's no incentive to commit crimes involving cryptocurrency in the first place*".
Chainalysis (2022)

4.1. Introduction

Some concepts underlying the AML/CFT/CPF regime were mentioned in the previous chapters, as they depict the *fil rouge* between the different parts of the analysis. Although this regulatory domain may be perceived as a single entity with clear goals and pre-defined objectives, however, despite international efforts it would be a mistake to think only one AML/CFT/CPF framework exists today. Indeed, jurisdictions hold discretional powers in setting their own rules, and the motives of different regimes generate political debates and heated controversies.

The measures to prevent and repress the misuse of the financial system for illegal purposes comprise two different approaches: (i) criminal sanctions applied to those performing illegal deeds, generally on an individual basis and in some jurisdictions also at an entity-level;[502] (ii) rules placing a set of compliance and "active cooperation" duties on regulated entities, qualified in various ways depending on the legal system – *e.g.*, civil, administrative.[503] The latter category of provisions is the main target of this work, but the two sets of norms share core goals and definitional aspects. Regulatory guidelines are given at the international level from both perspectives, albeit with different degrees of bindingness according to each specific instrument.

[502] Liability of legal persons schemes are demanded by Articles 7 and 8 of Directive 2018/1673 (*e.g.*, "corporate liability for criminal offences"). This directive used to be named 6AMLD, which now labels one of the proposals of the 2021 AML Package, as outlined below. Frameworks of liability of legal entities are the Italian *responsabilità amministrativa degli enti (derivante da reato)* as per the Italian Legislative Decree 231/2001, as amended, and the Spanish *responsabilidad penal de las personas jurídicas* as per Article 31bis of the Spanish Criminal Code. Article 31bis was introduced by Organic Law 5/2010 and amended by Organic Law 1/2015.

[503] As explained in Chapter 3, the boundaries between civil, administrative, and criminal frameworks may not be clear in all legal systems. Usually, there is a special regime in terms of both substantial and procedural rules. Frequently, different sanctions (whose qualification depends on the severity of the deed) target violations of various norms, and different norms target different actors – *e.g.*, individuals, corporate entities, intermediaries.

Both regulatory responses bear upon sensitive areas that are intertwined with specific socio-economic contexts – *e.g.*, organised crime-related factors, tax crimes such as tax evasion, and fiscal policies. It follows they tend to be in a political limelight and exposed to territorial-based fragmentation. Nonetheless, international efforts have been made towards cooperation and harmonisation. Criminal law features sovereignty concerns and is traditionally of national competence, which makes approximation of laws more complex. Illustratively, in the process of EU integration its harmonisation has been subject to specific conditions.

This chapter brings together different elements to provide the foundations for the arguments of Chapter 5 and the techno-regulatory analysis of Chapter 6. AML/CFT/CPF provisions are at the heart of it, together with their relationship with the IoM. In conducting the investigation, I anchored the reasoning to two assumptions based on the findings of the previous chapters: (i) the AML/CFT/CPF regime established at the EU level must be analysed considering its position within a regulatory system chaired by the global standardisation activity of the FATF, and (ii) the socio-technical and multi-layered nature of the *anonymity* trait of IoM ecosystems must be taken into account when addressing the topic from a regulatory viewpoint. These considerations depict a hybrid nature of this chapter: it addresses on the one hand EU legislation and standardisation, and on the other hand technical and regulatory standardisation.

Accordingly, I structured the chapter to cover the following topics: (a) the core aspects of AML/CFT/CPF provisions affecting IoM ecosystems and stakeholders; (b) the diachronic link between AML/CFT/CPF and the perception of IoM *anonymity*; (c) the landscape of global financial regulation, where both FATF's and EU measures are positioned; (d) the presence of siloed technical and regulatory standardisation; (e) FATF's approach to the extension of its guidance to the IoM; (f) main AML/CFT/CPF duties and the extent to which the framework suits the IoM; (g) the EU AML Package and the creation of a EU-wide Authority, its techno-regulatory role, and the introduction of the crypto travel rule; (h) how the challenge of attribution mirrors the problem of *anonymity* and *unaccountability* outlined in the previous chapters.

4.1.1. Ratio and evolution of AML/CFT/CPF regimes

As introduced in Chapter 3, the final goal of AML/CFT/CPF measures is to prevent criminals from enjoying the economic profit of illicit activities, thwarting their capacity to disguise the origin of funds and provide them with a legitimate appearance. For this reason, when the framework was established in the 1970s and 1980s the focus was on proceeds of organised criminal activities with substantial returns – *e.g.*, trafficking in drugs and illegal firearms and

corruption.[504] The crimes that generate proceeds whose laundering is considered by law as money laundering are dubbed "predicate offences".[505] Predicate offences have gone through an important evolution, up to the broad definition by Directive (EU) 2018/1673.[506]

Another key evolution in the criminal treatment of money laundering concerned the qualification of "self-laundering" – *i.e.*, the same person perpetrates both the predicate offence and the laundering. Traditionally, the latter was absorbed in the primary offence, as the secondary conduct is performed in relation to the first one. Later, at the international and EU levels the criminalisation of self-laundering emerged as advisable. The notions of predicate offences and self-laundering are not only useful in a criminal law context. The definition of what qualifies as money laundering is a prerequisite to apply AML/CFT/CPF measures; it qualifies the illicit nature of the proceeds themselves, which depends on how predicate offences are construed. Hence, attempts were made to establish a global minimum standard. A key role is played by several treaties of the United Nations (UN) and the Council of Europe.[507]

According to FATF, the international AML/CFT/CPF standard-setter, money laundering should be criminalised based on the Vienna and Palermo Conventions, terrorist financing as per the Terrorist Financing Convention, financial sanctions should be implemented as per UN Security Council resolutions on the prevention and suppression of terrorism and terrorist financing, and the prevention, suppression and disruption of proliferations of weapons of mass destruction and its financing.[508] Likewise, money laundering must be interpreted to encompass "all serious offences, with a view to including the widest range of predicate offences".[509]

As argued in Chapter 3, well before the advent of the "blockchain hype" and the popularisation of cryptocurrencies, the deployment of "follow the money" techniques had emerged as a pivotal tool to investigate the activities of criminal groups and constrain their business. The subtraction of economic resources to criminals mostly consists of preventing them from disguising

[504] Gelemerova L (2009), pp 34-36
[505] Money laundering is a subsequent offence, or *delictum subsequens*, to a main offence, dubbed predicate offence or *delictum principale*. The FATF's Glossary defines "proceeds" as "any property derived from or obtained, directly or indirectly, through the commission of an offence".
[506] The definition is provided in Chapter 3.
[507] Vienna Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UN General Assembly (1988)), Convention for Suppression of Financing of Terrorism (UN General Assembly (1999)), Palermo Convention against Transnational Organised Crime and Protocols against human trafficking, migrants' smuggling, illicit manufacturing and trafficking in firearms (UN General Assembly (2000)), Mérida Convention against Corruption (UN General Assembly (2003)), Strasbourg Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Council of Europe (1990), Warsaw Convention (Council of Europe (2005)
[508] FATF Recommendations 3, 5, 6 and 7. Financial Action Task Force (2021b)
[509] FATF Recommendation 3. Ibid. Furthermore, not only the financing of criminal acts should be criminalised, but also that of terrorist organisations and individuals regardless of existing terrorist acts (FATF Recommendation 5). "Proliferation financing risk" is strictly related to the "potential breach, non-implementation or evasion of the targeted financial sanctions obligations" (Interpretative Note to FATF Recommendation 1, Paragraph 3)

the nature of their income and re-invest clean money in fruitful ways. In this regard, Chapter 3 addressed the laundering "process", underlining its conceptual value. From this perspective, one may focus on the "conducts/behaviours" that compliance frameworks aim to avoid.

The notion of money laundering comprises the efforts to hide the illegal origin of funds and those to channel into criminal activities funds earned in a lawful way.[510] Article 1(3) EU AML Directive (AMLD),[511] defines as money laundering the following *intentional* conducts:[512]

a. "conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such 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. "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 or from an act of participation in such an activity";
c. "acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity";
d. "participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions" above.

Article 1(3) AMLD rephrases Articles 3(1) and 4 Directive 2018/1673, and Article 3(5) includes self-laundering.[513] Article 1(5) defines terrorist financing as "provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA".[514]

4.1.2. What about cryptocurrencies? The "dark web" and the Silk Road saga

The previous chapters provided background information on the risky perception of the IoM that spurred regulatory initiatives targeting the application of DLTs to the financial sector. Among the risk elements, in this work I focus on those related to the alleged *anonymity* of these

[510] Goforth CR (2020), p 9
[511] The term "EU AML Directive" refers to the last consolidated version of Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 and lastly by Directive (EU) 2019/2177. The original text of Directive (EU) 2015/849 is the "4th AML Directive (4AMLD), while Directive (EU) 2018/843 is dubbed "5th AML Directive (5AMLD)".
[512] In this regard, Article 1(5) provides that "knowledge, intent or purpose required as an element of the activities referred to in paragraphs 3 and 5 may be inferred from objective factual circumstances".
[513] The topic was addressed by the European Court of Justice (2001)
[514] Council Framework Decision 2002/475/JHA, replaced by Directive (EU) 2017/541

ecosystems. This is a most relevant perspective in terms of regulatory drivers in the IoM space, as the first concerns about the misuse of cryptocurrencies originated when their (purported) *anonymity* was leveraged to perform illicit transactions.[515] A set of investigations started reaching the headlines, prompting public fear towards these instruments. This social mistrust was enhanced by the fact that in the early stages of cryptocurrencies their essence and ongoing evolution was remarkably difficult to convey to a non-expert audience.

On top of this, the (purported) *anonymity* of cryptocurrencies was mostly exploited on the "dark web", unfamiliar to most people. Its understanding is grounded on the difference between the "Internet" and the "world wide web", often used as synonyms. While the Internet is a huge network of networks, the web is built on top of it as a model to access and share information – *i.e.*, the web is "only" a (large) part of the Internet. The web's content can be "structured" or "unstructured" and there are three "layers of accessibility". On the one hand, the "visible/clear/ surface web" is readily available to the public, accessible by regular browsers and searchable by main search engines. It makes up for about 4% of the web.[516] On the other hand, the "deep web"– roughly 96% of the web but growing exponentially – whose content is not indexed. Its content includes medical and financial records, social media files, other data that needs to be kept private and secure.[517] Within the "deep web", the "dark web" cannot be measured, because its content is intentionally hidden. Special browsers are needed to access it: tools such as I2P, Freenet and TOR, transmitting data through multiple layers of encryption.[518] The *anonymity* of the dark web makes it perfect for activities people don't dare to do on the visible web.[519]

These "darknets" can also be used for legitimate purposes – *e.g.*, to avoid identity theft or censorship –, and software such as TOR and I2P was not developed to enable illegal activities. Nonetheless, its features of *anonymity* make it vulnerable to be exploited to trade illegal services or products, spread extremist ideas, share illegal content.[520] Hence, the dark web has been increasingly at the heart of investigations, either proactively (*i.e.*, LEAs look for information and attempt indexing) or reactively (*i.e.*, to gather information on a suspect, engaging in

[515] As far as the "purported" nature of *anonymity* is concerned, the reader is referred to Chapter 2. Before the advent of specific intelligence strategies, however, it is understandable transactions were perceived as *anonymous*.
[516] Kavallieros D, Myttas D, Kermitsis E, Lissaris E, Giataganas G, Darra E (2021), pp 4-5
[517] Ibid, pp 5-6
[518] TOR's technology was developed in the 1990s by US intelligence. In 2016, TOR had approximately 2.5 million daily users. The layers' number depends on the users acting as "nodes" at a given time. The objective is to safeguard *user anonymity* and avert traffic analysis that could reveal messages' origin, destination and/or content. The decentralised and P2P I2P overlay network was created in 2003 and offers *anonymity* through garlic routing, a variant of onion routing. Freenet is arguably the third largest darknet user-wise. Ibid, pp 10 and 14-15 and 16-17
[519] Many "dark web" websites aim to be accessible only to people that already know of their existence. Ibid, p 6.
[520] Ibid, pp 7-8

activities of *de-anonymisation* of dark web traces).[521] In this context, a significant win relates to the first "scandal" related to the criminal use of cryptocurrencies: the Silk Road case.

The Silk Road was a "darknet market" defined as an underground "Amazon for drugs", operated as a TOR hidden service.[522] In facilitating the exchange of illicit products and services, darknet markets leverage Bitcoin's (perceived) *anonymity* to avoid regulatory oversight and law enforcement. Arguably, many people first heard of Bitcoin in relation to the Silk Road case, which explains how it came to be perceived as inextricably tied to criminal activities, if not a vehicle for them.[523] The Silk Road was founded in February 2011 and shut down in October 2013 after the arrest of its operators. In November 2013 the Silk Road 2.0 was launched, and one year later it was shut down by the FBI and Europol.[524] Other marketplaces such as Agora and Evolution thrived in the aftermath but were later closed voluntarily and with an exit scam, respectively. Meanwhile, AlphaBay became the most active darknet market, and Nucleus and Abraxas were successful but ended in exit scams in 2016 and 2015.[525] While Silk Road 3.0 emerged as a scam and was taken down in 2017 by its admins, Silk Road 3.1 was launched.[526]

4.1.3. The rise and fall of darknet markets and the present day

The "dark web" appeared as a safe place for cybercriminals to trade illegal goods and services,[527] share information and criminal "best practices", with payments in cryptocurrencies. Darknet marketplaces offer a platform to both monetise and fund cybercriminal activities (*e.g.*, ransomware).[528] Hence, they were found to increasingly target victims with monetisation potential, as well as sensitive and valuable data. When criminals have access to crucial data, they extort the victims threatening to disclose it publicly.[529] While a wide range of new technologies

[521] Ibid, pp 20-22
[522] "Dark Web markets, darknet markets, dark markets, black markets and crypto-markets are some of the new terms that have been introduced in the recent years referring to all the online illicit marketplaces that have been developed and operate in the Dark Web environment" (Kermitsis E, Kavallieros D, Myttas D et al (2021), p 85)
[523] Goforth CR (2020), pp 8-9. Adler D (2018)
[524] "Operation Onymous" arguably exploited users' mistakes as well as TOR's technical limitations and security issues. Kavallieros D, Myttas D, Kermitsis E, Lissaris E, Giataganas G, Darra E (2021), pp 22-23
[525] Tsuchiya Y, Hiramoto N (2021a), p 2
[526] Kermitsis E, Kavallieros D, Myttas D, Lissaris E, Giataganas G, (2021), pp 101-102
[527] Examples of goods and services – also in terms of "cybercrime-as-a-service" – are drugs, stolen information, corporate data theft, credit card fraud, child abuse material, human organs, weapons, malware, and advanced hacking.
[528] "Malware" is any "*mal*icious soft*ware*" that intentionally harms a computer system, network or service. It includes viruses, ransomware, spyware. A "ransomware" attack consists of locking users' files or encrypting their system until users pay a ransom to receive the decryption key. It can be downloaded unwittingly from a compromised website or delivered in a phishing email. The most famous ransomware attack is WannaCry in May 2017, affecting more than 300,000 computers in 150 countries. Irwin ASM, Dawson C (2019), pp 111-112
[529] Kavallieros D, Myttas D, Kermitsis E, Lissaris E, Giataganas G, Darra E (2021b), pp 35-36

aid darknet operations, cryptocurrencies play a key role by facilitating payments, and the major players are Bitcoin and Monero.[530] The adoption of Monero is reportedly increasing, with 67% of darknet markets supporting it in 2021 as opposed to 45% in 2020, and some supporting it exclusively (*e.g.*, Archetyp). Nonetheless, Bitcoin still leads the way, supported by 93% of darknet markets. Overall, the trend is worrying: although the number of markets has decreased, in 2021 their revenue set a record of a total worth of USD 2.1 billion.[531]

After the 2013 shutdown of the Silk Road, various darknet markets have been launched and other scandals have impacted on the public perception of the IoM.[532] While a comprehensive account would fall outside the scope of this research, it is useful to consider a few examples to contextualise the remainder of this chapter's analysis. On the one hand, there were "exit scams": once the owners and/or admins of a marketplace had gathered a significant amount of cryptocurrencies the site became unreachable and outgoing transfers were blocked (*e.g.*, Nucleus Market, Sheep Marketplace, TheRealDeal, Abraxas).[533] On the other hand, some markets were taken down. This is the case of AlphaBay and Hansa Market, shut down in July 2017 by a joint operation of the FBI, the US Drug Enforcement Agency and the Dutch National Police, supported by Europol.[534] Parallelly, the 2014 scandal of the (alleged) hack of the Tokyo-based Mt Gox exchange led to the loss of around USD 473 million.[535] Similar events affected Bitfinex in 2015/2016, Coincheck in 2018, and Bitgrail in 2018, and the four hackings combined involved losses for more than USD 1.2 billion.[536] As outlined in Chapter 3, however, the abilities of LEAs are constantly evolving. In 2021, the FBI shut down the REvil ransomware strain and OFAC sanctioned two Russia-based service providers involved in laundering activities, Suex and Chatex.[537] Against this backdrop, the FATF classified the most common instances of criminal cryptocurrency misuse in three groups: (i) illicit trafficking in controlled substances, to perform sales or *layering*; (ii) frauds, scams, ransomware attacks, extortion; (iii) use by

[530] Kermitsis E, Kavallieros D, Myttas D, Lissaris E, Giataganas G, (2021), p 86
[531] Chainalysis (2022), pp 100 and 109
[532] Tsuchiya Y, Hiramoto N (2021a), p 1
[533] "Multisig" or "Trusted Markets" (*e.g.*, Wall Street Market) make the process safer via multi-signature transactions (more than one key is needed to release payments). The Wall Street Market is also an "Invite/Referral Market": users need an invite code or a referral link. In 2021 many closures were planned, perhaps to avoid investigation. Instead of the usual exit scams, users could withdraw funds in advance. Kermitsis E, Kavallieros D, Myttas D, Lissaris E, Giataganas G, (2021), pp 87-89. Tsuchiya Y, Hiramoto N (2021a), p 2. Chainalysis (2022), p 101
[534] In the aftermath of this "Operation Bayonet", vendors' active on AlphaBay and Hansa migrated to Dream Market. Kermitsis E, Kavallieros D, Myttas D, Lissaris E, Giataganas G, (2021), pp 112-113. Tsuchiya Y, Hiramoto N (2021a), p 3. Jardine E (2021), pp 992-994
[535] Johnstone S (2021a), p 58
[536] Johnstone S (2021b), p 121
[537] Chainalysis (2022), p 4. In brief, the Office of Foreign Assets Control (OFAC) is the agency of the US Department of the Treasury in charge of administering and enforcing economic and trade sanctions.

professionals launderers to transfer, collect and/or layer proceeds.[538] More recently, the case of Tornado Cash, whose *obfuscation* technique was mentioned in Chapter 3, displayed the full extent of cryptocurrency misuse enabled by mixers. In August 2022, it was blacklisted by OFAC due to the accusation of laundering more than USD 7 billion, including USD 455 million arguably stolen by a hacking group tied to the North Korean government.[539]

Although these events hurt victims considerably, the perception of cryptocurrency-related ML/TF/PF is significantly exaggerated. According to CipherTrace, between 2019 and 2020 crypto-crime decreased by 57%, going from USD 4.5 billion to 1.9 billions.[540] Likewise, criminal activities are argued to be 160 times more likely to involve fiat currencies than cryptocurrencies.[541] This narrative is confirmed by Chainalysis, reporting that although in 2021 illicit crypto transactions reached an all-time high in terms of value – illicit addresses received 14 billion USD vis-à-vis 7.8 billion in 2022 – they also reached an all-time low in terms of share of crypto activity. Indeed, the total tracked transaction volume grew by 567% between 2020 and 2021, reaching USD 15.8 trillion in 2021. In other words, the growth in legitimate usage is more significant than the criminal one, which represented only the 0.15% of the volume.[542]

The same report provides metrics on ongoing laundering. At the beginning of 2022, cryptocurrency addresses identified as illicit hold a value of at least USD 10 billion.[543] In most cases, these wallets are associated with theft, darknet markets and scams. Cryptocurrency-related laundering appears heavily concentrated; most outgoing value from illicit addresses is sent to few services, some seemingly purpose-built. Given the amounts sent from illicit to hosted addresses, it was argued USD 8.6 billion (in cryptocurrency) was laundered in 2021.[544]

4.1.4. Multi-layered efforts and global financial standards

At the international level, AML/CFT/CPF efforts are coordinated by the FATF, a standard-setting organisation established in 1989 and already mentioned in the previous chapters. The

[538] Financial Action Task Force (2021e), p 12
[539] Marquardt P, Rosenberg G, Schisa W (2022). The accuse was facilitation of illicit cryptoasset activity by sanctioned persons, such as receipt of ransomware payments and state-sponsored cryptoasset theft. The designation was controversial because sanctions were imposed for the first time on a decentralised protocol (*i.e.*, a set of smart contracts on Ethereum). The goal is to prohibit any interaction with the application – *i.e.*, regulated entities must monitor, investigate, prevent and/or report any direct or indirect exposure to it.
[540] Goforth CR (2020), p 9. CipherTrace (2021)
[541] Goforth CR (2020), p 9. Clement S (2021). A similar position is found in many sources (*e.g.*, Lennon H (2021))
[542] Chainalysis (2022), pp 3-4
[543] A large portion does not originate from the criminal activity, but from the asset's value increase. Ibid, p 8
[544] Concentration means LEAs can hamper crypto crime significantly by disrupting these services. Ibid, p 10

scope of is activities is significantly broad, as they consist not only of policy making, issuing guidance to governments, authorities, regulated entities, the public at large, but also include monitoring the implementation and enforcement of its measures. Although FATF's Recommendations are instruments of soft law,[545] and as such not directly binding on individuals and organisations, participating jurisdictions committed to transposing them into national law.[546] In this regard, the FATF cooperates closely with FATF-Style Regional Bodies and observer organisations such as the International Monetary Fund (IMF), the World Bank and the UN.[547]

This chapter addresses AML/CFT/CPF regulation starting from international standardisation efforts. In this context, both the regulatory scope and the methodology are significantly close to the larger domain of financial regulation.[548] While a comprehensive analysis of this regulatory area falls outside the scope of this research, overlooking the role of soft law and global financial standardisation would insufficiently account for the role of FATF and the impact of other institutions' regulatory and policy activities on the IoM. Indeed, regulatory actions targeting cryptocurrencies and their stakeholders, as well as their underpinning methodologies, were not created from scratch, but relied on established mechanisms of coordination.

International financial regulation consists more of a compound of rules, standards, and best practices, than of a clear-cut legal area. In addition, there is a tendency to focus on the national implementations of its various ramifications (*e.g.*, banking, securities, insurance), each equipped with its areas of emphasis and objectives.[549] Hence, its specifics and standard-setting procedures run the risk of being neglected. Starting from the late 1980s, however, financial integration and increasing cross-border capital flows urged regulatory cooperation.[550] In other words, the need to prevent market participants from escaping national supervision required the setting of global standards and prudential guidelines through international forums that could suit the evolving nature of capital markets.[551] Nonetheless, while most areas of international economic law, such as tax and trade law, are construed on legally binding treaties, international financial regulation consists of global rules adopted as informal and non-binding agreements,

[545] The role of "soft law" and "standardisation" in the domain at hand is explored below and in Chapter 6.
[546] Karasek-Wojciechowicz I (2021), p 2
[547] Financial Action Task Force (2021b), p 8
[548] For an in-depth critical analysis: Brummer C (2015b), pp 1-22. Indeed, "irrespective of the correctness of positioning cryptoassets in the arena of financial regulation, the fact is that the financial use of cryptoassets has been expanding rapidly" (Johnstone S (2021c), p 157).
[549] However, all sectors of financial regulation share two focus points: (i) reduction of the information asymmetries; (ii) systemic risk generated by financial institutions. Brummer C (2015b), pp 3-4 and 7-10
[550] To protect financial market stability and consumers. Ibid, pp 10 and 17. Kerwer D (2005), pp 613-614
[551] Brummer C (2015c), p 62.

either by regulatory agencies or by institutions with undefined legal identities.[552] In this respect, soft law was defined as a compendium of "instruments or agreements that are not directly enforceable like treaties, but that nevertheless create powerful expectations",[553] and its role as regulatory mechanism is increasingly key.[554] In this sense, the global regulation of finance features a low degree of institutionalisation and widely relies on voluntary compliance.[555] However, the coerciveness of regulatory instruments is more a matter of enforcement than obligation. If compliance can be enforced, standards and best practices can be interpreted from a functional viewpoint as part of international law also if not formally recognised as such.[556]

The architecture of relevant organisations provides valuable insights.[557] On the global financial market arena, the main institutions to create regulatory policies are the G-20, the Financial Stability Board (FSB), the International Organisation of Securities Commissions (IOSCO) and the Basel Committee on Banking Supervision (BCBS).[558] The public perception of their role has risen since the 2008 financial crisis and after peer review processes proliferated in its aftermath.[559] From a systematic viewpoint, different types of entities are involved in financial regulation: they (i) set the core agenda for the international regulatory system (*e.g.*, G-20, FSB);[560] (ii) focus on standard-setting itself, issuing prescriptive guidance usually on specific sectors or issue areas (*e.g.*, FATF), and/or (iii) monitor the system and check compliance (*e.g.*, World Bank, IMF). This is an integrated system where "broad-based and more-political institutions set agendas and assess gaps, whereas more-technocratic sectoral and specialist standard setters promulgate best practices and, in some instances, granularised rule".[561]

The "agenda setters" sub (i) are not involved in the daily process of standard-setting. The definition of standards to be adopted or implemented at a national level is a task of less political bodies that are inherently "sectoral" – *i.e.*, their mandate focuses on specific financial

[552] Brummer C (2015b), p 3
[553] Merchant GE, Allenby B (2017), p 108. In the area of international business governance, soft law was referred to as "civil regulation", defined as "codes, regulations, and standards that are not enforced by the state and that address the social and environment impacts of global firms and markets" (Vogel D (2008), pp 262-264).
[554] Casanovas P, de Koker L, Hashmi M (2022), p 78
[555] Newman A, Bach D (2014), p 432
[556] Brummer C (2015b), p 5
[557] While these entities enshrine models of P2P technocratic cooperation, they are institutional players belonging to a hierarchical system of influence and power, with sophisticated internal designs. Brummer C (2015c), p 63
[558] The BCBS, the oldest standard-setter, was created in the 1970s to address risks arising from changes in banking.
[559] Brummer C (2015a), p viii and 1
[560] The G-20 and the FSB are the primary setters of the financial regulatory agenda. Since G-20's role was revived as a response to the 2008 crisis, it has been the most visible political forum for economic coordination. The FSB operates as its technocratic extension, with a focus on macroprudential regulation. Brummer C (2015c), pp 71-75
[561] These bodies feature diverging governance, but highly developed institutional structures, equipped with rules on membership, decisions, processes. Ibid, p 18, pp 69-70, pp 115-116

sectors.[562] In this respect, the BCBS is tasked with overseeing banks and other financial institutions. The best-known activities of the BCBC are the 1988 rules on capital adequacy ("Basel I"), their refinement in 2004 ("Basel II"), and recent efforts for a "Basel III".[563] Other bodies have limited mandates, such as the International Accounting Standards Board (IASB) and the Committee on Payments and Markets Infrastructure (CPMI).[564] Meanwhile, the Bank for International Settlements (BIS), in its regulatory capacity, supports the other institutions by conducting economic, monetary, financial and legal research.[565]

4.2. International Standards and the Financial Action Task Force

The mandate of the FATF is to define standards and promote effective implementation of regulatory and operational measures to fight ML/TF/PF and related threats to the international financial system.[566] The FATF Standards, known as Recommendations, relate to criminal justice, law enforcement, the financial system, its regulation, and international cooperation. They consist of a set of measures to be implemented by participating jurisdictions through individual regulatory and operational initiatives, and they are issued after consultation procedures.[567] Meanwhile, the FATF works with other international players to identify national vulnerabilities. Worldwide AML/CFT/CPF frameworks largely take after the FATF Standards, which include their Interpretative Notes and the definitions of the FATF's Glossary.[568] In terms of implementation, Member Jurisdictions are not expected to take identical measures on the grounds of their different legal, administrative, and operational frameworks, and diverse financial systems. Hence, the Recommendations are classified as "global standards".

---

[562] Brummer C (2015c), pp 76-77

[563] Basel I was adopted by all members and almost 100 non-members. It required banks to maintain 8% of their capital in risk-weighted assets. Basel II aimed to give the largest banks discretion regarding internal risk ratings. Basel III establishes a regime of capital requirements to identify financial institutions whose importance is systemic and determines practices of bank-compensation and corporate-governance with effects on financial stability. The BCBS is the primary standard-setter in the banking domain, IOSCO for securities, and the International Association of Insurance Supervisors (IAIS) for insurance. Brummer C (2015c), pp 79-81

[564] The IASB pursues the development of global accounting standards for investors, creditors, and regulatory authorities. The CPMI was created in 1990 to provide oversight and guidance on clearing and settlement – *i.e.*, technologies, procedures, rules for fund transfers among participating entities. Brummer C (2015c), pp 82-83, 86

[565] Brummer C (2015c), p 93

[566] The FATF has 39 Members: 37 members and 2 regional organisations (EC, Gulf Cooperation Council). It includes Associate Members (*e.g.*, Council of Europe's Moneyval, the Asia/Pacific Group on ML) and Observers (*e.g.*, Indonesia and bodies such as BCBS, Egmont Group, ECB, OECD, UN, IOSCO, IMF, World Bank, Europol, Interpol). The OECD cooperates closely and sanctions non-compliant institutions. Brummer C (2015c), pp 88-90

[567] Financial Action Task Force (2021b), p 7. Goforth CR (2020), p 10. Brummer C (2015c), pp 88-89

[568] Financial Action Task Force (2021b), pp 7-8

The FATF Recommendations are under constant revision and were last amended in March 2022.[569] Due to the specificity of the framework and its monitoring and enforcement, the Recommendations are regarded as one of the most successful examples of international standards. The scope of the regime was first broadened in 1996 (so-called "40 Recommendations"). In October 2001, efforts to combat the financing of terrorism (CFT) were included, thus creating the Eight (later Nine) Special Recommendations– *i.e.*, standards and common approaches for the detection, prevention, and suppression of the TF and terrorist acts – and establishing the current version of the framework, dubbed "FATF 40+9 Recommendations". Starting from 2008, the fight against the financing of proliferation of weapons of mass destruction (WMD) has been included by adopting a Recommendation to ensure effective implementation of targeted financial sanctions imposed by the UN Security Council.[570]

The contents of the Recommendations can be classified into six categories: (i) risk identification, development of policies and domestic coordination; (ii) pursuit of ML/TF/PF; (iii) application of preventive measures for the financial domain and other designated sectors; (iv) establishment of powers and responsibilities for investigative, enforcement and supervisory authorities; (v) enhancement of transparency and availability of beneficial ownership information of legal persons/arrangements; (vi) facilitation of international cooperation.[571]

The FATF Standards rely on participating countries having authorities and supervisors in place to regulate, monitor, supervise, and in some cases handle the licensing of, "regulated entities" in different sectors.[572] Supervisors are expected to have the powers to impose sanctions (disciplinary and financial) and to withdraw, restrict or suspend the license, if applicable.[573] At the receiving end of the cooperation obligations imposed on regulated entities there are national Financial Intelligence Units (FIUs).[574] A FIU receives, assesses, and shares financial information (*e.g.*, STRs/SARs, other data relevant for analysis and/or dissemination) with other national authorities or other FIUs.[575] Unlike other standard-setters, the FATF monitors

[569] The original Recommendations date back to the 1990s and focused on drug-related laundering, in the wake of the 1988 US efforts for a BCBS's Statement of Principles on Money Laundering and the Vienna Convention. While the frequent revision of principles is common for standard-setters, FATF also introduced a specific method to guide the application of the Recommendations – *i.e.*, Interpretative Notes (Brummer C (2015c), pp 88-89).
[570] Financial Action Task Force (2021b), pp 7-8. Brummer C (2015c), pp 88-89
[571] Financial Action Task Force (2021b), p 7
[572] Recommendation 26. Ibid
[573] Recommendation 27. Ibid. For DNFBPs, it can be a Self-Regulatory Body (Recomm. 28) – *i.e.*, as per Article 3(1)(5) AMLD, "a body that represents members of a profession and has a role in regulating them, in performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules relating to them"
[574] Recommendation 29. Ibid. In the EU, FIU establishment and operations is governed by Article 32 AMLD.
[575] In this respect, FATF establishes a framework of "mutual legal assistance" laid out in Recommendation 37, while in 1995 the Council of Europe established the Egmont Group to aid transnational information exchange

implementation of its principles through a system of mutual evaluations. A list of codes and criteria identify non-compliant jurisdictions, and a schedule of countermeasures is established.[576] The influence of FATF's guidance on national policies is complemented by the "blacklist" of non-compliant nations,[577] according to which regulated entities should perform enhanced CDD when dealing with individuals or entities of countries of "higher-risk".[578]

4.2.1. The FATF and Virtual Assets: definitions and timeline

Over the years, the focus of the FATF adjusted to the developments of the financial domain and the ways to transmit value over the Internet. It started to address IoM risks in June 2014, issuing a document with background notions on "virtual currencies (VCs)".[579] A year later, the first guidance to the application of the risk-based approach (RBA), defined below, to the cryptocurrency sphere was released.[580] These documents were limited in two ways: (i) they addressed the subset of VAs labelled as VCs, and (ii) exclusively focused on the "on and off ramps" to the traditional (regulated) financial system. In other words, on the points of intersection between the latter and activities in VCs (*e.g.*, VC-exchanges). Later, the FATF became increasingly aware of the evolution of the IoM towards "new products and services, business models, and activities and interactions, including virtual-to-virtual asset transactions".[581]

In October 2018, the FATF clarified the application of the Standards to "financial activities involving VAs", to urge the implementation of the measures on IoM-related service providers. The amended Recommendation 15 included "virtual asset service providers (VASPs)" into the standards' scope, also in terms of licensing, monitoring and supervision systems. The development of new products and services, and the introduction of different types of providers, led the FATF to provide clearer definitions of VAs and VASPs and to specify the Standards apply "to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs".[582]

---

[576] Brummer C (2015c), pp 88-89
[577] Goforth CR (2020), p 10
[578] Recommendation 19. Financial Action Task Force (2021b). Jurisdictions with "weak" ML/TF/ PF measures are identified through two "statements" routinely updated: "High-Risk Jurisdictions subject to a Call for Action", and "Jurisdictions under Increased Monitoring". The first document is the so-called "blacklist" and comprises countries with serious strategic deficiencies; currently, only the Democratic People's Republic of Korea and Iran. Financial Action Task Force (2021a) The second document is dubbed "grey list" and includes countries taking committed steps to resolve strategic deficiencies. Financial Action Task Force (2021c)
[579] Financial Action Task Force (2014). For an account of the way this work makes use of the term "cryptocurrencies" and "cryptoassets" instead of "virtual assets" or "virtual currencies" the reader is referred to Chapter 1.
[580] Financial Action Task Force (2015)
[581] Financial Action Task Force (2021e), p 7
[582] Ibid, p 8. Goforth CR (2020), p 10

The most recent FATF's definition of a VA is "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes", excluding "digital representation of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations".[583] The most recent definition of VASPs comprises natural or legal persons, otherwise not covered by the Recommendations, that as a business conduct – for or on behalf of another natural or legal person – one or more activities operations among: exchange between (i) VAs and fiat currencies or (ii) one or more VAs; (iii) transfer of VAs from one address or account to another; (iv) safekeeping and/or administration of VAs or instruments enabling control over VAs; (v) participation in and provision of financial services related to an offer and/or sale of a VA.[584]

In June 2019, the FATF adopted the Interpretative Note to Recommendation 15, to clarify the application of the RBA to VA activities and VASPs, supervision and monitoring mechanisms, licensing, preventive measures such as CDD, record-keeping, reporting, sanctions, enforcement, international cooperation. Relatedly, it issued the first comprehensive Guidance to apply its principles to VAs and VASPs, to aid national regulatory and supervisory responses, and to help the private sector understand the obligations.[585] This Guidance was revised in October 2021 after a public consultation. The update focused on (i) clarification and expansion of definitions; (ii) application of the Standards to stablecoins and conditions for the qualification of related entities as VASPs; (iii) risks posed by P2P transactions and countermeasures; and (iv) VASP licensing/registration; (v) "travel rule" implementation for the public and private sector; (vi) information sharing and co-operation among VASP supervisors.[586]

Meanwhile, in 2020 ransomware attacks had brought cryptocurrency risks into the spotlight again. The FATF noted how while some jurisdictions had implemented VAs-VASPs AML/CFT/CPF frameworks, in some cases these are not effective vis-à-vis the cross-jurisdictional development of cryptocurrencies, their growing adoption and functionalities. The ransomware-related use of VA emerged as a critical issue, especially when considering the growth of ransomware attacks on a global level.[587] Accordingly, in September 2020 the FATF published the "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing",

[583] Financial Action Task Force (2021e), p 109. Financial Action Task Force (2021b)
[584] Financial Action Task Force (2021e), p 109
[585] Financial Action Task Force (2019). Financial Action Task Force (2021b). Goforth CR (2020), p 11. Financial Action Task Force (2021e), pp 4 and 8
[586] Financial Action Task Force (2021e), pp 5-6
[587] Ibid, p 10

extensively addressed in Chapter 3, with a section on the concept(s) of *anonymity*.[588] Finally, a set of other documents bear influence on the FATF's regime for VAs and VASPs.[589]

4.2.2. The risk-based approach and crypto regulated entities: the FATF and the EU

The gist of AML/CFT/CPF measures tends towards global coherence in the form of compliance with the FATF Standards. At the most basic level, the regimes established in different jurisdictions rely on a set of "regulated entities", also labelled "obliged entities", required to provide "active cooperation" to the authorities, chiefly in terms of monitoring financial transactions and value exchanges. The end-goal of their compliance efforts is to timely draw the attention of competent authorities in case suspicions of illicit activities arise – more specifically, suspicions of "money laundering", "terrorist financing", and "proliferation financing", defined above. The number and type of reporting entities has increased over time. Their selection is grounded on the kind of involvement they have in financial transactions, thus on their (purported) oversight capacity in their day-to-day activities.[590] Although the range of regulated entities goes beyond the financial sector, the latter has a one-of-a-kind relationship with the compliance regime. As addressed in the previous chapters, the tension between financial *transparency* and *confidentiality* precedes the advent of cryptocurrencies. Indeed, FATF Recommendation 9 opens its part on "preventive measures" specifying that the presence of financial institution secrecy laws should not inhibit the implementation of the regime.[591]

The primary principle that sits at the core of all obligations and procedures comprised by the framework is the risk-based approach (RBA).[592] Accordingly, regulated entities are required to undertake preliminary assessments to be able to tune their compliance measures to

[588] Financial Action Task Force (2020d)

[589] In March 2020, the "Guidance on Digital ID" was released to help identification in digital contexts (Financial Action Task Force (2020c)). In June 2020, the "12-Month Review of the Revised FATF Standards on VAs and VASPs" identified areas in need of further guidance, while the "Report to the G20 on So-called Stablecoins" outlined issues in applying the standards to stablecoins (Financial Action Task Force (2020a). Financial Action Task Force (2020b)). In March 2021, a "Guidance on Risk-Based Supervision" also targeted VASP supervision, and in June 2021 the "Second 12-Month Review of the Revised FATF Standards on VAs and VASPs" identified implementation loopholes (Financial Action Task Force (2021f). Financial Action Task Force (2021d)). A revision of the Recommendations took place in June 2021. An amendment of the Interpretative Note to Recommendation 15 clarified the applicability of the requirements concerning PF (Financial Action Task Force (2021b)).

[590] The actual degree of oversight capacity of the different types of "reporting entities" is subject to heated debates. Various stakeholders do not always agree on the extent of daily monitoring burdens thrust on these entities.

[591] FATF Recommendation 9. Financial Action Task Force (2021b)

[592] While this work addresses duties imposed on "regulated entities", international and supranational frameworks also thrust on their members and supervisory authorities a set of RBA-related obligations – *e.g.*, in the EU risk assessments are to be issued EU-wide (by the EC), nation-wide and for specific sectors (by competent authorities). At the EU level, the application of the RBA is laid out by Article 6 AMLD with regard to the EU risk assessment, by Article 7 with regard to national risk assessments, by Article 8 with regard to entity-level application.

the principle of proportionality – *i.e.*, stricter if risk factors are higher and vice versa. To do so, they must consider risk factors identified by the FATF, such as the "red flag indicators", but also by the EU AMLD, national regulation, sector-specific and supervisory authorities. Consistently, they must set up internal policies, procedures, and controls.[593]

The RBA informs compliance in manifold ways. Besides obligations outlined below, the AMLD outlines the impact on internal structures and operations.[594] Pursuant to Article 8(1), the entity must take "appropriate steps" – proportionate to the entity's nature and size – to identify and assess the risk, considering "risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels". These risk assessments must be documented, updated, and made available to authorities and self-regulatory bodies.[595] As per Article 8(4), entities must have (proportionate) policies, controls and procedures in place. As examples of RBA at national-level, pursuant to Article 2(2)(2) "among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used", and Article 2(3) states that, provided a series of criteria are met and there is little risk, Member States can exempt a financial activity performed on occasional or very limited basis.[596]

According to FATF's terminology, regulated entities encompass financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs).[597] As per Interpretative Note to Recommendation 15 on "new technologies", countries should apply the Standards to VAs and VASPs and carry out risk-based assessments. Further, VASPs should be licensed or registered, adequately regulated, supervised, or monitored; they should not be supervised by a self-regulatory body, but by an authority that should conduct risk-based supervision and monitoring. Within the EU framework, regulated entities are listed by Article 2(1) AMLD, currently listing twelve categories.[598] Article 2(1)(g) and (h), added by the 5AMLD, include "providers engaged in exchange services between virtual currencies and fiat currencies" (*i.e.*, fiat-to-

[593] They may encompass organising training activities, audits, appointing a compliance officer, etc. The content of the RBA is outlined in FATF Recommendation 1 also in relation to Member Jurisdictions, that should identify, assess, and understand the ML/TF/PF risks they face, and adopt appropriate measures to mitigate them. Hence, countries can adopt a flexible set of measures, deploy their resources effectively and apply preventive measures commensurately. Financial Action Task Force (2021b), pp 8 and 10

[594] The AMLD is Directive 2015/849 (4AMLD) as amended by Directive 2018/843 (5AMLD) and by Directive 2019/2177. Consolidated text of Directive (EU) 2015/849. Directive (EU) 2018/843. Directive (EU) 2019/2177.

[595] Individual documentation may be deemed unnecessary if the sector's risks are clear (Article 8(2))

[596] Likewise, as per Article 4(1) they must apply the RBA to extend the Directive's scope "in whole or in part to professions and to categories of undertakings, other than the obliged entities referred to in Article 2(1), which engage in activities which are particularly likely to be used" for ML/TF purposes.

[597] DNFBPs comprise (insofar as they engage in specified activities) casinos, real estate agents, dealers in precious metals/stones, lawyers, notaries, accountants, trusts, and company service providers (Recommendation 22)

[598] Such as credit and FIs, professionals (*e.g.*, auditors, lawyers, accountants, notaries), casinos, art galleries

crypto exchanges) and "custodian wallet providers", respectively. As outlined in Chapter 1, a VC 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" (Article 3(1)(18) AMLD). A "custodian wallet provider" is an entity providing "services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer" VCs.

A comparison can be made with the US, where at the federal level FinCEN is the authority thrusted with the mission to fight the illicit use of the financial system. FinCEN first regulated cryptocurrency transactions in 2013, issuing a guidance on how to apply its rules to "persons administering, exchanging or using virtual currencies".[599] It targeted all stakeholders involved in the use, distribution, exchange, acceptance or transmission of VCs for another person, to clarify they can be regarded as "Money Services Business (MSBs)".[600] More specifically, "any person engaged in the business of accepting and transmitting value, whether physical or digital, that substitutes for currency (including convertible virtual currency, whether virtual-to-virtual, virtual-to-fiat, or virtual-to-other value) from one person to another person or location by any means" is regulated.[601] MSBs are required to register and follow AML/CFT rules as provided for by the "Currency and Foreign Transactions Reporting Act of 1970", as amended: the US Bank Secrecy Act (BSA).[602] The BSA is codified in 31 US Code §§ 5311 et seq. and lays out rules in line with the "active cooperation" enshrined by FATF Standards. In 2019, FinCEN issued guidance on the application of its Regulations to "Certain Business Models Involving Convertible Virtual Currencies".[603] Other requirements are set at the state level – *e.g.*, "Bit-License", introduced in August 2015 by the New York Department of Financial Services.[604]

4.2.3. An extensive array of obligations between CDD and STRs: the FATF and the EU

The structure of the FATF Recommendations provides an overview of the foundational elements of AML/CFT/CPF obligations, while EU implementation offers insights into their

[599] Department of the Treasury FinCEN Guidance (2013)
[600] 31 CFR §1010.100(ff). Goforth CR (2020) p10
[601] The obligations are equally thrust on "domestic and foreign-located money transmitters, even if the foreign-located entity does not have a physical presence in the United States and regardless of where it is incorporated or headquartered, as long as it does business in whole or substantial part in the United States". Financial Action Task Force (2021e), p 98
[602] Goforth CR (2020), pp 9-10. Several acts, including the USA PATRIOT Act, amended the BSA
[603] Department of the Treasury FinCEN (2019)
[604] Irwin ASM, Dawson C (2019), p 116

interplay. The section of FATF Recommendations on "preventive measures" outlines a primary set of obligations relating to CDD and record-keeping, as well as specific measures for certain customers or activities.[605] As per Recommendation 10, CDD must be carried out for new and existing (a) business relationships and, (b) under certain conditions such as a transfer above EUR/USD 15,000, for occasional transactions.[606] Additionally, CDD is required whenever there are (c) suspicions of ML/TF/PF, or (d) doubts on the veracity or adequacy of customer identification data. As per the Interpretative Note to Recommendation 15, the threshold above which VASPs must conduct CDD for occasional transactions is EUR/USD 1,000.

CDD measures comprise *identification* and *verification* of the *identities* of customers and beneficial owners.[607] In other words, they include KYC but also see beneficial owners as primary targets. Pursuant to Article 14(1) AMLD, *identity verification* shall "take place before the establishment of a business relationship or the carrying out of the transaction".[608] CDD must be applied to new and existing customers, on a risk-sensitive basis, at appropriate times, in specific circumstances.[609] CDD includes assessing purpose and intended nature of the business relationship, and ongoing monitoring (*e.g.*, transaction scrutiny).

The first CDD provision in the AMLD shows the relationship between CDD and the mitigation of *anonymity* risks. As per Article 10 "Member States shall prohibit their credit

---

[605] *E.g.*, Politically Exposed Persons (PEPs), correspondent banking, Money or Value Transfer Services (MVTS). As per FATF's Glossary, PEPs are individuals who are or have been entrusted with prominent public functions domestically or by a foreign country – *e.g.*, "heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials". MVTS are "financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belong"

[606] According to Article 3(1)(13) EU AMLD, a "business relationship" is "a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration". Article 11 EU AMLD lays out CDD duties as outlined by FATF. As per Article 11(1)(b)(ii), CDD is to be performed for an occasional transaction also when it constitutes a transfer of funds as per Regulation (EU) 2015/847, addressed below, exceeding EUR 1,000.

[607] The concept of beneficial owner is crucial. As per FATF Glossary, it is "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement". As per Interpretative Note to Recommendation 10, the beneficial owner of a legal person is the natural person(s) who ultimately have a controlling ownership interest in the legal person, depending on the ownership's structure – *e.g.*, it can be based on a threshold, such as any person that owns more than 25%. If the ownership criterium is not conclusive, the beneficial owner is the natural person(s) that exercise(s) control on the legal arrangement through other means, or, as a last resort, hold the position of senior managing official(s). In Article 3(6) AMLD it is defined 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". The provision lays out elements to identify the beneficial owner of corporate entities, trusts, legal entities such as foundations and trust-like legal arrangements.

[608] RBA-based exceptions are allowed – *e.g.*, it can "be completed during the establishment of a business relationship if necessary so as not to interrupt the normal conduct of business and where there is little risk" (Article 14(2))

[609] *I.e.*, "when the relevant circumstances of a customer change, or when the obliged entity has any legal duty in the course of the relevant calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s), or if the obliged entity has had this duty under Council Directive 2011/16/EU". Article 14(5).

institutions and financial institutions from keeping anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes",[610] and "take measures to prevent misuse of bearer shares and bearer share warrants". As mentioned above, CDD compliance must be performed on a risk-sensitive basis – *e.g.*, higher risks call for enhanced measures and low-risk situations *may* allow a simplified regime. Accordingly, the AMLD sets out a system of "simplified" and "enhanced" measures to be established at Member State level.[611] In this context, the risk factors listed sub (2) in Annex III – concerning "product, service, transaction or delivery channel" – include "products or transactions that might favour anonymity", "non-face-to-face business relationships or transactions, without certain safeguards", "payment received from unknown or unassociated third parties", "new products and new business practices". Because the RBA applies to *identification* and *identity verification*, "non-face-to-face business relationship or transactions" may constitute a risk factor, unless they rely on reliable and independent digital ID systems.[612] Regulated entities, without displacing their responsibility, may rely on *identification* and *verification* performed by regulated third parties.[613]

Other duties concern setting internal controls and procedures in compliance with the RBA (*e.g.*, policies, screenings, training programs, independent audits), and the obligation to submit Suspicious Transaction Reports (STRs) – in some jurisdictions Suspicious Activity Reports (SARs). Their submission is the core duty of the framework, to which the other ones are oriented. They are sent to FIUs (or sector-specific authorities) when the entity "suspects or has reasonable ground to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing".[614] Indeed, the goal is for authorities to be informed when an 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" (Article 33 AMLD).[615]

---

[610] To govern issues of intertemporal law, Article 10(1) specifies CDD must be performed no later than 10 January 2019, or in any case "before such accounts, passbooks or deposit boxes are used in any way"

[611] Albeit simplified CDD has a narrow scope of application after the amendments introduced by the 5AMLD. Factors of potentially "lower risk" are provided by Annex II, while those of "higher-risk" by Annex III

[612] Financial Action Task Force (2020c), pp 29-30. Annex III AMLD lists, among product/service risk factors, "non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities".

[613] Recommendation 17. Financial Action Task Force (2021b). The AMLD lays out necessary requirements in Articles 25 to 29. As per Article 25(1), "the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party". In digital ID systems, a regulated entity can act as a digital ID service provider (Financial Action Task Force (2020c), p 32)

[614] Recommendation 20 about FIs. Recommendation 21 outlines the principles of "tipping-off" (it is prohibited to disclose an STR was filed) and "confidentiality" (protection from liability for breaches of disclosure restrictions).

[615] As per Article 35, the transaction cannot be performed until the STR is sent and further instructions are complied with. However, if abstaining "is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation, the obliged entities concerned shall inform the FIU immediately afterwards".

4.2.4. From FATF Standards to regulatory and technical standardisation

FATF Recommendations are global regulatory standards, instruments of soft law, and formulated accordingly.[616] Some requirements are to be implemented at national level by *law*, which means by "any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance",[617] others by *law or enforceable means – i.e.*, "regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority".[618] The regulatory activity of the FATF is not, however, the only ongoing effort to set standards in the IoM space.

From a technical perspective, other initiatives have AML/CFT/CPF repercussions. In particular, standardisation efforts addressed blockchain technology and DLTs, where standards are an instrument to "accelerate the process of technology implementation, reduce transaction costs, level out regulatory risks, improve the interoperability of systems, and improve the quality of interaction between market participants, as well as it will increase the attractiveness of securing assets on a blockchain".[619] This landscape is populated by voluntary industry-driven initiatives, generating a fragmented scenario where the main focus is on terminology and security. A few international actions of technical standardisation are worth mentioning,[620] to introduce their relationship with regulatory standardisation, explored in Chapter 6.

On the one hand, the International Organisation for Standardisation (ISO) is the largest developer of voluntary standardisation, focusing on commercial, technical, and industrial standards. The ISO/TC 307 Technical Committee (TC) was created in 2016 for blockchain and DLT standardisation, to lay out a common language for safe and secure cryptocurrency use,

[616] To assess compliance, however, *should* is interpreted as *must*. Financial Action Task Force (2021b), p 128
[617] Due to the framework's global nature and the involvement of various legal systems, the FATF Recommendations specify *"*the notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country" (Ibid, p 115)
[618] Financial Action Task Force (2021b), p 115
[619] König L, Korobeinikova Y, Tjoa S, Kieseberg P (2020), p 1. World Economic Forum (2020b). Standardisation initiatives include European Telecommunications Standards Institute (ETSI) Industry Specification Group on Permissioned DL, ITU-T Focus Group, working groups by ISO, IEEE, Worldwide Web Consortium (W3C), EU Agency for Cybersecurity, European Committee for Electrotechnical Standardisation (CENELEC), Internet Engineering Task Force. Further, "NISTIR 8202 Blockchain Technology Overview" published by National Institute of Standards and Technology (NIST), "Distributed Ledger and Blockchain Technology Study Group" by ANSI Accredited Standards Committee X9, specifications issued by the German Institute for Standardisation (DIN).
[620] In line with the literature and despite the value of the ERC Token standard, this section does not consider "company specific protocols or processes which are sometimes falsely called "standard" […] as such implementations are only relevant for individual solutions and not globally applicable standardisation that is independent from the chosen blockchain platform". König L, Korobeinikova Y, Tjoa S, Kieseberg P (2020), p 4

including ISO/CD 22739:2020 on terminology, ISO/TR 23455:2019 on smart contracts, ISO/TR 23244:2020 on privacy and data protection, ISO 23257:2022 on architecture, ISO/TS 23258:2021 on taxonomy and ontology, ISO/TR 23576:2020 on security management of digital asset custodians, ISO/TS 23635:2022 on governance. ISO/TC 68/SC 8 focused on reference data for financial services, where ISO 24165 introduced the Digital Token Identifier.[621]

Secondly, within the International Telecommunication Union (ITU), the Telecommunication Standardisation Sector (ITU-T) develops international standards (*i.e.*, ITU-T Recommendations) to define infrastructural elements.[622] While the ITU-T Study Groups are technical groups that develop the Recommendations, Focus Groups are a flexible pre-standardisation exercise to respond to immediate needs.[623] The work of two Focus Groups is cited in this work: the one on Application of DLT, active from May 2017 to August 2019, and the one on Digital Currency including Digital Fiat Currency (DFC), active from May 2017 to June 2019. The Focus Group-DFC is a banking, fintech and telecom discussion forum, to share best practices, and develop deliverables, requirements for network infrastructure and CBDC standards.[624] Thirdly, the Cryptocurrency Security Standard (CCSS), introduced in 2014 and maintained by the CCSS Steering Committee and the Cryptocurrency Certification Consortium (C4), is a complementary open standard on cryptocurrency storage and usage – *i.e.*, "a set of requirements for all information systems that make use of cryptocurrencies, including exchanges, web applications, and cryptocurrency storage solutions".[625] It covers only wallet management.[626]

Although *technical* standards often pursue compliance goals, they usually refer to existing regulatory frameworks and do not pursue the establishment of *regulatory* standards. The two categories of standardisation, however, feature common aspects that mostly relate to the interplay between regulatory agencies and the expertise held by the private sector. In both contexts the lines are easily blurred between standards set by regulatory agencies and self-regulatory initiatives, as the first ones often rely on the second ones. This is because standardisation is one of the ways to solve or mitigate the problem of information asymmetry, as those inside the industry typically know it better than regulators. Often, this asymmetry is tackled by involving experts in regulatory processes or by adopting standards as minimum safeguards. The methodologies may mirror different phases of the development of a sector. Usually, self-regulatory

[621] Johnstone S (2021d), p 139. König L, Korobeinikova Y, Tjoa S, Kieseberg P (2020), p 6
[622] ITU-T (2022a)
[623] ITU-T (2022b)
[624] ITU-T (2022c)
[625] C4 (2022)
[626] In Chapter 1 I also mentioned the ITSA, the ITC and ITIN initiatives, the TTI by the BRI, with the TTF

efforts arise when there is minimal or non-existent regulation and are introduced for the industry to survive and grow.[627] While in the early phases standards may be perceived as a hindrance, the evolution of the industry introduces a plethora of stakeholders with various objectives and incentives. At this point, the appeal of short-term advantages is often overridden by long-term interests, providing a fertile ground to introduce standards in the form of "best practices". Later, "oversight regulation" is often driven by the shortcomings of self-regulatory initiatives.[628]

When a domain evolves quickly, regulators tend to rely on instruments that allow rapid responses, and they are often less formal. In these cases, standards are more about technical aspects than about distribution of powers.[629] Nonetheless, on a broader level financial regulators access industry expertise in many ways. Authorities often rely for technical advice and/or policy execution on self-regulatory organisations that are private sector authorities. The US SEC ordinarily draws from the monitoring and enforcement capabilities of the private sector, and almost every major regulatory authority receives suggestions from consumer panels, stakeholder groups, interested private actors, in terms of preferred regulatory strategies. However, the extent to which the private sector is formally involved in the decision-making process varies significantly. When self-regulatory organisations play a crucial role, such as in the US financial industry regulation and supervision, their involvement can go beyond self-regulation and private actors can take part in decision-making processes with regulators.[630]

Regulatory (*e.g.*, FATF) and technical (*e.g.*, ISO, ITU-T) standardisation, despite being usually pursued separately, are not detached concepts. On the contrary, they address similar (or the same) issues, and share self-regulatory organisations and industry stakeholders as invaluable source of knowledge. The ongoing debate on the crypto travel rule, outlined below, is a topical example of the importance of their interplay, and the same is true for CBDC interoperability mentioned in Chapter 5. As explored in Chapter 6, a cross-disciplinarity embedded into regulatory (or techno-regulatory) processes is at the heart of valuable and innovative regulatory methodologies today. From this perspective, I argue cross-disciplinarity could represent a step forward from cross-functionality (*i.e.*, presence of members of various regulatory authorities

[627] For instance, hacks can stimulate oversight and drive market participants to establish SROs. Tsuchiya Y, Hiramoto N (2021b), p 3. Industry members have different position: some want to be free from any centralised control or only accept community-based oversight, others actively seek to be regulated – *e.g.*, for the sake of legitimacy, to be accepted into commercial activities, as a competitive advantage (Johnstone S (2021e), p 21).
[628] Johnstone S (2021d), pp 135-136
[629] Brummer C (2015c), p 68
[630] Brummer C (2015d), pp 18 and 32

with different experiences and responsibilities) that is currently praised in the FATF architecture, where there is a combination of financial authorities and officials from LEAs.[631]

4.3. The EU AML/CFT Regime for Cryptocurrency Transactions

A key part of the EU activity in the AML/CFT sphere consists of incorporating FATF Standards into Union law.[632] Arguably, this alters their dynamics of diffusion: once a considerable number of jurisdictions legally endorse soft law, standards partially lose their nature of informal institutions, voluntary best practices, or products of private global governance. In the context of EU integration, EU law "acts as a legalisation mechanism that transforms soft law from informal transnational best practice into embedded rules".[633] The way standards are "hardened" influences the institutionalisation of global financial regulation.[634] After all, "the boundaries between voluntary and mandatory regulations, state and nonstate regulations, private and public law, and hard and soft law cannot always be sharply drawn".[635] Against this backdrop, considering the dynamics of global financial regulation, I explore the role of standards in the EU from a state of the art (in this chapter) and evolutionary angle (in Chapter 6).

Among other aspects, Article 5 TEU requires EU actions to comply with the principles of subsidiarity and proportionality. Arguably, it is not possible to achieve AML/CFT objectives in the Internal Market through regulatory actions at Member State level (principle of subsidiarity). Indeed, after three decades of activity in the area, the EC still underlines the detrimental effects of criminals exploiting the fragmentation among national regimes, and entities with cross-border activities having to comply with different approaches. From this perspective, Union action is required to ensure a levelled playing field when fighting inherently cross-border problems. The way in which EU initiatives do not go beyond what is necessary to achieve their goals (principle of proportionality) is underlined below (*i.e.*, minimum harmonisation).

The EU AML/CFT action is not a stand-alone framework. Besides the link with standardisation initiatives, it interacts with other pieces of EU legislation, in the areas of financial services and criminal law. Chiefly, it connects to the rules on payments and transfer of funds –

[631] Brummer C (2015c), p 106
[632] In this chapter, any reference to AML/CFT instead of AML/CFT/CPF responds to the need to fall in line with the wording adopted so far by EU institutions.
[633] Newman A, Bach D (2014), pp 430-432. The authors underlined the links between domestic law, global standards, soft law and private governance, while providing insights into the reasons for the resilience of some international standards vis-à-vis a frequent lack of global institutionalisation.
[634] Ibid, p 433
[635] Vogel D (2008), p 265

e.g., Electronic Money Directive 2 (EMD2), Payment Services Directive 2 (PSD2) – and other ties concern CDD and *identification* – *e.g.*, proposed recast of the eIDAS Regulation, which lays out rules on electronic identification for electronic transactions.[636] The relationship of the EU AML/CFT regime with the 2020 Digital Finance Package is underlined below.

4.3.1. The involvement of EU law and harmonisation initiatives

From 1991 onwards, the EU has drafted legislation to harmonise Member States' responses in the AML/CFT sphere. In terms of regulatory methodology, EU actions have so far taken the form of Directives of minimum harmonisation, where Member States can adopt stricter provisions than those laid out by the European regulator and considerable discretion is left to national transposition.[637] The EC recently confirmed the value of the approach, as the alternative of maximum harmonisation would be incompatible with the RBA.[638] Meanwhile, the evolution of EU measures to fight the misuse of the financial system mirrors the increasing socio-economic inter-connections at the global level and within the Single Market. This is not surprising, as integration provides opportunities to legitimate business, but also to criminals willing to launder illicit proceeds or fund criminal activities.

The preceding sections outlined the development of the scope of AML/CFT measures at the international level, from a limited framework to a comprehensive scheme. The EU harmonisation effort shows a similar process. The First AML Directive 91/308/EEC (1AMLD) had a narrow scope in line with the original 1990 FATF Recommendations.[639] However, it laid out the foundations of a framework on which the Second and Third Directives continued to rely. It took ten years before the Second AML Directive 2001/97/EC (2AMLD) updated the 1AMLD to comply with the "FATF 40 Recommendations", whose first version was adopted in 1996.[640]

---

[636] Directive (EU) 2015/2366. Directive (EU) 2009/110/EC. Regulation (EU) 2020/1503. Regulation (EU) 910/2014. European Commission (2021e). These frameworks belong to the multi-layered dogmatic context within which this work selectively addresses what is deemed relevant to answer its research question. While the EMD2 and the PSD2 offer complementary insights in terms of definitions, they do not provide innovative elements for what concerns mitigating the risks emerging from the socio-technical features of cryptocurrency transactions. Hence, for the sake of consistency, they are not analysed comprehensively.

[637] Article 5 AMLD: "Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing, within the limits of Union law"

[638] European Commission (2021a), p 5. Within EU requirements laid out by directives, in the case of "minimum harmonisation" a directive sets minimum standards and Member States retain the right of setting higher ones, while in the case of "maximum harmonisation" they cannot introduce stricter rules.

[639] 1AMLD: Council Directive 91/308/EEC

[640] 2AMLD: Directive 2001/97/EC

Similarly, the Third Directive 2006/70/EC (3AMLD) is closely related to the tightening of FATF's standards, as updated in 2003 and expanded to TF from 2001 onwards.[641]

Notwithstanding the ground-breaking character of early initiatives, the modern EU AML/CFT framework was established by the Fourth Directive (EU) 2015/849 (4AMLD), coupled with Regulation (EU) 2015/847 on information accompanying transfer of funds.[642] Three years later, a remarkable step forward was brought about by the Fifth AML Directive (EU) 2018/843 (5AMLD), whose provisions, outlined above, addressed the *anonymity* of VCs and providers of related services.[643] The legal basis of the current EU AML/CFT regime is Article 114 TFEU.

Additionally, Directive (EU) 2018/1673 focused on combating money laundering by means of criminal law, mostly in terms of prompting efficiency in cross-border cooperation and building upon Council Framework Decision 2001/500/JHA with regard to the criminalisation of money laundering.[644] Meanwhile, Directive (EU) 2017/1371 defined financial crimes affecting the financial interest of the EU, included in the predicate offences, while Directive (EU) 2017/541 introduced a common understanding of the terrorist financing crime.[645] Lastly, Directive (EU) 2019/1153 aimed to facilitate information exchange between authorities.[646]

4.3.2. The 2021 AML Package and the EU-wide rulebook

The landscape of EU legislative activities on AML/CFT is evolving. In July 2021 the EC put forward a set of legislative proposals – dubbed "AML Package" – to implement its May 2020 Action Plan for a comprehensive Union policy on preventing ML/TF.[647] The goal is not to thoroughly transform the framework, but to overcome the fragmentation caused by the national transposition of a directive-based and principle-based regime, thus ensuring its effective

[641] 3AMLD: Directive 2005/60/EC. The political and economic context of the 3AMLD was the aftermath of 09/11 and other terrorist attacks such as the 2004 bombings in Madrid. The definition of "serious crimes", the "predicate offences", was aligned to 2001 Council Framework Decision 2001/500/ JHA. Article 3(5)(f) of the latter includes as "serious crimes" all offences "punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months".
[642] 4AMLD: Directive (EU) 2015/849. In 2012, the FATF had extensively renovated its Recommendations, which still lie at the core of the new EU provisions
[643] 5AMLD: Directive (EU) 2018/843
[644] Directive (EU) 2018/1673. Reference is to the need to reach a sufficiently uniform definition of predicate offences and criminal treatment, including self-laundering (Recital 11: "Member States should ensure that certain types of money laundering activities are also punishable when committed by the perpetrator of the criminal activity that generated the property ('self-laundering') […]") and to pay attention to new risks and challenges generated by VCs (Recitals 5 and 6)
[645] Directive (EU) 2017/1371. Directive (EU) 2017/541
[646] Directive (EU) 2019/1153
[647] European Commission (2020c)

and consistent implementation. Meanwhile, the EC wishes to narrow the gap between AML/CFT actions and the Digital Finance Package adopted in September 2020, mentioned in Chapter 1, with main reference to the proposal for a Regulation on Markets in Crypto-Assets (known as the "MiCA proposal") and its definition of crypto-assets. From this perspective, in the AML Package cryptoassets are defined as per Article 3(1)(2) of the MiCA proposal, and "crypto-asset service provider (CASP)" means a CASP as defined in Article 3(1)(8).

The AML Package is largely based on Regulations and consists of rule-based obligations binding for all (natural and legal) persons within the EU. In other words, the proposed regime is based on legislative instruments that are applicable at domestic level in a direct and immediate way, without needing to be transposed into national legislation. Hence, the Union's approach to AML/CFT changes in terms of legal instrument for the sake of uniformity. The AML and the Digital Finance Packages adopt the same methodology of issuing their foundational norms through Regulations,[648] and in both cases the legal basis is Article 114 TFEU on the approximation of laws when it is necessary to the establishment and functioning of the Internal Market. In the two packages, the choice of legal basis is justified, respectively, considering the goal to remove establishment obstacles and improve the functioning of the internal market for financial services, and the capacity of ML/TF threats to generate cross-border level economic losses, functional disruption, and reputational damage.[649]

The AML Package implements the 2020 Action Plan, which was drafted in response to a set of analyses of the effectiveness the regime.[650] Building on the identified areas to improve, it is based on six pillars and chiefly on the need for harmonised and directly applicable rules, which had emerged as a priority to deal with cross-border situations. Three out of the six pillars demanded legislative action, and are addressed by the four legislative proposals, with the aim of establishing an EU-wide AML/CFT single rulebook, EU-level supervision, a support and cooperation system among FIUs.[651] The goal to establish a single rulebook is pursued by a Proposal for a Regulation on the prevention of the use of the financial system for ML/TF purposes (AMLR), and by a Proposal to recast Regulation (EU) 2015/847 to expand traceability

[648] In the AML Package all provisions that apply to regulated entities are laid out by Regulations, while organisational aspects of national regimes are governed by a Directive. European Commission (2021a), p 2
[649] Respectively, European Commission (2020b), p 4, and European Commission (2021a), p 4
[650] European Commission (2019)
[651] Besides the proposals for Regulations addressed below, the Package includes European Commission (2021d), whose last available text (5 December 2022), as amended during the legislative procedure, is Council of the European Union (2022d). The other pillars are ensuring effective implementation of measures, enforcing criminal law rules and information exchange, strengthening the international dimension.

requirements to cryptoassets.[652] While the latter is explored in the next section, the main points of the first proposal are the expansion of the list of "obliged entities" to include CASPs, the clarification of the requirements on internal policies, controls and procedures, and the granularisation of CDD measures, the streamlining of beneficial ownership requirements,[653] the clarification of red flags,[654] and the strengthening of the measures to mitigate the misuse of bearer instruments, and the inclusion of a limit to the use of cash for large transactions.[655]

From this last perspective, an EU-wide limit to cash payments of EUR 10,000 is set by Article 59, dubbed "limits to large cash payments".[656] In this respect, the EC plans to go beyond FATF Standards, to tackle Union-level risks.[657] To this end, Article 59(1) prevents "persons trading in goods or providing services" from accepting cash payments of over EUR 10,000 in a single transaction or several transactions which appear to be linked.[658] The threshold does not apply to private operations between individuals not acting in a professional function, nor to transactions made at credit institutions, albeit in the last case the operation shall be reported (Article 59(4)). Article 59 belongs to Chapter VII, dubbed "measures to mitigate risks deriving from anonymous instruments", which includes Article 58 on "anonymous accounts and bearer shares and bearer share warrants". Article 58(1) prohibits FIs and CASPs from keeping *anonymous* accounts, passbooks, safe-deposit boxes, crypto-wallets and any account that allows the *anonymisation* of the account holder.[659] Relatedly, the proposal underlines that it is necessary to prohibit *anonymous* crypto-wallets because cryptoassets' *anonymity* makes them vulnerable to criminal misuse, and *anonymous* crypto-wallets render transfers *untraceable* and hampers the *identification* of suspicious linked transactions and the application of adequate CDD.[660]

---

[652] European Commission (2021a). European Commission (2021c). The last available texts, as amended during the legislative procedure, are Council of the European Union (2022d) (5 December 2022) and Council of the European Union (2022c) (5 October 2022), respectively. If not specified otherwise, references to the provisions of the proposed AMLR and (recast of) FTR below are based on the most recent available text.

[653] The proposal sets rules to identify the beneficial owners of corporate and other legal entities, and a harmonised approach to beneficial ownership. It includes provisions to ensure consistent *identification* of beneficial owners of trusts and similar legal entities/arrangements. It sets disclosure requirements for nominee shareholders and directors and provides for mandatory beneficial ownership registration for non-EU entities doing business with an EU regulated entity or acquire real estate in the EU. European Commission (2021a), p 9 and Recitals 64-76

[654] The proposal clarifies rules on transaction identification. Further, to ease compliance with reporting duties and improve the effectiveness of analytical and cooperation activities, the AMLA is entrusted to develop technical standards with a uniform common template for STRs. Ibid, p 10 and Recitals 77-78

[655] Ibid, pp 2-3

[656] Article 2(1)(30) defines "cash" as "currency, bearer-negotiable instruments, commodities used as highly- liquid stores of value and prepaid cards, as defined in Article 2(1), points (c) to (f) of Regulation (EU) 2018/1672".

[657] Ibid, p 3

[658] Member States can adopt a lower limit. In three years, the EC will assess the impact of lowering the threshold

[659] If the instrument exists, before it is used CDD measures are to be applied to owners and beneficiaries.

[660] Ibid, Recital 93 Furthermore, as per Article 58(3) companies are prohibited from issuing bearer shares and shall convert the existing ones, unless they are listed or their shares are issued as intermediated securities, while the issuance of bearer share warrants is only allowed in intermediated form (Ibid, pp 10-11)

With reference to CDD measures, specifications are introduced on *identification* and *identity verification*, as well as the conditions to use means of electronic identification.[661] This pursues coherence with other Union policies on remote customer onboarding in compliance with the Digital Finance Strategy. The main reference is to the proposed revision of the eIDAS Regulation on a framework for a European Digital Identity and related wallets and trust service, in particular for what concerns the electronic attestation of attributes.[662] As explored below a new authority would be in charge of providing details on simplified and enhanced CDD measures.[663] Most importantly, the first version of the proposed Article 15(2) provided that FIs and CASPs have to apply CDD when initiating or executing an occasional transaction that consists of a "transfer of funds" as per Article 3(9) of the (proposed recast of) Regulation (EU) 2015/847, or a "transfer of cryptoassets" as per Article 3(10), exceeding EUR 1,000. In the last available text, however, Article 15(2) applies only to FIs, while as per Article 15(2a) CASPs have to apply: (i) CDD when performing an occasional transaction of at least EUR 1,000 (single operation or linked transactions), but also (i) at least Article 16(1)(a) – *i.e.*, *identification* of the customer and *verification* of the customer's identity – for transfers below said threshold.[664]

From a second viewpoint, the Action Plan outlined the need for EU-level supervision. This urgency had been underlined for some time, and Regulation (EU) 2019/2175 had attributed to the EBA core competencies on the coordination and monitoring of the implementation of the AML/CFT framework.[665] This methodology, however, had not proven sufficient vis-à-vis the difficulties of competent authorities to cooperate effectively both domestically and cross-border, the existing divergences in the application of the RBA, also in terms of supervision, and the specificities of the EBA's governance model.[666] Accordingly, the AML Package put forward a proposal for a Regulation creating an EU Authority for AML/CFT (AMLA and AMLA Regulation).[667] In this respect, the rules-based nature of the AMLR is expected to provide a consistent framework for the AMLA to supervise its application.[668] The tasks thrusted on the AMLA vary according to different targets. The authority is expected to:

---

[661] European Commission (2021a). In particular, regulated entities shall accept for CDD purposes electronic identification means and relevant trust services as set out in the eIDAS Regulation (Article 18(4)(b)).
[662] Ibid, Explanatory Memorandum. The eIDAS Regulation defines "electronic identification" as "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person" (Article 3(1)(1)), and "electronic identification means" as "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service" (Article 3(1)(2))
[663] Ibid, p 9, Recitals 35-39, referring to Regulation (EU) 910/2014, European Commission (2021e)
[664] Article 15(2b) provides the same for all obliged entities when it comes to cash transaction of at least EUR 1,000.
[665] Covolo V (2020), p 250
[666] Regulation (EU) 2019/2175. European Commission (2021b), p 3
[667] European Commission (2021b). European Parliamentary Research Service (2023)
[668] European Commission (2021a), p 3

- Perform direct supervision on "selected regulated entities" – *i.e.*, "the riskiest cross-border financial sector obliged entities" –, with related powers to adopt binding decisions, administrative measures, and pecuniary sanctions. In this context, the AMLA is expected to ensure group-wide compliance, carry out supervisory assessments, participate in group-wide supervision, develop a system to assess risks and vulnerabilities;
- Provide assistance to financial supervisors, review the adequacy of resources and powers, promote convergence and high supervisory standards, coordinate information exchanges;
- Coordinate peer reviews of standards and practices of non-financial supervisors, request investigation of possible breaches, perform reviews, provide assistance;
- Help national FIUs conduct joint analyses of cross-border cases, offer services and tools for information sharing, promote knowledge on detection, analysis, and dissemination of STRs, provide training and assistance, coordinate threat assessments;
- Adopt regulatory technical standards (RTSs), implementing technical standards (ITSs), guidelines or recommendations for regulated entities, supervisors or FIUs, to ensure consistency of EU rules with international standards, promote supervisory convergence.[669]

4.3.3. EU law, international standards, and AMLA's RTSs

AML/CFT measures adopted at the EU level are deeply intertwined with FATF Standards. Besides the prestige of the international framework, the cross-border nature of ML and TF would make siloed Union actions largely ineffective. For this reason, the EC pursues international coordination and the adoption of measures compatible with (or at least as stringent as) international ones.[670] The value of the tie is undisputed, but the formal relationship between EU law and international standards is a more complex and open-ended topic. It concerns the FATF's action but also BCBS's standards, in terms of implementation of the standards into EU law and legal basis for the participation of EU institutions in standard-setting processes. In line with the evolution of EU financial integration, the ECB, the EC and the EBA take part into the BCBS together with national authorities, the ECB also as a representative of the Single Supervisory Mechanism (SSM).[671] However, some areas tackled by the BCBS, such as AML/CFT, fall among the competences of national supervisory authority, not of the SSM.[672]

[669] European Commission (2021b), pp 11-12, Recital 9, Articles 5-6
[670] European Commission (2021a), Recital 4
[671] The EC and the EBA are observers; the ECB and SSM represent the Monetary and the Banking Union
[672] Viterbo A (2019), pp 212-213 and 223

In this context, the relationship between EU law and BCBS standards was analysed under the lens of an increasing politicisation of a technocratic debate on financial regulation. In the wake of the 2008 crisis, an emerging distrust in technical knowledge reduced the perceived value of technocracy as a basis for authority.[673] In addition, although the participation of EU institutions in the BCBS standard-setting process causes problems of legal basis under EU law, the issue was largely ignored upon the establishment of the Banking Union. Against this backdrop, literature focused on the need to improve the credibility of technocratic authorities in terms of transparency, accountability, protection of social values and public policy goals, by involving non-technical players and the civil society in developing standards.[674] This is not surprising: "when global standards are effective, the question of how to subject them to democratic control often arises", notably in terms of standard-setters accountability.[675] While the goal of this section is not to dwell on the democratic legitimacy of standardisation, I believe an EU-oriented cryptocurrency research on AML/CFT/CPF cannot ignore the challenges arising from the relationship between FATF Standards, the highly technical nature of the IoM, the mechanisms of EU law, and the dynamics between regulatory and technical standards.

From this perspective, it is insightful to consider the AMLA is expected to draft RTSs and ITSs related to key aspects of AML/CFT compliance. As per Article 38(1) AMLA Regulation, the AMLA can draft RTSs within the limits set by Article 290 TFEU to ensure consistent harmonisation when specified by the AMLR, Regulation (EU) 2015/847 and the 6AMLD.[676] RTSs are technical, do not imply policy choices and their content is limited by the delegating act. Their draft is submitted to the EC for adoption, which is by means of regulations or decisions (Article 38(4)). These instruments are not new to the EU financial services and banking domain, nor to the AML/CFT framework. Indeed, for instance, draft RTSs were published in 2021 by EBA on the AML/CFT central database,[677] and in 2017 by the ESAs on the implementation of group wide AML/CFT policies in third countries,[678] adopted by the EC in 2019,[679] and by the EBA on central contact points,[680] adopted by the EC in 2018.[681]

---

[673] Ibid, pp 206 and 227. The change of approach and perspective clearly emerges when comparing post-crisis literature with previous analyses of the success of the BCBS system – *e.g.*, Kerwer D (2005), pp 619-620
[674] Viterbo A (2019), pp 206 and 228
[675] Kerwer D (2005), p 611
[676] As per Article 290(1) TFEU, a legislative act may delegate to the EC the adoption of non-legislative acts to supplement or amend non-essential elements. Objectives, content and scope are defined in the legislative acts.
[677] European Banking Authority (2021)
[678] European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority (2017)
[679] Commission Delegated Regulation (EU) 2019/758
[680] European Banking Authority (2017)
[681] Commission Delegated Regulation (EU) 2018/1108

In this context, the AMLD, in combination with the regime on ESAs introduced by Regulation (EU) 2019/2175 (Article 9a on EBA's tasks related to AML/CFT), thrust on the ESAs the drafting a series of specifications. It refers to RTSs in Article 45 (6-7, 10-11) AMLD, and to guidelines in Articles 17, 18(4) and 48(10) AMLD– *e.g.*, on risk factors to be considered when performing CDD. The AML Package, however, besides appointing a dedicated Authority, increased the array of matters to be covered by RTSs. The qualification grants the outcome of AMLA's work, when adopted by the EC, with the status of Delegated Regulation and related binding effects. Indeed, they are to be adopted as a supplement to the AMLR (Article 15(6) AMLR, Article 42 AMLA Regulation). The AMLA is also mandated to adopt guidelines, recommendations and opinions (Article 43 AMLA Regulation) on several topics.[682]

In particular, as explored in further detail in Chapter 6, the most comprehensive drafting concerns the application of the RBA to CDD. As per Article 15(5) AMLR, the AMLA is tasked to specify: (a) entities, sectors and transactions with higher risk; (b) related thresholds for occasional transactions; (c) criteria to identify linked transactions. The standards must build on the inherent risk levels of business models and the EC's supranational risk assessment (Article 15(6)). The AMLA is also expected to develop RTSs setting out (i) minimum information (*i.e.*, standard dataset) to be obtained when performing standard, simplified and enhanced CDD, depending on each customer's risk level (*i.e.*, as per Article 22(2), inherent risk of the service, transaction's nature, amount and recurrence, channels used); (ii) simplified CDD measures to be applied in lower risk situations; (iii) reliable and independent sources to perform identity verification of natural and legal persons; (iv) list of attributes for an eID scheme and relevant trust services (as set out by the eIDAS Regulation) to fulfil the requirements (Article 22). The goal is to enable the private sector to develop secure innovative means to perform identity verification and CDD, also remotely.[683] Additionally, as per Article 50(3) AMLR, the AMLA is expected to provide draft RTSs outlining a common template for reporting suspicious

[682] The difference between adopting draft RTSs and issuing guidelines emerges in Recital 9 AMLA Regulation: "certain aspects of the methodology, which can incorporate harmonised quantitative benchmarks, such as approaches for classifying the inherent risk profile of obliged entities should be detailed in directly applicable binding regulatory measures – regulatory or implementing technical standards. Other aspects, which require wider supervisory discretion, such as approaches to assessing residual risk profile and internal controls in the obliged entities should be covered by non-binding guidelines, recommendations and opinions of the Authority". For instance, the AMLA is expected issue guidelines on risk factors for regulated entities (Article 16(3) AMLR), and on extra-EU trends, risks and methods, with enhanced CDD measures to apply (Article 26 AMLR). In the development of the guidelines, findings of international organisations and standard setters are to be heeded.

[683] European Commission (2021a), Recital 41. Indeed, these RTSs "should provide sufficient clarity to allow market players to develop secure, accessible and innovative means of verifying customers' identity and performing customer due diligence, also remotely, while respecting the principle of technology neutrality".

transactions, to be used uniformly throughout the EU. The objective is to ease compliance and reporting but also to increase the effectiveness of analysis and cooperation among FIUs.[684]

4.4. The Crypto Travel Rule and Active Cooperation in the IoM

Over the years, the FATF's framework has expanded the scope of its measures to include (a part of) the IoM space. However, the approach still relies on "active cooperation" and there was arguably no alteration of the framework's fundamentals to tailor the regime to the specificities of the cryptocurrency world. On the one hand, RBA-based procedures and policies were adapted to the IoM, and most jurisdiction made considerable progress in responding to emerging risks. On the other hand, these efforts are insufficient to address comprehensively the array of problems associated with the IoM and thrust on the industry burdens that may be counterproductive. One of the most topical examples is the technological difficulty encountered by service providers when it comes to ensuring originators and recipients of cryptocurrency transactions are *identifiable* and not *anonymous*, to comply with the so-called "crypto travel rule".[685]

The crypto travel rule consists of the expansion of information sharing measures previously applicable only to transfer of funds performed via wire transfers (the "travel rule") to the IoM space. These rules require FIs to collect and share with their counterparties certain data to ensure *traceability* throughout the payment chain. Against the backdrop of the findings of the previous chapters, it is not surprising an intrusive "active cooperation"-based regime may generate friction when applied to the IoM. Indeed, although obligations such as the crypto travel rule may further integrate the IoM and the traditional financial system, they also pose substantial risks of displacing activities towards unsupervised areas – *e.g.*, to DEXes, given their proximity to the inspiration underpinning the "blockchain hype".[686]

4.4.1. The travel rule: FATF Recommendation 16 and Regulation (EU) 2015/847

The goal of FATF Recommendation 16 on "wire transfers" is to thwart the capacity of criminals to misuse the wire transfer system to move their funds. This is pursued by making sure to detect any attempt, trace the relevant transactions and collect the necessary information to hold them *accountable*. Hence, a duty is imposed on some regulated entities to collect, share

[684] Ibid, Recital 78. As per Articles 13-14 AMLR, a set of RTSs concerns group policies, branches, subsidiaries.
[685] Goforth CR (2020), p 11
[686] Johnstone S (2021a), p 76

and, in specific cases, make available to the competent authorities (*e.g.*, FIUs and LEAs) certain information on originators and beneficiaries of all wire transfers, both cross-border and domestic.[687] In other words, a set of data must accompany the funds throughout the payment chain.

Details on data to be collected and shared are laid out in the Interpretative Note to Recommendation 16, where a different regime concerns domestic and cross-border transfers.[688] In this context, diverse rules are imposed on FIs and MVTSs depending on whether they are (i) the ordering, (ii) the intermediary or (iii) the beneficiary entity. From the perspective of ordering FIs, cross-border wire transfers must include: (a) name of the originator, (b) originator account number – or, if not applicable, a unique transaction reference number; (c) originators' address, or national ID number, or customer ID number, or date/place of birth; (d) name of the beneficiary; (e) beneficiary account number – or, if not applicable, a unique transaction reference number.[689] For cross-border transfers, countries may adopt a minimum threshold no higher than EUR/USD 1,000 – whether in a single transaction or more transactions that appear to be linked –, below which they can apply the domestic regime. All data must be verified for accuracy and stored as per the record-keeping obligations. Accordingly, the ordering FI should not be allowed to execute the transfer if it does not comply with the requirements. Secondly, intermediary FIs must ensure originator and beneficiary information are retained with the cross-border transfer and take reasonable measures to identify cases where any data is lacking, which also means having procedures to reject or suspend the transfer and take follow-up actions.[690] Lastly, beneficiary FIs must take reasonable measures to identify cross-border transfers that lack some data, in terms of both real-time and post-event monitoring.

The FATF's travel rule was implemented in the EU in 2015. Although the AML Package marks a decisive change from a principles-based to a rules-based regime, the EU AML/CFT effort has never been a stranger to Regulations. Indeed, the 4AMLD was accompanied by Regulation (EU) 2015/847 on information accompanying transfers of funds (Fund Transfers Regulation (FTR)) sent or received by a PSP or an intermediary PSP established in the Union

[687] As per FATF Recommendation 16, *wire transfer* is any electronic transaction on the originator's behalf through an FI to make funds available to a beneficiary at a beneficiary FI. FI-to-FI transfers, where both originator and beneficiary are FI acting on their behalf, are exempted from the travel rule. The *originator* is the "account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer". The *beneficiary* is the "natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer".
[688] This distinction is relevant because cryptoasset transfers are considered inherently cross-border.
[689] For domestic wire transfers if the ordering FI can make this data available within a specific timeframe, only the account number or unique transaction reference must be included with the transfer itself.
[690] Pursuant to the FATF's Glossary, *reasonable measures* are defined as "appropriate measures which are commensurate with the money laundering or terrorist financing risks".

(Article 2(1)).[691] In this case, "funds" are defined as "banknotes and coins, scriptural money and electronic money",[692] and the concept of "transfer of funds" refers to transactions performed, at least partially, by electronic means, including credit transfers, direct debits, money remittances and transfers via payment cards, e-money instruments, mobile phones or other digital/IT devices (Article 3(9)). As per the FTR, the transfer's domestic or cross-border nature is assessed in terms of intra-EU (all PSPs involved are EU-based) and extra-EU (Articles 5-6).

4.4.2. The advent of the crypto travel rule: recent evolutions

Before the Interpretative Note to Recommendation 15 on "new technologies" was revised in 2018, the travel rule bore no mention to cryptocurrency funds, and at the EU level the FTR included no reference to the IoM sphere. However, the revision of the Interpretative Note addressed a specification on the application of Recommendation 16 to VA transfers. Countries were asked to introduce new rules on FIs and VASPs, whereby (i) originators obtain and hold required and accurate originator information and required beneficiary information, submit it to the beneficiary (if any) timely and securely, and on request make it available to the authorities; (ii) beneficiaries obtain and hold required originator information and required and accurate beneficiary information, and on request make it available to the authorities. The scope of application of other rules laid out by Recommendation 16 was extended accordingly – *e.g.*, data monitoring, freezing actions, prohibiting transactions with designated persons/entities.

Consistently, the AML Package includes a proposal to recast the FTR to narrow the crypto travel rule gap and adjust the regime to specific cryptoasset features.[693] The new rules target PSPs, CASPs and intermediary PSPs and introduce the obligation to collect and make accessible to the authorities specific data on originators and beneficiaries of cryptoasset transfers.[694] In doing so, the reform explicitly targets IoM-related *anonymity*, as "the global reach, the speed

[691] Regulation (EU) 2015/847. Article 2(4) excludes PSP-to-PSP fund transfers, and other cases, from the regime
[692] By reference to Article 4(15) Dir. 2007/64/EC (PSD) replaced by Article 4(25) Dir. 2015/2366 (PSD2). The definition of "funds" refers to Directive 2009/110/EC (EMD2), where e-money is "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer" (Article 2(2)).
[693] The most recent version of the text of the recast proposal is Council of the European Union (2022b). Whenever the previous European Commission (2021c) is quoted here with no further specification, it means the provision at hand remained the same in the more recent text. As per Council of the European Union (2022b) Recital 34f, the recast will be reviewed after the adoption of AMLR and AMLA Regulation, for the sake of consistency.
[694] As outlined above, this proposal refers to MiCA's definition of "cryptoassets", that corresponds to FATF's definition of "virtual assets", since the definition of CASPs encompasses VASPs. Meanwhile, the proposal includes "electronic money tokens" as per Article 3(1)(4) MiCA. European Commission (2021c), Article 2(4).

at which transactions can be carried out and the possible anonymity offered by their transfer, particularly expose crypto assets to the risk of criminal misuse against jurisdictions".[695]

The requirements of the proposal apply to (i) transfers of funds sent or received by a PSP or an intermediary PSP established in the EU, (ii) transfers of crypto-assets as defined in Article 3(10),[696] (iii) including transfers of crypto-assets by crypto-ATMs, where the CASP of the originator or the beneficiary is established in the EU (Article 2(1)). Considering risks related to cryptoassets and their specificities, all related transfers are considered cross-border transfers rather than domestic, as required by the FATF's Interpretative Note to Recommendation 16.[697]

In line with the RBA, the original version of the recast proposal distinguished between transfers (i) of more than EUR 1,000 – *i.e.*, individual transfers exceeding the threshold or more transfers seemingly linked – and (ii) below this threshold, where the latter were subject to a more lenient regime. This approach was rejected during the legislative process, and it is now argued the requirements should not depend on the amount because the *pseudonymity* of cryptoassets enables "large illicit transfers while circumventing traceability obligations and avoiding detection, by structuring a large transaction into smaller amounts", and most of these assets are "highly volatile and their value can fluctuate significantly within a very short time-frame that makes the calculation of linked transaction more uncertain".[698]

Hence, no matter the transferred value, according to Article 14(1-3) the CASP of the originator is required to: (a) obtain and hold for five years accurate – *i.e.*, "verified for accuracy" according to predefined criteria (Article 14(5-6)) – information on the payer – *i.e.*, name, distributed ledger address and/or crypto-asset account number,[699] address, official personal document number, customer identity number or date and place of birth, current LEI or equivalent official identifier (if applicable); [700] (b) certain information on the beneficiary – *i.e.*, name and distributed ledger address and/or crypto-asset account number, current LEI or equivalent

[695] Council of the European Union (2022b), Recital 7a
[696] A "transfer of crypto-assets" is "any transaction with the aim of moving crypto-assets from one distributed ledger address, crypto-asset account or any other device allowing to store crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same" (Ibid, Article 3(10))
[697] "Due to the inherent borderless nature and global reach of transfers of crypto-assets and of the provision of services in crypto-assets, there are no objective reasons to distinguish the money laundering and terrorism financing risk of national transfers compared to cross-border transfers. In order to reflect those specific features, an exemption from the scope of this Regulation for domestic low-value transfers of crypto-assets is therefore not appropriate, in line with FATF expectation to treat transfers of crypto-asset as cross-border transfer in nature" (Ibid, Recital 20a).
[698] Ibid, Recital 22a
[699] Please see below for further remarks on these elements.
[700] The Legal Entity Identifier (LEI) is "a unique alphanumeric reference code based on ISO 17442 standard assigned to a legal entity" (Article 3(21), Ibid).

official identifier (if applicable); (c) securely submit it to the beneficiary entity in advance of, simultaneously or concurrently with the transfer (Article 14(4)).[701] In turn, beneficiary CASPs are required to (i) monitor that the required data is included in the transfer or follows it (Article 16(1)); (ii) before making the assets available to the payee, verify the accuracy of the data using reliable and independent sources (Article 16(2)). Further, intermediary CASPs must ensure all data is relayed with the transfer, as well as comply with data retention obligations (Article 18a).

Upon request, all the information must be shared with the authorities. Meanwhile, it is prohibited for originating CASPs to execute any transfer before they can ensure full compliance, and beneficiary CASPs must establish procedures to apply when the required data is lacking, to decide whether to execute, reject or suspend the transfer, and to determine follow-up actions (Article 17(1)). Notably, if the beneficiary CASP realises there is missing/incomplete information, it must "reject the transfer or ask for the required information on the originator and the beneficiary before or after making the crypto-assets available to the beneficiary, on a risk-sensitive basis" (Article 17(1)). If a CASP repeatedly fails to provide the required data, the beneficiary CASP must (a) take actions such as issuing warnings or setting deadlines, return the cryptoassets to the originator, or alternatively hold the cryptoassets so they are not made available to the beneficiary, pending review from the authorities; (b) report the failure and adopted measures to the authorities (Article 17(2)); (c) consider the missing/incomplete data when deciding on the suspiciousness of the transfer or related transactions to report them accordingly (Article 18). Intermediary CASPs that become aware of missing/incomplete information can decide whether to reject the transfer and return the assets or to ask for further data. Follow-up measures are to be taken if the counterparty fails to cooperate (Article 18c).

4.4.3. Revision of the FTR: self-hosted addresses and other debates in the EU

The proposed recast provides for the possibility that a "distributed ledger address" – defined as "an alphanumeric code that identifies an address on a network using distributed ledger technology or similar technology where crypto-assets can be sent or received" (Article 3(17)) – and/or a "crypto-asset account number" – *i.e.*, an account held by a CASP "in the name of one

[701] As per Article 14(4), the data referred to by Article 14(1-2) does not need to be attached directly to or included in the transfer. Further, Article 15(1) provides that "in the case of a batch file transfer from a single originator, Article 14(1) shall not apply to the individual transfers bundled together therein, provided that the batch file contains the information referred to in Article 14(1), (2) and (3), that that information has been verified in accordance with Article 14(5) and (6), and that the individual transfers carry he distributed ledger address of the originator, where Article 14(2)(b) applies, the crypto-asset account number of the originator , where Article 14(2)(ba) applies, or the individual identification of the transfer, where Article 14(3) applies".

or more natural or legal persons which can be used for the execution of transfers of cryptoassets" (Article 3(18)) – may not exist in some transfers. Indeed, the originator may hold a cryptoasset account with a CASP, a "distributed ledger address", but also "any other device allowing to store cryptoassets" (Article 3(19)). Accordingly, in terms of data to collect, any reference to a "distributed ledger address" is limited to cases in which the transfer is "registered on a network using distributed ledger technology or similar technology", and any reference to an "account number" is limited to situations in which "such an account exists and is used to process the transaction" (Article 14(1)(b)). When this is not the case, the CASP of the originator must ensure the transfer is accompanied by a "unique transaction identifier" (Article 14(3)) that allows *traceability* of the transfer back to the originator and the beneficiary (Article 3(12)).

Because the AML/CFT framework is intermediary-based, it is not surprising the recast of the FTR does not apply to "person-to-person transfers" (Article 2(4)), defined as "a transaction between natural person acting as consumers for purposes other than trade, business or profession, without the use or involvement of a CASP or other obliged entity" (Article 3(14)).[702] One of the key points of the proposal, however, explicitly covers the regime applicable to transfers involving self-hosted wallets, using the innovative label of "self-hosted addresses", defined as distributed ledger addresses not linked to a CASP nor to similar entity established outside the EU (Article 3(18a)). Indeed, as per Recital 27, the recast applies to cryptoasset transfers to or from a self-hosted address if a CASP is involved, although it acknowledges the complexity of this regulatory endeavour and provides for a further evaluation to be performed by the EC.[703]

In the FTR recast proposal, transfers involving self-hosted addresses are provided with specifications in the context of the duties of originating and beneficiary CASPs. In particular, as per Articles 14(4a) and 16(1a), respectively, the CASP of the originator and of the beneficiary must obtain and hold the information mentioned above and ensure the transfer of cryptoassets can be individually identified. In addition, in case of a transfer exceeding EUR 1,000 to a self-hosted address, the CASP of the originator must "take adequate measures to assess if such address is owned or controlled by the originator", and in case of a transfer exceeding EUR 1,000 from self-hosted address the CASP of the beneficiary must take adequate measures to

[702] Similarly, the upcoming MiCA Regulation excludes hardware and software providers of non-custodial wallets from its scope of application (Council of the European Union (2022a), Recital 59)

[703] Indeed, Recital 44a provides that "Given the potential high risks associated with, and the technological and regulatory complexity posed by self-hosted addresses, including in relation to the verification of the ownership information" within a year after the application date of the Regulation "the Commission should assess the need for additional specific measures to mitigate the risks posed by transfers from and to self-hosted addresses, including the introduction of possible restrictions, and assess the effectiveness and proportionality of the mechanisms used to verify the accuracy of the information concerning the ownership of self-hosted addresses".

assess if the address is owned or controlled by the beneficiary. Indeed, as clarified by Recital 29b, upon transfers to/from self-hosted addresses, the CASP can usually collect information from the customer. In principle, the CASP is not required to verify data on the user of the self-hosted address. However, when the amount exceeds EUR 1,000 and is sent/received by/from a CASP on behalf of a customer to/from a self-hosted address, the CASP must verify that the self-hosted address is owned or controlled by that customer.

While the regime to be applied to transfers involving self-hosted addresses generates one of the key controversies surrounding the FTR recast proposal, another topical aspect concerns the interplay between the travel rule and data protection rules. Although the domain of privacy and data protection is not directly addressed by this work, in this scenario a few remarks are warranted. Indeed, the debate underlines the need to design the interplay between the AML/CFT/CPF sphere and privacy and data protection safeguards in the regulatory framework, which will be explored in Chapter 5 in terms of *privacy-transparency* trade-offs. Likewise, the specific crypto travel rule context (but the same could be argued outside the IoM) testifies to the need to design a regulatory framework whose compliance can be eased by technology – *i.e.*, RegTech solutions. This topic is at the heart of Chapter 6.

As provided for by Article 20(1) FTR recast proposal, the processing of personal data for its purposes is subject to the GDPR. Indeed, the data required by Article 14(4) must be submitted in compliance with the GDPR. Nonetheless, as outlined in Recital 25a, cryptoassets exist in a "borderless virtual reality", and many jurisdictions outside the EU have different data protection rules and/or enforcement measures. In this regard, Recital 17 argues the personal data transfer to a third country must comply with the relevant GDPR regime. At the same time, however, service providers with branches or subsidiaries outside the EU should not be hampered from sharing data about suspicious transactions within the same organisation but must apply adequate safeguards.[704] Because of this complex interplay, the proposal mandates on the European Data Protection Board, in consultation with the EBA, the duty to issue guidelines on how to implement in practice data protection requirements when transferring personal data to third countries in the context of a cryptoasset transfer. The EBA is also mandated to issue guidelines on suitable procedures to be adopted to determine whether to execute, reject or suspend a transfer whenever, upon transferring personal data to third countries, it is not possible to ensure compliance with the relevant data protection requirements.

[704] On the role of data protection issues in cross-border CBDC design: Fanti G, Pocher N (2022).

4.4.4. Active cooperation and the challenge of attribution vis-à-vis disintermediation

While the international debate evolves towards extending the scope of the travel rule to IoM transactions, the controversy comprises technical issues interwoven with policy decisions and business incentives, mirroring the tension between the evolution of the IoM and the needs of an AML/CFT/CPF regime that is intermediary based. At least three problems have emerged:

i. the impact of the rule to self-hosted to hosted wallet transactions and the legitimacy of restrictions;
ii. the challenge of linking cryptocurrency-related activity to the respective actors, at least in terms of *attribution* to *real-world identities* to be *identified* as originators and beneficiaries;
iii. the absence of global standards and technical solutions to underpin affordable compliance.

The first two issues could be phrased as a challenge of *attribution* of IoM activities, under two perspectives: (a) who is to be (and can be) regulated under the AML/CFT/CPF scheme, and (b) who are the *real-world identities* involved in the transaction as payer and payee. In other words, both viewpoints relate to the issue of *accountability* frequently mentioned in this work, albeit in this research *accountability* is usually referred to end users (*i.e.*, payer/payee). The problem sub (iii) is denounced by the industry, and it is an underlying issue that assumes a regulated entity is identified but lacks a RegTech solution to comply with the requirements.[705]

As the AML/CFT/CPF regime is traditionally based on the key role of intermediaries in the detection of suspicious transactions, also the revision of the FTR pivots on CASPs. When this approach is transposed to the IoM, however, it generates foundational problems. Arguably, this extension of preventive measures "fails to address the technological and structural peculiarities that distinguish cryptocurrencies from traditional banking and financial systems".[706] Although the previous chapters limited the value of the "blockchain hype", showing how IoM ecosystems are more intermediated than advertised, it is true that permissionless blockchains are inherently middlemen-free, that individual freedom is at the core of the onset of DLT-based monetary applications and that there are trends of *enhanced disintermediation*. For instance, as outlined in Chapter 2, self-hosted wallets significantly impact the efficacy of AML/CFT/CPF rules.

[705] de Koker L, Goldbarsht D (2022), p 309. Council of the European Union (2022b), Recital 36a: "In order to ensure technology neutrality, this Regulation should not mandate for the use of a particular technology when crypto-asset service providers transfer transaction information. To ensure the efficient implementation of requirements applicable to crypto-asset service providers under this Regulation, standard setting initiatives involving or led by the crypto-asset industry will be critical. Those protocols should be interoperable through the use of international or Union-wide standards in order to allow for a swift exchange of information".
[706] Covolo V (2020), p 247

Notably, two noteworthy scenarios generate a two-fold regulatory issue. On the one hand, in case of self-hosted to self-hosted wallet transactions the fact that there is no regulated entity involved eludes the travel rule and cash-related restrictions. While this encouraged regulators to consider restrictions, in terms of bans or often threshold limits, the issue generated a heated debate. Questions of legitimacy have arisen, and advocacy groups argue it could give way to total surveillance – at odds with fundamental liberties such as privacy and autonomy, and with financial inclusion – and also possibly generate a displacement of a considerable portion of activities towards unsupervised areas.[707] On the other hand, in case of self-hosted to hosted wallet transfers, when regulated entities receive a transfer they are required to obtain originator data but have no counterparty entity to interact with. Hence, self-hosted wallet holders could eventually be unable to transact with regulated PSPs, if unable or unwilling to provide the necessary information, or if the PSP adopts a de-risking approach and refuses to accept any transaction to/from self-hosted wallets in light of their real or perceived risk.

Hence, conflicting sentiments arise about the implementation of the crypto travel rule by the AML Package. While it is not easy to mitigate the risk of abuses without displacing illicit activities to P2P transfers, one wonders whether restricting self-hosted wallets unduly affects the freedom of economic activity, and/or whether the degree of enforceability of such limitations should bear any weight in the relevant policy-making.[708] Indeed, under the current regime it seems impossible to enforce restrictions outside the scope of regulatable entities,[709] while CASPs denounce the lack of affordable compliance tools, and experts outline the application of compliance requirements is over-burdening the industry.

Meanwhile, DeFi shows that even if the development of innovative services is influenced by regulation, part of the IoM is still leveraging technology to stay outside the border of compliance. As explored in Chapter 2, these new schemes generate a challenge of attribution of activities to a regulatable entity. The crypto travel rule is a prime example of how AML/CFT/CPF regulation is still dependent to the model of CEXs and has not captured DEXes yet.[710]

In this context, doubts have arisen about the nature of P2P trading platforms and DEXes, as strictly speaking these entities do not provide a service of exchange or conversion. Indeed, P2P exchanges provide users with a marketplace, handled by a software, that aids the connection between prospective buyers and sellers.[711] While the issue has been debated in the US, its

[707] Whitehouse-Levine, Kelleher L (2020)
[708] Pocher N (2021a)
[709] Pocher N (2021b)
[710] Johnstone S (2021b), p 125
[711] Covolo V (2020), pp 235-236

scope narrows significantly when considering the understanding of CASP provided by the MiCA proposal, referenced by the AML Package. Indeed, Article 3(1)(9) MiCA proposal includes as "crypto-asset service" the operation of a trading platform – where "multiple third-party buying and selling interests for crypto-assets can interact in a manner that results in a contract, either by exchanging one crypto-asset for another or a crypto-asset for fiat currency" –,[712] the execution of orders on behalf of third parties, placing activities, order reception and transmission on behalf of third parties and the provision of related advice. But even when a P2P platform falls within the scope of a given AML/CFT/CPF framework, identifying the entity that can be the target of the compliance regime is problematic due to the *non-centralised* architecture. Indeed, usually a DEX project after its launch does not involve an organised group but is operated automatically by the protocol and governance tokens holders.[713]

In this context, not only the share of IoM activity performed in contexts of *enhanced disintermediation* is not trivial, but the CEX-centric nature of compliance can generate a substantial shift of liquidity to DEXes. For the time being, the increase of DEX trading volume was linked to two drivers. Firstly, the total value locked in DeFi projects increased from USD 250 million in January 2019 to USD 1 billion in January 2020 to over USD 27 billion in January 2021 to more than 60 billion USD in April 2021. Secondly, the fact that DEXes currently do not fall within the VASP definition may have displaced speculative and illegal activity towards parts of the markets more complex to reach by regulation.[714] While the definition of the MiCA Regulation can mitigate the formal exclusion from the scope of the regime, it cannot solve the technical conundrum that makes it impossible to thrust "active cooperation" duties on them.

As introduced in Chapter 2, this is highly problematic. Indeed, it is possible to detect a considerable increase of DeFi laundering-related misuse, going from few examples in 2020 to a prevalence in 2021, when the increase DeFi protocols' usage for laundering rose of 1,964%.[715] Meanwhile, in 2021 for the first time CEXes did not receive more than 50% of the funds originating from addresses identified as illicit: CEXes received 47% and DeFi protocols

[712] European Commission (2020b), Article 3(1)(1)
[713] Massari J, Catalini C (2021)
[714] Johnstone S (2021b), p 125. Massari J, Catalini C (2021)
[715] The Spartan Protocol hack is a prime example of the use of DeFi for money laundering. After over 300 million USD-worth of cryptocurrency was stolen, the hackers converted the funds into anyETH and anyBTC (*i.e.*, Ethereum and Bitcoin composites respectively built on separate blockchains to the originals), then swapped some anyBTC for Bitcoin. At this point two DeFi chain-hopping protocols were used to convert funds into Ethereum and renBTC, and the funds were sent to a DEX and swapped for new Ethereum and wrapped Ethereum. The use of these platforms makes investigations significantly more complex. Lastly, the funds were sent to Tornado Cash, the mixer mentioned above and in Chapter 3. The hack took place in May and the hackers continued to launder funds until October. Notably, the activity would have been less effective if they had used centralised services, also on the grounds of their capacity to freeze funds in the event of suspicions (Chainalysis (2022), pp 7 and 12).

17%, while in 2020 they had received 2%.[716] Meanwhile, data reveal the preferred choice of malware operators to receive payments on self-hosted wallet addresses, with the second choice being to receive them to addresses hosted by high-risk exchanges with low or non-existent compliance. Likewise, in 2021 funds originating from cryptocurrency thefts have increasingly been sent to DeFi platforms (51%) or risky services (25%), while only 15% went to CEXes, possibly because compliance is "an existential threat to the anonymity of cybercriminals".[717]

4.5. Conclusions

This chapter investigated the AML/CFT/CPF regulatory context. Although the primary target of this research is EU law, Union-level initiatives are intertwined with the activity of the FATF in its prime function of global standard-setter. In this domain, most content of EU initiatives consists of implementing the FATF Recommendations. Indeed, besides the undisputable prestige of the framework, the cross-border nature of ML/TF/PF challenges siloed regional or local actions. Against this backdrop, this chapter addressed the evolution of AML/CFT/CPF regimes and the impact of the concept of predicate offences on the scope of application of compliance regimes countering financial crime. Accordingly, I provided an overview on the perception of IoM-related risks and the (purported) *anonymous* character of the sphere. To do so, I referred to scandals that depicted cryptocurrencies as the currency of choice of darknet marketplaces on the dark web, accessed using *anonymity*-enhancing tools, while also reporting data on the likely overestimation of cryptocurrency-related ML/TF/PF.

Further, focus was on the FATF as a sector-specific player within the dynamics of global financial regulation. In doing so, it underlined how models and products of technocratic cooperation are influenced by their position within a hierarchical system and analysed FATF Recommendations as global standards and instruments of soft-law, and their evolution along with the ways to transmit value over the Internet. Meanwhile, this chapter outlined the main AML/CFT/CPF obligations, through the lens of their implementation at EU level. Notably, it underlined how the RBA underpins all duties imposed on regulated entities and specified details of CDD and STR compliance. Moreover, it analysed selected technical standardisation initiatives on cryptocurrencies, blockchain technologies or DLTs. It underlined how technical and regulatory standards entail different methodologies but share the interplay between

[716] Ibid, pp 7 and 12
[717] Ibid, pp 61 and 74

regulatory agencies and private sector expertise. It expanded on the nature of the AML/CFT EU regulatory methodology as minimum harmonisation, while addressing the main initiatives included in the AML Package that pursues to overcome fragmentation. In doing so, it accounted for the impact of the process whereby standards are embedded into domestic law.

In this respect, in this chapter I focused on the different goals of the AML Package to establish an EU-wide AML/ CFT/CPF Single Rulebook, a system of EU-level supervision, and a support and cooperation system among FIUs. Relatedly, I underlined the prospective limitation of large cash payments and the prohibition of *anonymous* cryptoasset wallets. At this point, I analysed the proposed Regulation establishing the AMLA, placing the overview in the context of how an EU-based cryptocurrency-oriented research on AML/CFT/CPF is affected by the relationship between FATF Standards, the technical nature of compliance in the IoM, the mechanisms of EU law, and the dynamics between regulatory and technical standards. Starting from the formal relationship between EU law and international standards, in this chapter I addressed the AMLA and its task of drafting RTSs.

The application of the intermediary-based approach of the FATF's framework to the IoM space generates significant problems, and I argue they are exemplified by the difficulty to comply with the crypto travel rule and the related recast of the FTR at the EU level. The debate provides insights that go beyond its specifics and is an emblem of the tension between the nature of IoM ecosystems and a framework of "active cooperation". In this context, a multifold challenge of attribution of cryptocurrency activities emerges. The chapter focused on the impacts of the compliance regime on P2P or self-hosted to hosted wallet transfers and the legitimacy of possible consequent restrictions. Meanwhile, it heeds the challenge of linking transactions to the respective actors, at least in terms of attribution to *real-world identities*. Finally, it contextualised the shortcomings of the current approach vis-à-vis the revolution brought about by DeFi platforms and DEXes also in terms of money laundering trends.

5. Balancing Privacy and Transparency: Insights from CBDCs and a Case-Study Taxonomy [718]

"*Policy makers may have competing goals in providing anonymity to individuals, allowing the central bank or the private sector to provide identity-based services, and designing services to reduce illicit activities. From a solution perspective, these trade-offs will be reflected in choices about how identity is managed by the CBDC system*".
Oliver Wayman Forum (2022)

5.1. Introduction

The previous chapters explored how the promise of an electronic version of cash, possibly grounded on blockchain and DLTs, has electrified the world over the past decade. This prospect created an excitement for technological disruption that reminds of the 1990s, when the Internet entered the mainstream. As explained in Chapter 1, cryptocurrency-related developments were labelled to form an IoM and an IoV,[719] and their core premise lies in the functioning of blockchain systems. Being secured by cryptography and economic incentives and governed (in principle) by *non-centralised* consensus, they enable value transfers that transcend the need of a central authority. Accordingly, these setups showed the potential to replace legacy financial infrastructures, by eliminating layers of intermediation and informed a new "hype" of direct participation of citizens and businesses to a new global economy.[720]

As explored in Chapters 2 and 3, IoM ecosystems generate questions concerning *anonymity* and *disintermediation*, leading to socio-technical issues of *obfuscation* and *traceability*. Against the backdrop of the tension between *private* transactions and *accountability*, the chapters investigated the trade-off between *anonymity* and *transparency* from an AML/CFT/CPF standpoint. As outlined in Chapter 4, AML/CFT/CPF measures pivot on *identification* and *identity verification*, while *anonymity* is dependent on the observer and *anonymous* transactions are those that cannot be related to *identified* or *identifiable* individuals. *Accountability* emerged as ensured by the *auditability* of transactions, and *auditability* assumes access to certain data is

[718] *Contents and parts of this chapter have already appeared in the following co-authored publications:* Pocher N, Veneris A (2022a). Pocher N, Zichichi M (2022). Pocher N, Veneris A (2022b). Fanti G, Pocher N (2022)
[719] Tapscott D, Euchner J (2019), pp 12-19. Antonopoulos AM (2017b)
[720] Werbach K (2020). Walch A (2018). Casey M, Crane J, Gensler G et al (2018)

allowed in given circumstances without breaching *confidentiality*. Indeed, not only *privacy* and *transparency*, but also *confidentiality* and *auditability*, are not a zero-sum game, and can be balanced in different ways.[721] Since technology can be leveraged to embed a specific balance, an IoM scheme can be assessed by referring to given benchmarks (*e.g.*, PETs).

The prospect of a widespread adoption of programmable money has unsettled both governments and the private sector. As outlined in Chapter 1, leveraging tokenisation privately-driven projects of *(global) stablecoins* reached the headlines – *e.g.*, Facebook/Meta's Libra/Diem. Amidst this quest for value interconnection, monetary institutions have been trying to innovate payments and transmission channels, but also to rethink the essence of cash.[722] Their motivation partly lies in its possible disappearance, which could deprive citizens of government-issued money, and in the pursuit of novel payment channels to secure monetary identities and geopolitical boundaries.[723] Although central banks' interest in digital currencies started in 2014, most initiatives have stepped into the spotlight more recently and explore the deployment of blockchain technology. In 2021, with 86% of central banks reportedly exploring CBDC,[724] it became clear that if the full potential of this interconnection is fulfilled, the impact will affect many fields, including privacy and data protection, and law and regulation at large. Indeed, billions of IoT devices are increasingly deployed in our lives, and continuously collect valuable data related to huge economic sectors, such as healthcare and supply-chains.[725]

As argued below, the relationship between CBDCs and regulation inherently differs from the one between cryptocurrencies and regulation. This is due to the regulated nature of the stakeholders involved in CBDC projects and to their underpinning goals, that for the most part diverge substantially from those of cryptocurrencies. Indeed, the choice to consider CBDCs as part of the IoM for the purposes of this work does not intend to convey the message that cryptocurrencies and digital fiat money are concepts that can be equated from a phenomenological or ideological perspective. While investigating CBDC projects, however, it became clear to me that the design of these currencies provides most valuable insights into the features of IoM ecosystems. Most importantly, CBDCs display in a clear fashion the traits of *privacy*, *anonymity* and *transparency* introduced by previous chapters, and their socio-technical aspects.

---

[721] In line with the CBDC discourse, this chapter primarily addresses the trade-off between *privacy* and *transparency*. Indeed, as outlined in Chapter 2, *anonymity* is one of the possible ways in which *privacy* can be protected.
[722] Allen S, Capkun S, Eyal I (2020). Auer R, Cornelli G, Frost J (2020). Allen JG, Rauchs M, Blandin A, Bear K (2020)
[723] Allen S, Capkun S, Eyal I (2020). Adrian T, Mancini-Griffoli T (2019). Allen JG, Rauchs M, Blandin A, Bear K (2020). Sandner P, Gross J, Grale L, Schulden P (2020). European Central Bank (2020b). BIS (2021). Swartz L (2020)
[724] Codruta B, Wehrli A (2021)
[725] Al-Fuqaha A, Guizani M, Mohammadi M et al (2015). Ahlgren B, Hidell M, Ngai EH (2016). Pocher N, Zichichi M (2022)

I believe the multi-stakeholder interest in CBDCs offers an invaluable chance to dissect models of digital currencies and understand the way their features are influenced by technical and social factors, which are in turn affected by regulation. In setting the design of a specific CBDC model, a balance (or trade-off) is chosen between *privacy*, *anonymity*, and *transparency*, which in my opinion sheds a light on how these characteristics can be assessed in cryptocurrency ecosystems as well. In addition, I think the design of AML/CFT/CPF compliance in CBDCs and the multi-layered question of setting relevant cross-border standards inspires a broader discussion on the value of AML/CFT/CPF standardisation also when regulating cryptocurrency ecosystems. Hence, in this chapter I will: (a) provide foundational notions on CBDCs and account for key events in their evolution, to contextualise the magnitude of the phenomenon; (b) focus on the value of *interoperability* and the need for standardisation; (c) summarize core aspects of CBDC design choices; (d) evaluate the impact of public and private stakeholders; (e) investigate the link between AML/CFT/ CPF compliance in CBDCs and regulatory aspects of the use of cash (and its limitations), vis-à-vis *privacy* and data protection concerns; (f) explore the *privacy* and *transparency* dimensions of CBDCs, showing the role of trade-offs and the dynamics of balancing *confidentiality* and *auditability*; (g) elaborate on how features such as PETs impact on the issue at hand; and (h) show how they can be used as one of the benchmarks to evaluate specific models to create a preliminary taxonomy.

5.2. Overview on Central Bank Digital Currencies

Amid the globalisation of the economy, payment transmission systems have significantly evolved in the past decades. This is related to infrastructural advancements in the institutional domain – *e.g.*, real-time gross settlement (RTGS), fast retail and instant payments –, but also to the activity of the FinTech and Big Tech private sector.[726] Today, most efforts are pursued jointly, through mechanisms of public-private partnership (PPP). Within this context, the advent of DeFi, IoT and AI has driven even more rapid developments, and in the wake of the whitepapers of Bitcoin in 2008, Ethereum in 2013, and Libra/Diem in 2019,[727] central banks started entertaining the idea of creating a digital representation of sovereign money.[728]

The literature offers various definitions of "sovereign currency", that in broad terms is understood as one "set as such by a sovereign law, issued by an authorised issuer, and whose

[726] Carstens A (2021)
[727] Nakamoto S (2008). Buterin V (2013). Amsden Z, Arora R, Bano S, Baudet M, Blackshear S, et al (2019)
[728] Allen S, Capkun S, Eyal I et al (2020). Barotini C, Holden H (2019). Opare EA, Kim K (2020)

value results from a statutory rule".[729] Central banks and monetary authorities traditionally issue two types of "central bank money", both relevant to CBDC explorations:

i. *general purpose* or *fiat money*: the official and "sovereign" currency, also known as cash, consisting of coins and banknotes. It is legal tender – *i.e.*, it is legally recognised as a means to satisfactorily meet financial obligations –, and available to the general public;
ii. *bank reserves* or *settlements accounts*: provided exclusively to authorised institutions participating in RTGS systems (*e.g.*, commercial banks and non-bank PSPs), through the opening of reserves accounts.[730]

"Central bank money" is a liability of the relevant central bank. By contrast, most money in circulation is "commercial bank money" or "electronic money (e-money)". Because it is issued by private actors such as FIs – *e.g.*, commercial banks, non-bank PSPs and e-money institutions –, it essentially becomes a liability of private entities to the public. Because the end-user has a claim against an FI to redeem the value in "central bank money" – *i.e.*, cash – on demand, it extends "central bank money".[731]

5.2.1. CBDC typology

The first explorations into the digitisation of "central bank money" did not target ordinary public and private financial transactions (*i.e.*, fiat money, cash). Indeed, the initiatives were originally limited to "bank reserves" or "settlement accounts", hence to inter-banking activities. It was only at a later stage that institutions started to entertain the idea of issuing digital fiat money. Accordingly, at the present day there are two subsets of investigations into CBDC schemes, developed in a parallel fashion and responding to different payment needs:

i. *wholesale CBDC*: a settlement scheme between FIs, detached as a concept and also in practice from cash flows. Various designs and technologies have been explored by the public sector, often in partnership with private entities, with the goal to update or complement existing solutions for central bank deposits and improve the specifics of interinstitutional money transmission in terms of speed and security; and
ii. *retail CBDC*: a digital form of fiat money offered to the public as legal tender, for everyday use. It is the most transformative subset of CBDCs, mirroring an evolution towards

[729] ITU-T Focus Group on Digital Currency (2019)
[730] They are scriptural deposits recorded on a centralised ledger held, settled and managed by the central bank.
[731] Allen S, Capkun S, Eyal I et al (2020). For definitions and conceptual disambiguation: ITU-T Focus Group on Digital Currency (2019). BIS (2020). Brummer C (2019). Geva B (2018). Bossu W, Itatani M, Margulis C, et al (2020)

a more democratic monetary transmission channel. Retail CBDCs, to different extents depending on the specific design of the use case, expand the concept of "central bank money" and require central banks to safeguard stability, efficiency and security when devising issuance and distribution mechanisms.

The CBDC concept draws from many disciplines such as economics, technology, law, finance, sociology, which challenges the pursuit of comprehensive definitions. A *retail CBDC* can be defined as "a credit-based currency in terms of value, a cryptocurrency from a technical perspective, an algorithm-based currency in terms of implementation, and a smart currency in application scenarios".[732] Ostensibly, "CBDC is not a well-defined term. It is used to refer to a number of concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value".[733]

Indeed, CBDCs are all but a unitary concept, and feature a complex nature also in terms of architecture and use cases. Likewise, over the past decade central banks, governments and monetary authorities have motivated their research endeavours and a possible issuance in various ways, as well as they linked the growing interest in CBDCs to many drivers.[734] Nonetheless, there are a few core factors that seem to have played a key role in sparking this interest. First, the use of cash has been decreasing, in favour of digital alternatives such as debit and credit card transactions and wire/electronic fund transfers.[735] Secondly, impacts were exerted by many private altcoins and tokenisation initiatives following Bitcoin and Ethereum, up to the complex automated cost-effective and globally reaching financial instruments dubbed DeFi.[736] Attempts to limit their volatility, which limits usability as money, led to the development of stablecoins and mega-stablecoins.[737] Thirdly, the development of digital money outside legacy networks challenges traditional payment and monetary policy mechanisms, due to the risk of currency substitution and its geopolitical impact.[738] In this sense, the investigation of tokenised fiat money pursues financial stability. Meanwhile, CBDC interest mirrors the effort to leverage the programmability of digital cash technologies into a new functional form of money to serve

[732] Yao Q (2018)
[733] BIS (2018)
[734] Adrian T, Mancini-Griffoli T (2019). Allen JG, Rauchs M, Blandin A, Bear K (2020). CBDC policy goals include mitigating currency substitution, fostering safety, resilience, efficiency and competitiveness of payment systems, financial inclusion, continuous access to central bank money. World Economic Forum (2021a), p 23. World Economic Forum (2021d), p 200
[735] In some jurisdictions, like Sweden or Canada, the decline in the use of cash has been reportedly stark.
[736] Amler H, Eckey L, Faust S, Kaiser M, Sandner P, Schlosser B (2021)
[737] Amsden Z, Arora R, Bano S, Baudet M, Blackshear S, Bothra A, Cabrera G (2019) f
[738] Barotini C, Holden H (2019). BIS (2021). Golubova A (2021)

a growing global economy, to shape a new interplay between citizens and monetary instruments.[739] Finally, CBDCs are investigated to provide payment efficiency, new monetary policy transmission channels, financial inclusion, safety/privacy, regulatory compliance.[740]

5.2.2. History of CBDC projects

Although central bank interest in digital money started emerging in 2014, most retail CBDC initiatives gained notoriety about five years later. As of today, central banks and governments explore plans to issue digital sovereign currencies, and multi-stakeholder commentaries touch upon diverse aspects such as security, privacy, technology infrastructure, regulation, and cross-border challenges.[741] The first pilots in wholesale CBDCs, DLT-based settlement and cross-border transfers, emerged in 2015-2016 – *e.g.*, Bank of Canada (Project Jasper),[742] Bank of England (RSCoin),[743] Monetary Authority of Singapore (Project Ubin), ECB and Bank of Japan (Project Stella), Deutsche Bundesbank (Project Blockbaster), Banque de France (Project Madre), Banco Central do Brasil (Project Salt). While the Monetary Authority of Hong Kong (Project LionRock) was still addressing interbank settlements, retail projects started to explore the relation between digital fiat money and cash – *e.g.*, Sveriges Riksbank (e-Krona Project). The 2017-2018 pilot initiatives are both retail – *e.g.*, central banks of Finland (Project e-hryvnia), Turkey (Digital Turkish Lira), Ukraine, Cambodia (Project Bakong), Uruguay (Project e-Peso), Israel (Project e-Shekel), Venezuela (Project Petro), the Marshall Islands – and wholesale – *e.g.*, Denmark, South Africa (Project Khokha), Switzerland (Project Helvetia), New Zealand, Norway, Thailand (Project Inthanon) – and unveil CBDC concepts often diverse.[744]

In early 2019 around 70% of central banks declared to be engaging in CBDC-related activities.[745] Although only 30% voiced plans to issue within the medium term, in 2019 CBDC

[739] Rennie E, Steele S (2021)
[740] Allen S, Capkun S, Eyal I et al (2020). Barotini C, Holden H (2019). Opare EA, Kim K (2020). Auer R, Banka H, Boakye-Adjei NY, Faragallah A, Frost J, Natarajan H, Prenio J (2022)
[741] Adrian T, Mancini-Griffoli T (2019). Allen JG, Rauchs M, Blandin A, Bear K (2020). Auer R, Cornelli G, Frost J (2020). Sandner P, Gross J, Grale L, Schulden P (2020). European Central Bank (2020b). BIS (2018). Khiaonarong T, Humphrey D (2019)
[742] The Jasper project is representative of sandboxing initiatives and had different phases: (i) in 2016 the Bank of Canada experimented with an Ethereum-based RTGS system; (ii) in 2017 it repeated the sandboxing with additional liquidity requirements for settlement, moving to the permissioned Corda; (iii) in 2018 it partnered with commercial banks to extend the functionality of the system. The new system also allowed the settlement of stock trades from the Toronto Stock Exchange; (iv) in 2018-19 the bank partnered with the Monetary Authority of Singapore – that had just completed three phases of Project Ubin – to experiment on a cross-border, -currency, and -platform payment system. One bank used Corda and the other Quorum, to test interoperability.
[743] Danezis G, Meiklejohn S (2016)
[744] Auer R, Cornelli G, Frost J (2020)
[745] Barotini C, Holden H (2019)

research reached the headlines. A key moment was Facebook's Libra announcement in June 2019. The project, rebranded to Diem in 2020 and abandoned in 2022, was to be deployed on a permissioned DLT run by the "Libra/Diem Association" of corporate and non-profit organisations.[746] Meanwhile, the ECB started to explore the implications of cryptoassets on monetary policy, and in October 2020 a report was issued on principles and configurations for a possible Digital Euro.[747] After reports were published by the Bank of Korea and the Bank of Japan, the first cross-border settlement mechanism between DLT platforms was concluded by Bank of Canada and Monetary Authority of Singapore within Project Jasper/Ubin.

At the beginning of 2020, central banks working on CBDCs had risen to 80%, nearly half of them at PoC phase and a few pilots.[748] In July 2020 the Bank of Lithuania issued the first state-backed digital collector coin, LBCOIN, which can be transferred P2P. In the U.S., which had been remarkably silent on CBDCs, in May 2020 the non-profit Digital Dollar Project released a whitepaper on the reasons for a digital USD, while the Federal Reserve Bank of Boston announced a collaboration with MIT's Media Lab on a Digital Dollar. In October 2020 the first CBDC, the Sand Dollar, was launched by the Central Bank of the Bahamas. Meanwhile, the Eastern Caribbean Central Bank launched DXCDCaribe, Brazil launched the PIX instant-payment platform, the Bank of Russia unveiled interest in a Digital Ruble, and the Reserve Bank of Australia started considering a wholesale CBDC system labelled eAUD.

At the beginning of 2021, 86% of central banks were exploring CBDCs: 60% at the stage of doing advanced experiments and 14% at a pilot phase.[749] In January, the EC and the ECB announced a cooperation on a Digital Euro and launched the project in July,[750] while in February the e-Krona Project was extended.[751] Meanwhile, e-CNY's testing was widened, and launch was announced by early 2022. Retail initiatives were reportedly initiated in New Zealand, Vietnam, Kazakhstan (Digital Tenge) Madagascar (e-Ariary), Nigeria (e-Naira), Honduras, Guatemala (iQuetzal), Bhutan (Digital Ngultrum), Laos, Peru, Philippines, Palau, Brazil (Digital Real), Tanzania, Mexico, Namibia, Zimbabwe, Singapore (Project Orchid).[752] Concurrently, the Bank of Canada unveiled and scrutinised three academic proposals,[753] and in May the Bank of Korea issued its own competition for CBDC PoCs.

[746] Amsden Z, Arora R, Bano S, Baudet M, Blackshear S, Bothra A, Cabrera G (2019)
[747] ECB Crypto-Assets Task Force (2019). European Central Bank (2020a)
[748] Boar C, Holden H, Wadsworth A (2020)
[749] Codruta B, Wehrli A (2021)
[750] European Central Bank (2021a). European Central Bank (2021b)
[751] Sveriges Riksbank (2021)
[752] CBDC Tracker (2022)
[753] One among them: Veneris A, Park A, Long F, Puri P (2021)

This era also shows the maturation of mCBDCs projects on the cross-border behaviour of local systems – *e.g.*, the 2019-20 Project Aber by the Saudi Arabian Monetary Authority and Central Bank of UAE, and Project Inthanon-LionRock by the Hong Kong Monetary Authority and the Bank of Thailand. In February 2021 a major mCBDC collaboration was announced by the Monetary Authority of Hong Kong, Central Bank of UAE, Bank of Thailand and the People's Bank of China, while other projects address the issue of cross-border CBDC schemes, such as Projects Dunbar and Jura.[754] In December 2021, the Reserve Bank of Australia announced the end of Project Atom on a wholesale CBDC.[755]

The trend continued in 2022: wholesale CBDC research was disclosed in Denmark and retail initiatives in Jordan, Iraq, Nepal, Oman, Qatar, Saudi Arabia, Uganda, Yemen, Zambia, Rwanda, Taiwan, Trinidad and Tobago, Sudan, Malaysia, Iran (Crypto-Rial). In January the Federal Reserve published a paper to initiate public discussion about a U.S. CBDC,[756] and later the Federal Reserve Bank of Atlanta disclosed its Project Hamilton, while the BIS and the Federal Reserve Bank of New York announced the New York Innovation Center as a strategic partnership to investigate a wholesale CBDC model.[757] Meanwhile, the Bank of Korea completed a first phase of testing and the Bank of Russia concluded a pilot.[758] In January 2022, 76% of Arab central banks were reportedly researching CBDCs, among which two central banks are expected to issue a CBDC within three years.[759] In March, the BIS concluded the mCBDC Project Dunbar,[760] explicitly drawing interoperability and competition best practices from the Pix project.[761] In October 2022, the BIS Innovation Hub Hong Kong Centre published the outcomes of the collaboration with the Hong Kong Monetary Authority and the Hong Kong Applied Science and Technology Research Institute, presenting a prototype developed within Project Aurum focusing on a combination between a wholesale and a retail CBDC model.[762] Towards the end of 2022, the ECB reported on the progress of the Digital Euro investigation.[763]

---

[754] Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021). BIS Innovation Hub Hong Kong Centre, HKMA, Bank of Thailand, Digital Currency Institute PBoC, Central Bank UAE (2021)
[755] Project Atom (2021). It explored a CBDC for funding, settlement, repayment of a tokenised syndicated loan. A "syndicated loan" is a loan that is offered by a group of lenders (the "syndicate", composed of FIs and institutional investors) to a single borrower (usually a corporation, projects requiring a loan too large for a single lender). Spreading out the loan mitigates risk if the borrower defaults.
[756] Board of Governors of the Federal Reserve System (2022)
[757] CBDC Tracker (2022)
[758] Ibid
[759] Arab Monetary Fund (2022). *Arab central banks* are those of Jordan, UAE, Bahrain, Tunisia, Algeria, Djibouti, Saudi Arabia, Sudan, Syria, Somalia, Iraq, Oman, Palestine, Qatar, Comoros, Kuwait, Lebanon, Libya, Egypt, Morocco, Mauritania, Yemen
[760] With Corda-based and Quorum-based prototypes. BIS (2022)
[761] Duarte A, Frost J, Gambacorta L, Koo Wilkens P, Song Shin H (2022)
[762] BIS Innovation Hub Hong Kong Centre, HKMA (2022)
[763] European Central Bank (2022a). European Central Bank (2022b)

5.2.3. Cross-border perspectives and standardisation

CBDCs are often examined as stand-alone sovereign projects, and especially the analysis of retail CBDCs often targets domestic projects or comparisons. However, cross-border implications of tokenised "central bank money" generate important questions. Starting from 2021, the BIS has explored the interactions between CBDC systems, both retail and wholesale,[764] sparking interest in academia as well.[765] In this context, "cross-border CBDC, or multi-CBDC, is a term that describes one or more systems that automatically handle cross-border payments between domestic CBDCs".[766] These schemes reportedly improve efficiency and allow FIs to hold foreign CBDCs directly, thus reducing both latency and fees charged to end-users.[767]

Among the manifold technical, organisational, governance and legal open questions generated by multi-CBDC designs, two concepts emerge as foundational for any further discussion on cross-border CBDC schemes: *interoperability* and *standardisation*. The DLT space increasingly discusses *interoperability*,[768] which in cross-border CBDCs comes into play in three ways: (a) cross-currency capabilities between (supra)national systems; (b) if CBDC schemes are developed in public-private cooperation users of various providers can transact with each other only if *interoperability* is guaranteed by design; (c) a cross-border CBDC should be interoperable with domestic payment schemes. *Interoperability*, however, relies on standardisation, which consists of developing industry-wide technical, regulatory, and supervisory standards – possibly within schemes of international cooperation, as addressed in Chapters 4 and 6. From the CBDC perspective, the value of standards was highlighted with regard to message formats, cryptographic techniques, data requirements, user interfaces, KYC, transaction monitoring.[769] Indeed, both technical and regulatory standards are necessary to *interoperability* at different levels – *e.g.*, messaging, privacy, AML/CFT/CPF, *identity*, DLT protocols.[770]

Against this backdrop, there are three methods to set up a cross-border and cross-currency CBDC, with different consequences: (i) developing compatible standards, (ii) interlinking

[764] Auer R, Haene P, Holden H (2021). Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021). On cross-border CBDC research initiatives: Fanti G, Pocher N (2022)
[765] Kochergin D, Dostov V (2020). Jung H, Jeong D (2021), p 133.
[766] Fanti G, Pocher N (2022), p 5
[767] Ibid, p 5
[768] *i.e.*, broadly speaking, the features of systems that can aid data exchange. Auer R, Haene P, Holden H (2021)
[769] Reportedly, "common technical standards, such as message formats, cryptographic techniques, data requirements and user interfaces can reduce the operational burden of participating in multiple systems. Aligned legal, regulatory and supervisory standards can simplify know-your-customer and transaction monitoring processes" (Ibid)
[770] World Economic Forum (2021c), p 187

different systems, (iii) creating a single multi-currency system. Among these options, only the last case leads to an integrated "payment system", comprising a single set of participants, a single infrastructure, a single ledger, a single rulebook and a single governance. In the other cases, *interoperability* relies on "payment arrangements".[771] The choice among different options exerts significant impacts on the resulting *privacy-transparency* trade-off of the given model.[772] This, in turn, requires careful planning and extensive techno-regulatory reflections.[773]

The setup of an mCBDC would deliver on the promise of improving payment efficiency, while the alternatives are fostering communication between sovereign schemes or witnessing the creation of a global private stablecoin.[774] Indeed, along with the efforts to digitise fiat money, one cannot ignore the activity of private players and its geopolitical impact. In early 2020, Facebook/Meta renamed its Libra effort to Diem, and unsuccessfully pursued a Swiss licence. In April 2021 the focus was limited to the U.S. as a stablecoin backed 1:1 with assets to the US dollar, and in January 2022 the Diem Association sold its assets to Silvergate.[775] The role played by Diem's regulatory hurdles in abandoning the project clearly emerge from the sale announcement, where after underlining the priority conceded to controls against illicit misuse (such as prohibition of *anonymous* transactions) it was reported how the dialogue with federal regulators had made it clear the project could not move ahead.[776]

Meanwhile, the e-CNY's launch and mCBDC cross-border partnerships are prospectively able to influence not only global payment systems and currencies, but also standardisation itself. Reportedly, while no other major central bank has announced a CBDC launch, in October 2021 there were about 123 million individual and 9.2 million business e-CNY wallets.[777] Hence, China may strengthen its leadership in e-payments and shape digital finance's standards in ways that threaten *transparency* and *accountability*.[778] Experts urge the U.S. to boost

[771] Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021). For details on pros and cons of these strategies: Auer R, Haene P, Holden H (2021). Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021). In this context, the BIS urged the inclusion of cross-border considerations in CBDC projects, and in its role of "central bank to the world's central banks" it is expected to lead *standardisation* through its CPMI working group and Innovation Hubs. Duffie D (2020). Auer R, Haene P, Holden H (2021). Golubova A (2021). PYMNTS (2020). BIS (2021)

[772] For an analysis of how *privacy* and *transparency* properties depend substantially on each specific technical design of the cross-border CBDC: Fanti G, Pocher N (2022), pp 11-16

[773] For an overview on the interplay between regulation and technology in mCBDC projects: Ibid, pp 17-20

[774] Auer R, Haene P, Holden H (2021). Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021) m

[775] Diem (2022) Bloomberg (2022) Diem (2021) Diem had established a parternship with Silvergate in May 2021, whereby Silvergate had become the exclusive issuer of the Diem USD Stablecoin.

[776] Diem (2021)

[777] Soderberg G, Bechara M, Bossu W et al (2022), p 2

[778] This is because, even if the e-CNY can translate into a significant advantage for China's economy in terms of efficiency and financial inclusion, in the absence of adequate oversight "in the hands of a state that has already deployed a massive network of cameras and biometric detectors to monitor its people and store data on their political, social, and digital behaviour, the addition of comprehensive information on payments could represent a staggering enhancement of authoritarian control". Duffie D, Economy E (2022), pp xi-xii

governmental CBDC activity, while the U.S. Federal Reserve is only at the early stages of assessing whether to adopt a CBDC and declared in January 2022 to be waiting for support from the executive branch.[779] While the report's authors do not advocate for an immediate creation of a "digital dollar", they stress the importance of developing technology and standards due to the time it will take to develop a design that balances "privacy, security, accessibility, efficiency, and transparency". Should the U.S. choose a monetary digitalisation grounded on private sector solutions (*e.g.*, stablecoins), it would still take time to draw up proper regulation and deploy the infrastructure.[780] In March 2022 the U.S. President issued an executive order,[781] which mandates urgent CBDC exploration by the Government and the Federal Reserve.

5.3. The Impacts of CBDC Design Choices

Because retail CBDCs are to be offered to millions of people, they need to be equipped with different layers of safeguards. Reportedly, they should embody five core characteristics: (i) trade-off between *privacy* and data protection and compliance with other regulations such as AML/CFT/CPF; (ii) universal and unrestricted accessibility; (iii) resilience, continuous operation online and offline; (iv) security; (v) high performance, scalability for daily and cross-border use.[782] CBDCs should guarantee accessibility irrespective of financial means, dexterity, or impairments, to ensure financial inclusion, and should be usable everywhere, even without Internet access and by travellers. Although *user* and *transaction privacy* should be protected, compliance must be ensured with AML/CFT/CPF standards. Further, they should be compatible with banking and retail payment systems, so that users can access their funds from commercial bank accounts, and merchants can accept CBDCs as a means of payment. Finally, they should provide seigniorage income to central banks but also foster competition in the payments market.[783] Although CBDCs are proposed as a solution to a wide range of policy challenges, no system can address in the best way all these goals, which means stakeholders are called to define their individual high-level priorities and objectives and, accordingly, their designs. In this context, some policy options are crucial – *e.g.*, the approach to *privacy* and individual rights, roles and responsibilities of the public and private sector – and translate into three key

[779] Board of Governors of the Federal Reserve System (2022)
[780] Duffie D, Economy E (2022), p xii. World Economic Forum (2021a), p 21
[781] US Presidential Actions (2022)
[782] Pocher N, Veneris A (2022a). Veneris A, Park A, Long F, Puri P (2021)
[783] Pocher N, Veneris A (2022a). Veneris A, Park A, Long F, Puri P (2021). "Seignorage income" is the interest a central bank earns on the money it lends or the return it receives on acquired assets.

trade-offs often falling along a spectrum: (i) *anonymity* vs. centralised identity-based services, (ii) self-reliance vs. reliance on distributors, (ii) centralised vs. distributed control.[784]

5.3.1. Core architectural options

Traditionally, payment systems are token-based or account-based, which mirrors how access is granted to end-users and the *authentication/identification* method to conduct a transaction.[785] CBDC architectures can deploy different types of wallets and their design can include more than one type of wallet. As with other digital wallets, they serve the function of *authenticating* the user and are the interface for performing transactions, storing private and public keys used to sign them.[786] On the one hand, access to a token-based means of payment relies on the validity of the traded object. In principle, it is an *anonymous* and bearer instrument grounded on cryptographic principles, while in an account-based CBDC access depends on the *identification* and *identity verification* of the account holder, reminiscent of traditional accounts requiring KYC.[787] Hence, in an account-based CBDCs the system comprises a ledger and a payment service, which refers to how payments are initiated, verified, cleared, and settled.[788]

The core architecture and distribution method of a CBDC can be designed in various ways. The different models can be classified accordingly and may involve public and private actors.[789] Chiefly, they can be: (i) *one-layered*: the system is under sole management of the central bank (*e.g.*, distribution, KYC, settlement); or (ii) *two-layered*: when FIs (*e.g.*, commercial banks, PSPs) act as intermediaries for end-users.

As shown in Figure 6 below, CBDC architectures can be "direct", "hybrid", or "indirect/synthetic". The direct structure is described as *one-tier* or *unilateral*,[790] as only the central bank is involved (*e.g.*, it holds the CBDC ledger, it handles user relationships) and the CBDC

[784] Oliver Wayman Forum (2022) , p 12
[785] Bossu W, Itatani M, Margulis C, et al (2020). Auer R, Böhme R (2020)
[786] As explored in Chapter 3, wallets can be custodial or non-custodial. If the wallet is custodial in a token-based system the custodian holds the private keys to sign a transaction, while in case of identity-based access it holds the link between *identity* and CBDC account necessary for authentication. If the wallet is non-custodial in a token-based system users manage their own private keys, while in the case of identity-based access they must be able to prove ownership independently of any distributor – *e.g.*, through a national ID system. Oliver Wayman Forum (2022), p 33
[787] Allen S, Capkun S, Eyal I et al (2020). Fanusie YJ (2020). Kochergin D, Dostov V (2020). In other words, "in an account-based CBDC, ownership is tied to an identity, and transactions are authorised via identification. In a CBDC based on digital tokens, claims are honoured based solely on demonstrated knowledge, such as a digital signature" (Carstens A (2021), p 17)
[788] BIS (2018). Viñuela C, Sapena J, Wandosell G (2020). Group of 30 (2020). The impact of account-based and token-based systems on the integration between CBDC architectures and IoT was addressed in Pocher N, Zichichi M (2022)
[789] Adrian T, Mancini-Griffoli T (2019). Auer R, Böhme R (2020). Viñuela C, Sapena J, Wandosell G (2020)
[790] Soderberg G, Bechara M, Bossu W et al (2022), p 8

is a direct claim of the public. On the contrary, "hybrid" and "indirect/synthetic" CBDCs are *two-tier*, resembling traditional mechanisms.[791] In the "hybrid" model, the central bank holds the CBDC ledger, but payment services are provided by private actors. A part of the literature provides for a further distinction: if the central bank keeps the full CBDC ledger, the model is "hybrid", while if it keeps only the wholesale ledger, the design is labelled "intermediated". Nonetheless, both in the "hybrid" and "intermediated" models the CBDC remains a direct claim on the central bank, even if transactions are managed by private actors.[792] In "synthetic" CBDCs the private sector handles transactions and updates the ledger, held indirectly by the central bank by settling reserve accounts.[793] In this case, the CBDC is not a liability of the central bank, but of the issuing commercial bank or other PSP.

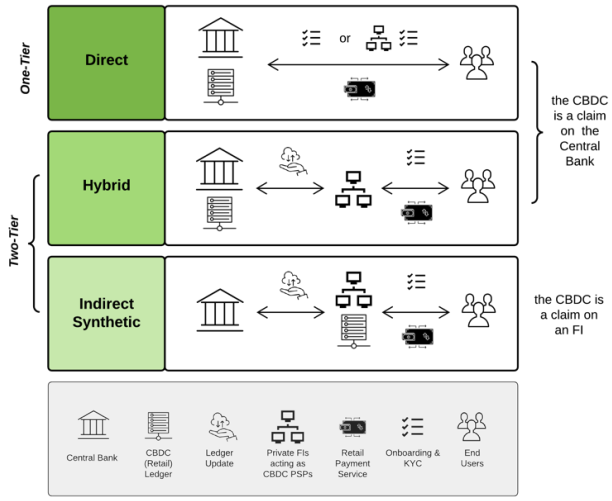

Figure 6: retail CBDC architectures. From: Pocher N, Veneris A (2022a)

Most ongoing projects adopt a hybrid model, where the central bank issues CBDCs to banks and PSPs, and they distribute them to users providing account-related services.[794] By contrast, in synthetic schemes the CBDC is a stablecoin offered by a private actor and backed by its reserve account with the central bank, which means private intermediaries bear a responsibility to cover the relevant liability.[795] When end-users do not possess a direct claim on the central bank, some authors argue the instrument cannot be defined as a CBDC. Indeed, the nature of a

[791] Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021). Auer R, Böhme R (2020). Carstens A (2021), p 17
[792] BIS Innovation Hub Hong Kong Centre, HKMA (2022), p 4. Auer R, Böhme R (2021)
[793] Adrian T, Mancini-Griffoli T (2019). In these cases, FIs hold reserve accounts with the central bank.
[794] Duffie D, Economy E (2022), p 10
[795] Bossu W, Itatani M, Margulis C, et al (2020). Kriwoluzky A, Kim CH (2019). Group of 30 (2020). Bossone B (2020), p 38. Reportedly, this resembles special-purpose licences granted to non-bank FinTech firms in jurisdictions such as India, Hong Kong, China, and Switzerland (Adrian T, Mancini-Griffoli T (2019)).

synthetic CBDC can vouch against its qualification as a CBDC, that is assumed to be a direct liability of the central bank.[796] Nonetheless, other experts argue that if the stablecoin is pegged 1:1 to the sovereign currency by means of regulation, it is ostensibly as if users are holding central bank money, which is the essence of a CBDC.[797]

From this perspective, a valuable addition to the discussion on CBDC designs is that of Project Aurum and its prototype that envisions the issuance of two types of tokens within a two-tier CBDC system. In particular, the model foresees a wholesale (interbank) CBDC system where a wholesale CBDC is issued to FIs, to be then distributed by FIs in a retail system through by a dedicated CBDC e-wallet system. From the retail perspective, end-users are offered two different types of tokens: (a) "intermediated" CBDC or CBDC-token, a liability of the central bank, and (b) CBDC-backed stablecoins, issued by FIs.[798]

5.3.2. Offline use

CBDCs need to be used even when there is (temporarily) no access to the Internet: offline payments are crucial for a system's resilience in crisis situations, but also in locations with unstable telecommunication systems to boost financial inclusion.[799] Facilitating offline transactions results in a trade-off between hardware/software security, costs, and convenience, and raises new regulatory challenges. Although specifics on the implementation of offline transactions fall outside the scope of this work and are overviewed in the literature,[800] their AML/CFT/CPF impact warrants a few remarks. Reportedly, offline transactions can be implemented via tamper-proof hardware.[801] Many processor chips, including smartphones', have Trusted Execution Environment capability,[802] and can be leveraged for hardware/software enclaves to store a small amount of CBDCs for daily transactions (*e.g.*, supermarket, restaurant, gasoline). Another approach is to issue debit-like cards, pre-loaded with a number of CBDCs from the user's wallet held on a smart device (*e.g.*, smartphone, tablet, computer). The cards can be programmed with near-field or range-controlled communication and when activated by a nearby radio-frequency signal (*e.g.*, a merchant's terminal) they can transmit offline the

[796] Bossu W, Itatani M, Margulis C, et al (2020)
[797] Kriwoluzky A, Kim CH (2019). Soderberg G, Bechara M, Bossu W et al (2022), p 8
[798] BIS Innovation Hub Hong Kong Centre, HKMA (2022), pp 3 and 18
[799] Soderberg G, Bechara M, Bossu W et al (2022), p 13
[800] Auer R, Böhme R (2021). World Economic Forum (2021d). Veneris A, Park A, Long F, Puri P (2021)
[801] Allen S, Capkun S, Eyal I et al (2020). Veneris A, Park A, Long F, Puri P (2021). Gang X, MU of Science Technology (2019)
[802] *E.g.*, SGX in Intel, TrustZone in ARM, KNOX in Samsung. In broad terms, a TEE is an isolated secure area of a main processor that provides for enhanced confidentiality and security for trusted applications running on a device.

required amount, as credit/debit cards. These cards must be synched with an online wallet to deposit/withdraw funds, and stored amounts and transaction frequency can be limited to mitigate risks, as explored below.[803] All novel hardware designs call for global CBDC hardware/software *interoperability* standards.

5.3.3. The public-private interplay and public-private partnerships

Different CBDC designs lead to diverging public-private monetary policy dynamics. The topic relates to a broader discussion on the preferable degree of competition between public (central banks, governments) and private (*e.g.*, commercial banks, FIs, corporations) actors in digital currencies. In the CBDCs context, the main controversy is whether society can best reap this opportunity if central banks replace private FIs/FinTech firms or joins forces with them.[804] The first policy option is mirrored by *direct one-layered* CBDCs, while it is more complex in *two-layered* approaches, that assume the central bank is willing to waive a portion of power.[805] *Two-layered* CBDCs, however, vary in terms of boundaries of the involvement of private actors in the value chain.[806] The collaboration between central banks and distributors does not translate into a binary decision, and a range of options sees control distributed at different degrees.[807] Most importantly, in hybrid structures central banks still hold the CBDC ledger and manage end-users accounts, while in both hybrid and synthetic cases payment services, relationships with end-users, and AML/CFT/CPF processes are managed by the private sector.

The idea of outsourcing CBDC activities to private actors has generated academic and political debate.[808] In PPPs, public sector's goals meet profit objectives of the private industry,[809] while public authorities benefit from private sector's expertise and flexibility.[810] In the CBDC arena, the main question is how to guarantee innovation, efficiency, fair competition and financial inclusion against monetary and financial stability risks, that are traditional objectives guaranteed by central banks themselves.[811] In a nutshell, PPPs seek to preserve comparative

[803] Veneris A, Park A, Long F, Puri P (2021). World Economic Forum (2021d)
[804] Kriwoluzky A, Kim CH (2019). Group of 30 (2020). Nabilou H (2019). Brunnermeier MK, Niepelt D (2019)
[805] Jagati S (2020)
[806] Adrian T (2020)
[807] Oliver Wayman Forum (2022) , p 23. Soderberg G, Bechara M, Bossu W et al (2022), p 9
[808] Although conflicting definitions of PPPs exist today, in general terms they are arrangements "between government and the private sector in which partially or traditionally public activities are performed by the private sector". Savas ES (2000), p 4. Similarly, see Bexell M, Moerth U (2010), p 6. Bevir M (2009), p 85
[809] Vutsova A, Ignatova O (2014), p 85; Ross TW, Yan J (2015), p 449
[810] Linder S (1999)
[811] Group of 30 (2020). Auer R, Banka H, Boakye-Adjei NY, Faragallah A, Frost J, Natarajan H, Prenio J (2022)

advantages: private actors interact with end-users, develop interface designs and innovate, while public institutions regulate, supervise and supply trust. Public-private scenarios may stimulate competition, foster innovation and inclusion, while reducing risks and costs for central banks. By contrast, they may pose financial stability and liquidity risks in case of synthetic CBDCs if the responsibility to maintain adequate asset backing rests on private actors.[812] Further issues are raised by collection, use and dissemination of the data and metadata of user payments. Additionally, CBDC private stakeholders may have different incentives than public entities and be in a different market position than ordinary private actors in PPPs, since FinTech companies already provide substantial hardware to central banks.[813] For instance, they may pursue profit maximisation at the cost of abusing of information advantage, or concealing operational weaknesses, and the consequent loss of trust would generate instability.[814]

Hence, foreseeably central banks would need either to manage complex infrastructures or set up advanced supervision schemes.[815] Establishing and taking part in a new retail payment model requires skills that are far from traditional for central banks, also in terms of technical expertise vis-à-vis the impacts of possible failures on the economy and financial stability. Reportedly, this remains true in all possible involvement scenarios of the central bank, be it as scheme leader, coordinator, participant, or supervisor, depending on the CBDC design. Although some concerns may be mitigated by partnering with FinTech firms, managing vendors and partners also requires new abilities. Alternatively, the private sector can be involved by adopting a hybrid model where distributors operate part of the system.[816]

5.4. AML/CFT/CPF Considerations in the CBDC Domain

When CBDCs started to emerge, it was clear their innovative techno-legal character was accompanied by a certain degree of traditionality in terms of the type of stakeholders involved – *i.e.*, central banks and regulated or regulatable intermediaries such as FIs and PSPs. From this perspective, CBDC issues are channelled into a familiar structure of regulated environments. Nonetheless, CBDCs bring about a few outstanding dilemmas, deeply influenced by the specific chosen design – *i.e.*, (i) wholesale vs. retail, (ii) *one-tier* vs. *two-tier*, (iii) centralised

[812] BIS (2021). Carstens A (2021), p 17. Kriwoluzky A, Kim CH (2019). Group of 30 (2020). Nabilou H (2019). Jagati S (2020). Ojo M (2021). Auer R, Böhme R (2020)
[813] Jagati S (2020)
[814] Kriwoluzky A, Kim CH (2019), p 13
[815] Auer R, Böhme R (2020).
[816] Oliver Wayman Forum (2022), pp 14-15

vs. decentralised, and (iv) account-based vs. token-based. A selection of these regulatory conundrums is addressed in this chapter, albeit with no attempt to offer a comprehensive account. Naturally, CBDCs raise many other issues, most of which belong to areas traditionally less harmonised across jurisdictions than the ones addressed – *e.g.*, private and property law, contract law, tax law, insolvency law, private international law.[817]

As a preliminary issue, given the CBDC-hype, it is interesting that almost no jurisdiction would currently allow their issuance without amending domestic laws. A 2020 IMF study highlighted how CBDC issuance poses several risks for the central banking community, burdening it with legal, financial, and reputational questions.[818] Two public law domains, "central bank law" and "monetary law", are crucial to warrant CBDCs a sound legal basis, and experts concluded that while the first one could be addressed through reforms, the latter poses structural policy challenges of less straightforward solution. First, if a CBDC is to be a liability of the central bank (*i.e.*, direct, hybrid and intermediated forms) its issuance must be regulated by "central bank laws".[819] This is necessary to warrant the CBDC a legal basis in compliance with the principle of attribution of powers and central bank mandate. Likewise, the qualification of a CBDC as "currency" must be regulated under "monetary law": if it is to be used as a means of payment to extinguish monetary obligations, "monetary law" must treat is as such.[820] Overall, it was argued the legal treatment in both fields will largely depend on the technical and operational design, and reforms are required to ensure the soundness of the framework. Notably, controversies arise as to the lack of legal basis to issue token-based instruments, and account-based CBDCs to the public. Both aspects would require relevant amendments.[821]

Although their AML/CFT/CPF aspects are discussed extensively, CBDCs are not treated as cryptocurrencies, but as fiat currency.[822] Several studies outline how different architectures may lead to various AML/CFT/CFP repercussions, where key questions concern the allocation of compliance duties, account management, identity/transaction checks. The relevance of CBDC-related AML/CFT/CPF discussions in this work emerges by the ongoing development of a new sensitivity to the interplay between technology, regulation, and technical standardisation. Indeed, in line with what was suggested in Chapter 4 and is explored in Chapter 6, CBCD

[817] Bossu W, Itatani M, Margulis C, et al (2020). Brummer C (2019)
[818] Bossu W, Itatani M, Margulis C, et al (2020)
[819] "Central banks laws" establish central banks, their decision-making bodies, autonomy, and their mandate: actions beyond it generate challenges vis-à-vis administrative law principles of "attribution" and "specialty". Ibid, p 13
[820] "Monetary law" lays out the legal foundation for the socio-economic use of monetary value. The basic principle is that it is up to a sovereign State to establish its own currency system. Ibid, p 27
[821] Ibid
[822] Allen JG, Rauchs M, Blandin A, Bear K (2020)

or stablecoin *interoperability* requires AML/CFT/CPF technical standards, whose development is currently hindered because the framework has not been yet "collated into a standardised data format to allow for automation". Interestingly, it was suggested that a given government or organisation establishes a (centralised) database to provide regulated entities in the digital currency space with transaction- or customer-related risk scores on illicit activity.[823]

5.4.1. CBDCs and limits to the flow of cash

Even if Bitcoin is acknowledged as a *pseudonymous* means of payment, the previous chapters outlined how altcoins have increasingly evolved toward higher levels of cryptographic complexities. Accordingly, the FATF voiced growing concerns in terms of *virtual-to-virtual layering*,[824] while tech advancements in privacy coins and pervasive *obfuscation* mechanisms were complemented by the advent of DEXes, unhosted wallets and cross-chain atomic swaps.[825] In this context, the FATF identified examples of *anonymity* as "red flag indicators" of suspicious activities in the IoM sphere.[826] As explored in Chapter 2, controversies on *anonymity* in financial transactions well preceded the IoM. Not only the debate on e-cash dates to the '90s,[827] but the core issue originated with regard to physical cash. Indeed, cash is reportedly one of the preferred means of transfer for ML/TF/PF purposes, and in Europe most STRs concern its use or its smuggling.[828] Even if cash is still the favourite means of payment also for the legal economy, it was estimated only one-third (at most) of circulating cash serves legitimate purposes, and several analyses correlate cash diffusion and illicit activities.[829]

While it falls beyond the scope of this work to assess the opinions on the role of cash in criminal activities, its attractiveness lies in *anonymity* and lack of *traceability*. Although *identification* can take place upon deposit, a bearer instrument carries no origin or beneficiary information *per se*. Meanwhile, "cash intensive businesses" – *i.e.*, operating mainly on cash and whose assets are mostly cash or liquid, such as restaurants, retail shops and supermarkets – are crucial to launder illicit proceeds and were identified as the preferred choice for criminal groups to infiltrate the legal economy.[830] Because the trait of *anonymity* is inherent to this means of

[823] World Economic Forum (2021c), p 187
[824] Financial Action Task Force (2021e)
[825] Pocher N (2021b). Pocher N (2021a)
[826] Financial Action Task Force (2020d)
[827] Chaum DL (1983). Chaum D, Grothoff C, Moser T (2021). Magnuson W (2020)
[828] Riccardi M, Levi M (2018), p 135
[829] Ibid, pp 139-141
[830] This business type makes it easier to justify as legitimate extra illicit proceeds and enables the deposit of large amounts of cash as earnings for "placement" purposes. Ibid, pp 136 and 145

payment – one of the purest examples of a fungible asset – the fight against financial crime has long faced the *anonymity problem* and addressed it by leveraging *identification* and *traceability*. Indeed, (some form of) *identification* is arguably needed to safeguard the payment system, and AML/CFT/CPF and anti-fraud practices imply a trade-off between access to the means of payment and *traceability*. If CBDCs are designed to replicate cash-like *anonymity*, but at the same time overcome the physical limitations of coins and banknotes, significant concerns arise. The vulnerability of a fully *anonymous* token-based CBDC system arguably threatens public interest, which makes some level of *identification* crucial in a CBDC design.[831]

Interestingly, cash being dangerous from an AML/CFT/CPF perspective was one of the drivers of e-money solutions, due to the degree of control they can enable through programmability.[832] Indeed, monitoring and/or limiting the use of cash is a widespread method to counter criminal activities and was one of the first measures to mitigate ML/TF/PF risks, establishing cash-use thresholds and incentives to use traceable means of payment. Reportedly, three types of thresholds can limit the flow of cash, placed on (i) purchases (*e.g.*, on all/certain goods, day/month/per person limit depending on the type of costumer, AML/CFT/CPF obligations on cash-intensive businesses); (ii) cross-border transfers (*e.g.*, FATF's Recommendation 32 on "cash couriers" and its Interpretative Note on "declaration" or "disclosure" systems); (iii) banknote denomination.[833] Meanwhile, cash transactions above certain volumes may trigger compliance duties and other measures – *e.g.*, Interpretative Note to FATF's Recommendation 29 provides that members should consider a reporting system for large cash transactions. Against this backdrop, it is pivotal to underline that although CBDCs are usually benchmarked to cash in terms of capacity to offer *privacy* and *anonymity*, this feature is far from limitless, and many jurisdictions have implemented transactional reporting thresholds and other limitations.[834]

As per cross-border transfers, Regulation (EU) 2018/1672 provides for a declaration obligation on natural person, defined as "carriers" (Article 2(1)(h)), entering or leaving the Union carrying cash of a value of EUR 10,000 or more (Article 3(1)).[835] Here, "cash" comprises four categories: (i) currency, (ii) bearer-negotiable instruments, (iii) commodities used as highly-liquid stores of value, (iv) prepaid cards (Article 2(1)(a)), where "currency" means coins and banknotes circulating as a medium of exchange, the holders of "bearer-negotiable instruments" can claim a financial amount without having to prove identity or entitlement (*e.g.*, traveller's

[831] BIS (2021) Carstens A (2021), p 17
[832] Allen S, Capkun S, Eyal I et al (2020). Nabilou H (2019)
[833] Riccardi M, Levi M (2018), pp 147-148
[834] World Economic Forum (2021b), p 157
[835] Regulation (EU) 2018/1672

cheques and promissory notes), the definition of a "commodity used as a highly-liquid store of value" refers to an annexed list of goods with a high value-volume ratio and easily convertible into currency (*e.g.*, coins with gold content of at least 90%; and bullion such as bars, nuggets or clumps with gold content of at least 99,5%), and "prepaid cards" are non-nominal, not linked to a bank account, and store (or provide access to) a monetary value that can be used for payments, to acquire goods or services and to redeem currency (Article 2(1)(c-f)).

Furthermore, in the EU CDD obligations arise for FIs upon establishing a business relationship or when customers perform transactions of EUR 15,000 or more, and "traders in goods" are subject to the AML/CFT/CPF regime upon receiving cash payments above EUR 10,000. In Canada and in the U.S., regulated entities must report transactions of CAD/USD 10,000 or more within 24-hours.[836] In the past, the EU had unsuccessfully considered unified restrictions to payments in cash,[837] while some countries already limit cash use between private individuals and/or between consumers and businesses, and/or between businesses, if no regulated intermediary is involved in the transaction.[838] Bearer's instruments, such as bearer's checks and passbooks, are usually equated to cash. Illustratively, the following limits are in place: EUR 500 in Greece; EUR 1,000 in France (only for residents, otherwise EUR 10,000; not applicable between private individuals); EUR 1,000 in Portugal (for residents, otherwise EUR 3,000); EUR 2,500 in Denmark (not applicable between private individuals), Poland (not applicable between private individuals), Spain (not applicable between private individuals; for a non-resident consumer the limit is EUR 10,000); EUR 3,000 in Belgium (not applicable between consumers), Lithuania, Slovakia (but between private individuals EUR 15,000); EUR 5,000 in Bulgaria, Italy (starting from 2023), Slovenia (not applicable between consumers); EUR 7,000 in Latvia; EUR 10,000 in the Czech Republic, Malta (for selected goods); EUR 15,000 in Croatia.[839] In these jurisdictions, transfers of higher values must be made through regulated intermediaries. Similar strategies are applied in Jamaica, Mexico, Uruguay and India.

As outlined in Chapter 4, however, the AML Package proposed an EU-wide cash-payment limit of EUR 10,000 for professional purposes.[840] As per Article 59(1) AMLR, "persons trading in goods or providing services may accept or make a payment in cash only up to an amount of EUR 10,000 or equivalent amount in national or foreign currency, whether the transaction is

[836] FINTRAC (2019). 31 U.S.C. Title 31
[837] Ecorys and Centre for European Policy Studies (2017)
[838] Sands P, Campbell H, Keatinge T, Weisman B (2017)
[839] European Consumer Centre France (2022)
[840] European Commission (2021f). European Commission (2021a). Article 2(1)(30) defines "cash" with reference to Regulation (EU) 2018/1672 outlined above.

carried out in a single operation or in several operations which appear to be linked", where Article 59(4) specifies the limit does not apply to "(a) payments between natural persons who are not acting in a professional function; (b) payments or deposits made at the premises of credit institutions. In such cases, the credit institution shall report the payment or deposit above the limit to the FIU". While the 4AMLD had tried to mitigate cash-related risks by including among obliged entities "persons trading in goods" when making/receiving cash payments amounting to more than EUR 10,000, the approach proved ineffective vis-à-vis the differences at Member State level. Hence, in conjunction with the Union-wide limit, "persons trading in goods" would no longer be considered regulated entities.[841] Indeed, the proposal prevents traders in goods and services from accepting cash above EUR 10,000 for a single purchase, while it allows Member States to establish lower ceilings. In this respect, the EC is expected to assess costs, benefits and impacts of lowering the limit and its enforceability.[842] The approach towards cash-related risks also emerges in the FTR recast proposal,[843] where simplified regimes for transfers below EUR 1,000 do not apply if originating PSPs receive the funds in cash (Articles 5(3)(a) and 6(3)(a)), or if beneficiary PSPs pay out the funds in cash (Articles 7(4)(a)).

5.4.2. The privacy and data protection conundrum

A major cryptocurrency driver was the desire to exchange money privately, without involving a third party. After the adoption of the GDPR, a wave of global-scale sensitivity to data protection concerns started to permeate the law and technology domain. At times, this seems at odds with AML/CFT/CPF, while blockchain-based environments raise specific questions. An extensive array of contributions addresses the interplay of blockchain, privacy and data protection,[844] where scholars focused on contrasts in permissionless blockchains,[845] PETs and *de-anonymisation*. The topic is most relevant to CBDCs and is at the heart of heated debates: public-private dynamics of CBDC designs originate diverging questions, as private actors may be made part of mechanisms of information exchange detrimental to the privacy of end-users.

A literature review shows how AML/CFT/CPF aspects are often discussed as opposed to privacy and data protection: the more data is (or can be) disclosed to regulated entities and

[841] European Commission (2021a), Recitals 14 and 94
[842] Ibid, Recital 95
[843] European Commission (2021c)
[844] Finck M (2019a) Karasek-Wojciechow I (2021) Salmensuu C (2018) Berberich M, Steiner M (2016) Goodell G, Aste T (2019)
[845] Karasek-Wojciechowicz I (2021)

LEAs, the more intrusive the consequences may be on financial aspects of end-users' lives.[846] By contrast, a system with *full privacy* ostensibly thwarts compliance regimes. These considerations are mirrored by the research on CBDC designs, with attempts to build *anonymity*-oriented pilots while avoiding drawbacks. Relatedly, experts put forward a CBDC architecture to combine *privacy* with oversight by holding CBDCs outside of custodial relationships.[847] The proposal is based on the distinction between *privacy* and *data protection*, to be heeded when applying *privacy by design*. Indeed, although the latter is favoured for data protection, *data protection* concerns access and use of private information once it is collected (*i.e.*, prevention of unauthorised use of data), while *privacy* means preventing individuals and businesses from revealing data on their habits and behaviours. It follows that *privacy*, as architectural property and fundamental design feature, cannot depend on authorities "granting" or "guaranteeing" it through *data protection* schemes.[848] In this sense, data should not be collected to begin with.

As mentioned above, the *privacy* and *transparency* properties of CBDC models are strongly linked to the technical design – *i.e.*, often, to the enterprise solution underpinning the prototype. Chiefly, the chosen technology stack embeds a twofold design choice, pertaining to (a) architecture (*e.g.*, specifics of the ledger), that affect the roles and relationships between processes and software systems, and (b) transaction representation (*e.g.*, type of encryption with respect to the different actors involved in the system, account-based or UTXO-based model). These options govern the way to encode transactions with respect to the data flow to various stakeholders.[849] Evidently, the role played by private actors within a CBDC model influences the data flow and data protection dynamics. Remarks were provided on data access and accessibility depending on whether distributors (*i.e.*, providers of CBDC gateway services) act as (i) wholesale processors, in a system where each entity processes its transactions, (ii) processing agents, within a scheme where distributors participate in the core system and access a broad range of data and meta-data (*e.g.*, users' profiles and buying patterns) according to the chosen model for identity management and data storage, (iii) custodians and gateways in a centralised model, where distributors perform limited functions and access little information.[850]

Although this debate is relevant to digital payments at large,[851] CBDCs are arguably vulnerable to aid mass monitoring, profiling, surveillance, endanger the control of personal

[846] Garratt RJ, Van Oordt MR (2019)
[847] Goodell G, Al-Nakib HD, Tasca P (2021)
[848] Ibid, pp 3 and 6
[849] Fanti G, Pocher N (2022), p 11
[850] Oliver Wayman Forum (2022), pp 49-54
[851] Garratt RJ, Van Oordt MR (2019). Goodell G, Al-Nakib HD, Tasca P (2021)

information and protection against its misuse, threaten data protection, security, and safety. Chiefly, concerns about data abuse and personal safety arise from the combination of transaction, geolocation, social media and search data, and the protection of individual *privacy* against governments and commercial players was framed as a basic right. In this respect, the understanding of CBDC-related *privacy* is broad:[852] albeit often treated as a single concept, it concerns different stakeholders – *e.g.*, central banks, settlement and payment providers, retailers. In this sense, experts focused on how to govern access to the system, to establish public-private roles in guarding identity and transaction data, but also under which conditions public entities can access CBDC data and metadata and if/how to share it with the private sector.[853]

Against this backdrop, public-private CBDCs generate pressing dilemmas. While significant concerns followed financial digitisation, PPPs may offer more secure solutions that other setups, easing the application of advanced cryptography to wallet architectures and transaction environments and speeding up the application of DLTs, thus protecting consumers, lowering costs and strengthening compliance. At the same time, specific technologies require adequate controls to protect personal data and, in the absence of safeguards, a CBDC based on a public (permissioned) blockchain could become the "most privacy-invading citizen surveillance tool we have ever seen".[854] Relatedly, data privacy preferences and regulatory frameworks vary across the globe and CBDC initiatives embody context-specific inclinations.[855]

5.4.3. The competence for AML/CFT/CPF compliance

If one of the drivers of CBDC initiatives is the intention to mirror cash usability, it seemingly makes little sense for procedures to resemble those of traditional bank accounts. Hence, it is not a surprise that token-based CBDCs were argued to be more conducive to goals of financial inclusion and access to central bank money than account-based ones. Nonetheless, not only it was argued CBDC implementation offers the perfect opportunity to mitigate some of the new risks by embedding sophisticated AML/CFT/CPF detection and anti-fraud solutions,[856] but it is also clear that if a CBDC initiative underestimates AML/CFT/CPF compliance during the design phase it does not mean users and regulated entities will be allowed to operate beyond such

[852] Rennie E, Steele S (2021), pp 6-17. BIS (2021)
[853] Carstens A (2021). Oliver Wayman Forum (2022), pp 17-18
[854] Jagati S (2020)
[855] Carstens A (2021). For an analysis of *privacy* and *transparency* requirements in cross-border CBDCs, with specific regard of data-sharing dynamics in different CBDC models: Fanti G, Pocher N (2022)
[856] Oliver Wayman Forum (2022), p 19

principles. Instead, one can expect compliance burdens to be shifted to private entities offering CBDC product/services to the end-users. These observations lead to preferring either a *two-layered* structure or one where the CBDC itself offers strong *anonymity*, but regulators require private service providers converting CBDCs to other currencies to implement KYC on their customers. Of course, a central bank may also undertake the costly compliance effort herself and keep records *anonymous* if she is the sole processor of CBDCs' settlement.

As mentioned above, CBDC architectures have different AML/CFT/CPF repercussions. A key question relates to the responsibility for compliance duties, KYC, account management, identity and transaction checks. While in a direct CBDC structure the central bank would need new resources and expertise,[857] *two-layer* models allow compliance to be outsourced to PSPs and commercial banks, to be either managed directly or delegated. Hence, *two-tier* structures may be favoured by central banks, which do not traditionally interact with public end-users but rather with a handful of private financial institutions. This intermediated access model is favoured to leverage existing customer-facing services and avoid duplication of KYC resources. From this perspective, public-private cooperation was argued to help reduce risks and costs, as central banks do not ordinarily manage onboarding, customer service, dispute resolution, technology maintenance, transaction monitoring and compliance.[858] Accordingly, it was suggested the most balanced architecture would be hybrid, with central banks issuing CBDCs and the private sector handling payment services in a way deemed more convenient and efficient.[859]

5.5. Privacy vs. Transparency: the Topical Role of Trade-Offs

If digital fiat money is advertised as a cash substitute, any desire for *privacy* should not threaten the integrity of the financial system. As argued in Chapters 2 and 3, *anonymity* and *privacy* are not binary properties, but range within a spectrum.[860] In this respect, the two concepts refer to two different abilities of the individual to exert control on which personal data is shared/when/with whom (*privacy*) and not to have their identity known (*anonymity*).[861] Meanwhile, IoM *anonymity* has a socio-technical nature,[862] influenced on the technical side by specific tools, governance, system architecture, and on the social side by the possibility of

[857] Bossu W, Itatani M, Margulis C, et al (2020), p 10
[858] Zhang T (2020). Sidorenko EL, Sheveleva SV, Lykov AA (2021), p 498. Auer R, Böhme R (2020)
[859] Auer R, Böhme R (2020)
[860] Experts addressed the difference between anonymous, identified and pseudonymous clients: De Koker L (2009). "Crypto" digital payments enhance these complexities: Pocher N, Veneris A (2022b)
[861] Oliver Wayman Forum (2022), pp 17-18
[862] Rogaway P (2016). Sardá T, Natale S, Sotirakopoulos N, Monaghan M (2019), pp 557-564

identification and *traceability* and the use of forensics, vis-à-vis strategies to prevent it.[863] Undeniably, policy makers are caught between offering CBDC users the highest degree of *anonymity*, making *identity data* hardly accessible to the public and the private sector, and establishing identity-based services. In different jurisdictions, this clash is influenced by aspects not CBDC-related – *e.g.*, the attitude towards data protection and digital ID management.[864]

Although a *privacy-transparency* tension is inherent to CBDCs, in line with the arguments of Chapter 2 the relationship emerges as a trade-off. To establish the desired one, it is possible to rely on technology (*e.g.*, cryptographic techniques) and/or on regulation that sets data governance policies (*e.g.*, usage or access limitations). While the first option seems more resilient and tamper-proof (*e.g.*, independence from political changes, lack of compliance), policy measures are more flexible and adapt to societal needs.[865] Against this backdrop, not only CBDCs can be designed to embed various *privacy-transparency* trade-offs, but DLTs themselves are conducive to balancing the individual right to *privacy* against AML/CFT/CPF public interests. While a fully *transparent* CBDC, with visible *real-world identities*, may violate human rights, if *privacy* is provided without limitation, and no information can be revealed, misuses for illicit purposes may not be averted. Luckily, nuanced solutions are available, and most CBDCs offer some *privacy* to end-users and some *visibility* to authorities. These trade-offs can be addressed from the perspectives of *confidentiality* and *auditability*,[866] and designs can be classified accordingly and correlated with the AML/CFT/CPF understanding of *anonymity*.

The interlink between technical and regulatory compliance suggests *design-based* regulatory techniques, explored in Chapter 6.[867] Indeed, the notion that compliance aspects ought to be considered from the early stages of a system's design is gaining momentum, and this forward-looking approach requires preliminary engineering and standard setting as to the regulatory objectives and the available technological options or tools.

5.5.1. Confidentiality and auditability in CBDC designs

As highlighted in Chapter 2, the AML/CFT/CPF field does not differentiate between *anonymisation* and *strong pseudonymisation*. Rather, *anonymity* encompasses both the impossibility

[863] Pocher N, Veneris A (2022b)
[864] Oliver Wayman Forum (2022), p 21
[865] Ibid, pp 17-18
[866] Pocher N, Veneris A (2022b). European Central Bank and Bank of Japan (2020)
[867] Pocher N, Veneris A (2022b). Pocher N, Zichichi M (2022). Nabilou H (2019). Zetzsche DA, Arner DW, Buckley RP (2020). Torra V (2017). Yeung K (2017), pp 118-136

to link data to (an) *identified* person(s), and situations in which the link is (only) significantly hampered. Thus, it can happen the same data qualifies as *pseudonymous* for data protection purposes and *anonymous* under the AML/CFT/CPF framework.[868] Against this backdrop, CBDC research provides guidelines for *identity management* (*i.e.*, the decision on which data to collect on individuals and with whom to share it) by taxonomising relationships between the system and users' *individual identities*. The relationship can be: (i) *anonymous*: when the individual is not known to the central bank, distributors, other counterparties, and it is extremely difficult to determine *real-world identities* on the basis of the accessible data; (ii) *pseudonymous*: when, although *real-world identities* are not recorded, a *unique identifier* is linked to each transaction and authorised parties can determine *real-world identities* for purposes such as law enforcement and investigation; (iii) *knowable*: when *real-world identities* are known to the central bank and/or to distributors and are linked to all accounts and transactions.[869]

Accordingly, *user privacy* trade-offs range between complete *anonymity* – when a distributor assigns a system identifier not tied to the user's *real-world identity* and obscured from transactions, unlikely for KYC reasons – to *fully centralised* and *identity-based* services. Along this spectrum, three viable configurations emerge, where identity is (i) *pseudonymous* to all; (ii) known to the distributor but not the CBDC system; (iii) known to both the central bank and the distributor. It follows *identity management* strongly influences the level of *individual privacy*, from high individual privacy to high provision of centralised identity-based services.[870]

In this context, it is clear that users' individual *privacy* can be assessed with reference to the central bank, if the system is centralised, or also in relation to the distributor(s). This is far from trivial: while in public surveys *privacy* protection always ranks as a top priority in payments, individuals do not only care about what data is collected, but also with whom it is shared and for what purpose. The participants in the CBDC system (*e.g.*, central bank, distributors, PSPs) can be granted different levels of *visibility* into user data.[871] As argued above, multiple solutions can be adopted within the same CBDC scheme, and a regime of *anonymity* and *pseudonymity* can be provided for low-value transactions and low-balance wallets, possibly coupled with the limit to hold only one CBDC wallet, and in conjunction with an *identity-compliant* wallet, while "step-up authentication" mechanisms can allow additional risk-based checks.[872]

[868] Karasek-Wojciechowicz I (2021), p 3
[869] Oliver Wayman Forum (2022), pp 25 and 36
[870] For instance, the existence of an independent (outside the central bank's perimeter) national ID system arguably allows for a centralised-based system that does not change a jurisdiction's *privacy* approach. Ibid, pp 21, 25, 37
[871] Ibid, pp 17-18 and 36
[872] Ibid, pp 21 and 39

5.5.2. The role of Privacy-Enhancing Technologies

Privacy by design was first formalised with regard to PETs, to exemplify how technology can pursue regulatory goals.[873] Indeed, PETs can be defined as "technologies or systems that incorporate technical processes, methods or knowledge to achieve specific privacy or data protection functionality, or that implement specific requirements of data protection laws and reduce the risks associated with processing personally identifiable information, such as the risk of data breaches".[874] As explored in the previous chapters, *privacy* and *anonymity* are twofold, and PETs can be implemented to protect *individual privacy*, but also to pursue enhanced *anonymity* and *untraceability*, thus crippling the fight against illicit activities. This janiform use responds to different goals and is technically mirrored at the implementation level by specific combinations. For instance, ZKPs are leveraged by the AEC Zcash, but Ethereum and Quorum deploy zk-SNARKs as well. This concept is at the core of the remaining parts of this chapter.

From an AML/CFT/CPF perspective, data protection must be balanced with *accountability* and the deployment of PETs poses *auditability* challenges. Indeed, to ensure *accountability* in a financial scenario third parties need to scrutinise transactions, where *auditability* is the "understanding of transaction information by the authorised third parties, or the degree to which a given environment allows an authorised entity to audit confidential transaction information by viewing and interpreting the information".[875] From this perspective, PETs offer compromises to tackle *privacy* and *confidentiality* issues generated by sharing data in a distributed environment by limiting data access to unauthorised parties. Reportedly, they are the best technology option to replicate the *privacy* feature of cash, where they can "maximise the potential of CBDC for achieving policy goals while providing privacy".[876]

While PETs support *privacy* and *transparency* in manifold forms, the balance is technically challenging and if they are applied concurrently "there could be a trade-off between enhancing confidentiality and effective auditability".[877] Hence, experts analysed the ways *privacy* can be coded into blockchain systems,[878] and the compatibility with regulation. For instance, not all PETs have the same impact on data retrieval, where the AML/CFT/CFP goal is not only proactive compliance (*e.g.*, balance and payment limits), but also retroactive (*e.g.*, data retention,

[873] Cavoukian A (2011). Hustinx P (2010), pp 253-255. Tamò-Larrieux A (2018), pp 22-23
[874] World Economic Forum (2021e), p 12
[875] European Central Bank and Bank of Japan (2020), p 1
[876] World Economic Forum (2021b), p 157
[877] European Central Bank (2020b)
[878] Renwick R, Gleasure R (2020)

auditing, mandated disclosure). In this respect, the ECB and Bank of Japan delved into the impacts exerted by different PETs on the balance between *confidentiality* and *auditability* when sharing payment and securities settlement data in a permissioned distributed network.[879] Although the focus of the project was limited to transactions between participants of a wholesale system, thus excluding by its findings end-user data,[880] the analysis provides insights into *confidentiality* and *auditability* levels in an IoM scenario. Indeed, when PETs are applied to transaction data to make it *confidential*,[881] they impact data *auditability* in different ways. Accordingly, PETs are systematised as *segregating*, *hiding*, and *unlinking*, as outlined below.

The function of *segregating* PETs is to share information on a "need to know" basis, so that each participant's *visibility* is limited to a subset of transactions. In the permissioned Corda, transaction data is protected at the level of network communication, where each communication can be partaken solely by authorised and identified participants, and the so-called "notaries" receive (all or part) of the information to avoid double-spending. In the permissioned Hyperledger Fabric, transaction data is safeguarded by dividing the network into subnetworks and ledger subsets, with each channel requiring authentication and authorisation, and a network service orders the transactions. Finally, as introduced in Chapter 3 "layer 2 payment channels" allow *confidentiality* by permitting native funds to be transacted off-ledger. This may become a payment channel hub when an intermediary is involved. A related technique enhances *confidentiality* by performing transactions outside the main network is to establish sidechains.[882]

Secondly, *hiding* PETs foster *confidentiality* at transaction level by implementing cryptography against unauthorised interpretation. In the Ethereum-based Quorum, when participants transact privately data is stored in private ledgers with only one-way hash values stored publicly. In Pedersen commitments, participants can share only commitments instead of transaction amounts, so that they are uninterpretable to third parties, but inputs-outputs equivalence can be verified. Thirdly, as explored in Chapter 3 ZKPs allow "to share the output of some computation with a second party, without sharing the inputs to the computation, while ensuring the output is valid according to a publicly available function".[883] A third party can verify information without content disclosure. In zk-SNARKs, a trusted party sets up a secret parameter that generates proving and verification keys, used by senders and for validation, respectively.[884]

[879] European Central Bank and Bank of Japan (2020)
[880] Ibid, p 3
[881] *i.e.*, prevent unauthorized parties from viewing and interpreting it, where "view" refers to the existence of visible transaction data and "interpret" to the possibility to derive value and identities. Ibid, p 4
[882] Ibid, pp 6-8. The topic is addressed by Chapter 3.
[883] World Economic Forum (2021b), p 162
[884] European Central Bank and Bank of Japan (2020), pp 8-11

Finally, *unlinking PETs* conceal the *identities* of the parties from the *pseudonyms* stored on the ledger, making it difficult to determine transaction relationships from ledger data. A common technique already explored with regard to its application in Monero is "one-time address", where different addresses are used for different transactions, and deterministic wallets mitigate address management's drawbacks. Otherwise, mixing mechanisms shuffle transactions for relationships to be *unlinkable*, where the degree of *confidentiality* rests on the amount of mixed data, as outlined in Chapter 3. If the scheme is centralised, providers are entrusted with the original data; this can be averted in P2P mixing, but the latter requires other parties to be found timely. Lastly, "ring- and multi-signatures" allow it to be proven that a signer is part of a group of signers without disclosing its identity. Because transaction amounts are stored in the clear, these techniques are often combined with *hiding* techniques.[885]

The study shows how PETs exert different impacts on the *auditability* of *confidential* transaction data, where *auditability* is measured by assessing (i) *accessibility* to necessary data – *i.e.*, the auditor can access the data it needs to perform the audit via alternative data sources, that exist by design or are credible parties implementing PETs –, (ii) *reliability* of the obtained data – *i.e.*, the auditor can be certain the original data can be acquired using the obtained data –, and (iii) *efficiency* of the auditing process, measured by resources' consumption. When all criteria are met, *auditability* is *effective*.[886] In other words, *effective auditing* is performed when the auditor receives the necessary data from trusted sources or from identifiable participants and can verify its correctness with what is recorded on the ledger, and the process does not require excessive resources.[887] Reportedly, *effective auditability* can take place after the application of *segregating* PETs (*e.g.*, in Corda transaction data is shared by design with "notaries", in Hyperledger Fabric with "ordering services"), Quorum's private transaction, Perdersen commitment, and centralised mixing. Hence, it can be argued they may allow *anonymity* and *transparency* to be balanced in a CBDC-wise desirable way.[888] By contrast, ZKPs, mixers, one-time addresses, and multi/ring-signatures, prohibit *accessibility* of transaction data to auditors.

As anticipated above, PETs may be combined to deliver the desired balance. For instance, ZKPs are key in financial applications, as they "enable auditability and prevention of fraudulent activity, even within the scope of private transaction data" and are "efficient enough to be used for verifying all the protocol rules in a blockchain-based financial system with auditing

[885] Ibid, pp 11-14
[886] Ibid, pp 15-17
[887] European Central Bank and Bank of Japan (2020), p 24
[888] Pocher N, Veneris A (2022b)

capabilities".[889] From this viewpoint, an accurate assessment of ZKP *auditability* reportedly depends for the most part on the specific implementation. In case only transaction amounts are hidden, for instance, the evaluation on *auditability* resembles that of Pedersen commitment.[890]

5.6. Embedded Trade-Offs: a Case-Study Taxonomy

The way regulatory requirements are embedded into CBDC designs reveals trade-offs between *privacy* and *transparency*, where different use-cases enshrine diverging choices of sovereign institutions. Meanwhile, the specific design of a DLT-based system, such as the implementation of specific PETs, unveils a balance between *confidentiality* and *auditability*. Hence, a CBDC scheme embeds a specific trade-off between *privacy* and *transparency* in the form of *confidentiality* and *auditability*. This way of thinking mirrors the methodology underpinning *privacy by design*, notably the notion of *embedding privacy into the design*, thus making it an "essential component of the core functionality being delivered".[891] Accordingly, CBDC schemes can be classified as per the trade-off between *privacy/confidentiality* and *transparency/auditability* they embed. Against this backdrop, the goal of this section is to highlight a few concrete examples of how technology can be leveraged to reach various objectives. To this end, Figure 7 places CBDC projects across a spectrum of conceivable nuances.

As explored in Chapter 2, studies on identity *privacy* have largely focused on eliminating *identifiers*, where a solution has not yet been found to make it impossible for attackers to gather information on the *identity* of senders/recipients if it is recorded on a ledger available publicly or selectively. Hence, reportedly, it may not be feasible for CBDCs to achieve cash-like *anonymity* if such data is recorded on the ledger. Meanwhile, experts focused on achieving transaction *privacy* without preventing validators from verifying consistency of transaction amounts with account balances and compliance with predefined requirements, often through ZKPs. Other solutions leverage secure multiparty computation, rotation of public keys and TEE hardware-enclaved computing.[892] From a CBDC perspective, a way to offer *anonymity* while reaching a desirable level of *accountability* is to provide tailored solutions for different types of transactions, setting up schemes that can be defined as "mixed solutions".[893] Indeed, in theory *privacy* can be tackled selectively, meaning certain low-value transactions could be undertaken

[889] World Economic Forum (2021b), p 162
[890] European Central Bank and Bank of Japan (2020), pp 20-21
[891] Information & Privacy Commissioner of Ontario (2013)
[892] Allen S, Capkun S, Eyal I et al (2020)
[893] Pocher N, Veneris A (2022b)

without acquiring *identity* data. This type of CBDC model usually involves a token-based solution. Evidently, any trade-off will need to be identified at the beginning of the design cycle. Nevertheless, registration and *identity* verification can still take when a user signs up.

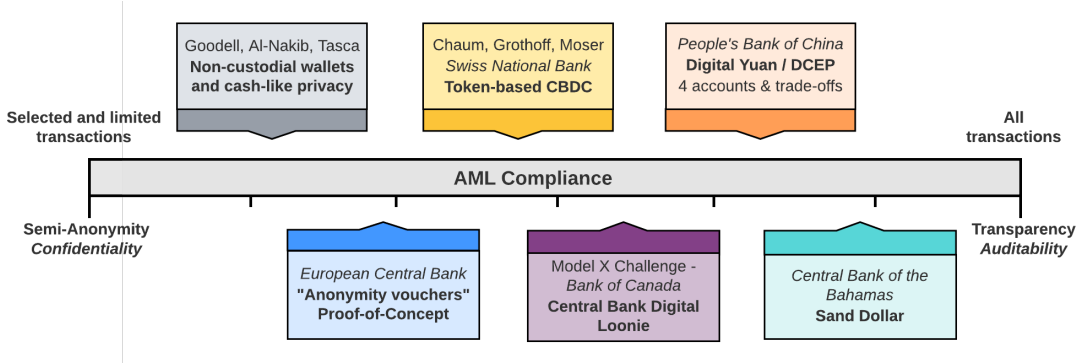

Figure 7: selected CBDC projects ranging from *accountable anonymity* to *transparency*
From: Pocher N, Veneris A (2022b)

5.6.1. Owner-custodianship and cash-like privacy

As mentioned above, it is possible to design a CBDC that combines *privacy* and oversight by holding CBDCs outside of custodial relationships.[894] The proposal is grounded on the distinction between *privacy* and *data protection*, where *privacy* is a key design feature that cannot depend on *data protection*. Reportedly, "exceptional access mechanisms that allow authorities to trace the counterparties to every transaction and, therefore, do not achieve anonymity at all".[895] In other words, data on individuals and businesses should not be collected to begin with. In this respect, the proposal mirrors the core features of cash – *i.e.*, *privacy*, owner-custodianship, *fungibility*, and accessibility. Accordingly, it relies on non-custodial wallets and envisions the application of PETs to ensure transaction counterparties are not revealed, while ensuring compliance with regulation. Three options are considered: (i) stealth addresses, Pedersen commitments, ring signatures; (ii) ZKPs; (iii) blind signatures or blind ring signatures.[896]

The scheme is overseen by the public sector, operated by regulated private entities, and can be tuned to different needs.[897] Because account-based systems cannot offer *privacy* if *identifiers* can lead to determine transaction parties, the system is token-based and non-custodial

[894] Goodell G, Al-Nakib HD, Tasca P (2021). On self-custody see also Barresi RG, Zatti F (2020)
[895] Goodell G, Al-Nakib HD, Tasca P (2021), pp 3, 6 and 12
[896] Ibid, pp 3 and 7
[897] *E.g.*, prohibit certain businesses from accepting payments larger than a given amount without collecting additional data or impose on specific individuals or non-financial businesses a cap on withdrawals to unhosted wallets

wallets do not carry *unique identifiers* or addresses that can be associated with other transactions, and do not reveal data that can identify bearers, owners, sources of funds (*e.g.*, keys or addresses associated with other transactions).[898] The proposal pursues an *anonymity* defined as "true but partial", where parties are *anonymous* but all transactions are controlled by a regulated entity. No one can unmask counterparties; even if authorities have all records some transactions involve non-custodial wallets, as it happens with cash. Hence, even if one knows all retail users and their transaction history, it is impossible to link non-custodial wallets to specific users.[899]

5.6.2. Semi-anonymity and the EUROchain

In 2019, the ECB explored the application of cash-like *anonymity* to a retail CBDC as part of the EUROchain network.[900] The group conceived a DLT-based simplified PoC for a *two-tier* CBDC where a degree of *privacy* for low-value transactions is ensured with no detriment to AML/CFT/CPF controls for higher values. The PoC was developed on Corda with the goal to avoid that users' *identities* and transaction histories are seen by the central bank and intermediaries other than the one chosen by end-users. Within this scheme, the latter are onboarded by an intermediary of their choice, and receive a *pseudonymous identity* that will be their CBDC network address.[901] On top of this, end-users are equipped with untransferable *anonymity vouchers*, to transfer a specific amount of CBDCs within a given timeframe with no oversight on transaction data. The thresholds are automatically enforced at the intermediary level, with a specific authority issuing the vouchers and carrying out checks for large-value transactions.

Hence, the transfer scheme allows intermediaries to perform checks but largely safeguards *confidentiality*. Features of enhanced *privacy* are based on Corda's *confidential party* mode, allowing states to be assigned to end-users with one-time keys not revealing *pseudonymous* identities.[902] However, Corda's data segregation model does not solve the issue of intermediaries being able to build knowledge graphs based on past transaction data of CBDC units. Moreover, *privacy* could be enhanced with rotating public keys, ZKPs and hardware enclave computing. Using rotating keys would limit the ability of the nodes to *link* transactions to users, since they would be generating new *pseudonyms* for every transaction.[903]

[898] Ibid, pp 2, 5-7, 10
[899] Ibid, pp 12 and 22
[900] European Central Bank (2019)
[901] Ibid, p 3
[902] Ibid, p 7
[903] Ibid, pp 9-10

5.6.3. Token-based transaction privacy

As highlighted above, bearer-type token-based CBDCs may provide higher transaction *anonymity*, especially when the payment is hardware-based – *e.g.*, prepaid cards storing tokens for offline use. In this respect, token-based systems were argued to be the only avenue to reach a cash-like *transaction privacy*.[904] At the same time, the hardware-based subset presents some features that may not suit a CBDC scenario, chiefly in terms of online transferability and AML/CFT/CPF compliance. In proposing a non-DLT-based CBDC that is a "true digital bearer instrument", it was claimed a token-based option is necessary for assets not to be associated with transaction history – contrary to what happens with account-based systems.[905] The proposed architecture is, however, software-based, for the sake of *transparency* and *accountability*.

In this architecture, payers and payees interact only with commercial banks. Customers/payers are identified when they withdraw CBDCs, and merchants/payees upon receipt. Other than this, no *identification* is needed to perform the transaction, which means customers' and merchants' identities are not unveiled to the central bank. The withdrawn coins are subject to an encryption performed by the smartphone that "blinds" the relevant number. When the merchant deposits the coins, the central bank can carry out anti-double spending checks without knowing which user withdrew it nor the total transactions amounts. Building on E-Cash, GNU Taler and Chaum's work,[906] the privacy of buyers is safeguarded by blind signatures, preventing commercial and central banks from linking transactions to buyers. Meanwhile, conversion limits may be imposed for AML/CFT/CPF purposes, and the GNU Taler key-exchange protocol aims to ensure income *transparency* and consumer *privacy*. Hence, KYC and authentication services are performed by commercial banks. Finally, the authors specify the possibility to implement jurisdiction-specific limits on withdrawals/payments in the proposed design.

5.6.4. Model X: a Canadian Central Bank Digital Loonie

As mentioned above, "mixed solutions" can provide nuanced balances between *privacy* and *transparency* suitable to different transactions. This concept is strongly related to the objective of supporting offline transactions. In this context, a Canadian PoC developed by a team from the University of Toronto and York University provided a CBDC model in the context of a

[904] Chaum D, Grothoff C, Moser T (2021)
[905] Ibid
[906] Chaum DL (1983)

"competition of proposals" published by the Bank of Canada in April 2020.[907] The approach underpinning the proposed Central Bank-issued Digital Loonie (CBDL) is two-phased and account-based; the scheme is first *centralised* and later evolves towards *decentralisation*.

In particular, users obtain wallet addresses, represented by *quasi-anonymous identifiers*, after undergoing an e-KYC performed by a third-party authenticator. Although the system is not built to identify and share users' identity or transaction-data to other system parties, the users do not remain *anonymous* if the encrypted process triggers compliance flags, or if there is any court order. It is proposed wallets have upper limits sufficient for typical cash-like transactions, and special provisions, such as reduced functionality or expiration dates, for visitors. For offline transactions, there is a CBDL-card, and a smart-device-based functionality that emulates it. For AML/CFT/CPF purposes offline transfers via CBDL-cards could be capped.[908]

In 2021, a group of researchers put forward another "mixed" CBDC solution. For what concerns the degree of *privacy*, their account-based model features three types of transactions, defined as "fully private", "semi-private", and "fully transparent".[909] The first option foresees "cash-like" transfers performed within a "privacy pool" inspired by Zcash, but replacing the UTXO-based model with an unspent account state model. In this case, zk-SNARKs are leveraged so that neither the identities of the parties nor the transaction amount are revealed to third parties, yet imposing *by design* balance, transfer and turnover limits for purposes of regulatory compliance.[910] Secondly, "semi-private" transfers take place between accounts held in said "privacy pool" and transparent CBDC accounts, which resemble commercial bank accounts. Thirdly, "fully-transparent" transfers are performed between transparent CBDC accounts.

5.6.5. China's e-CNY

As highlighted above, the People's Bank of China is consistently expanding the testing scope of the e-CNY. At the time of writing, most information can be derived from public talks by Chinese officials and by a first white paper released in July 2021.[911] In this sense, valuable comments pertain to the concept of *controllable anonymity* or *managed anonymity*. The e-CNY is informed by the principle of "anonymity for small value and traceable for high value" and is reported to offer four or five types of accounts/wallets. The decision on which account to assign

[907] Veneris A, Park A, Long F, Puri P (2021)
[908] The report foresees the application of PETs in the advanced stages of the project, when the need may arise to obfuscate data (*e.g.*, stream of transactions) from private validators (Ibid).
[909] Gross J, Sedlmeir J, Babel M, Bechtel A, Schellinger B (2021) pp 16-19 and 23-25
[910] Ibid, pp 21-23
[911] Working Group on E-CNY People's Bank of China (2021)

to a given user depends on characteristics such as CBDC amounts, anticipated use, and other information provided by the same user during the registration procedure.

Reportedly, the two most *anonymous* types of account (*i.e.*, "least privileged wallets") require few identifying pieces of information and notably *no real-name identity* (*i.e.*, it is not necessary to provide a *real-world identity*). In these cases, risks of money laundering and other criminal abuses are mitigated by imposing strict balance and transaction limits – *e.g.*, a daily transaction limit and a relatively low balance limit. On the contrary, depending on the provided information, the least *anonymous* types of individual or corporate wallets must be opened at a counter and can be linked to a bank account or even used as one. Further, the implemented restrictions (if any) vary, depending on the "strength of customer personal information", with regard to both types of transactions that can be performed and relevant amounts. Meanwhile, the e-CNY offers both software and hardware wallets.[912]

The U.S. report mentioned above outlined this system of *managed anonymity* by dividing accounts linked to the e-CNY into: (i) "broad" accounts, possibly linked to *real-world identifying data* such as ID cards, phone numbers or email addresses; and (ii) "narrow" bank accounts held at a commercial bank. The e-CNY achieves its cash-like *anonymity* from the perspective of users and operating institutions because the latter are not able to see who is paying what to whom. On the contrary, the People's Bank of China can trace the flow because it can see the links between addresses and *real-world identities.* From this point of view, this CBDC system was argued to "exchange privacy for compliance".[913]

5.6.6. Transparency and the Sand Dollar

If one proceeds along the *anonymity* to *transparency* spectrum, we find *transparency*-oriented solutions that comply with current regulatory frameworks for e-payments. Obviously, privacy and data protection requirements still need to be met, but transactions could be fully *transparent* to the entity operating the infrastructure. A high level of *transparency* is already offered by one of the few CBDC projects already operating, launched by the Central Bank of the Bahamas in late 2020. Its CBDC tokens represent a claim on the central bank and are recorded and transferred on a private DLT with all parties being *identifiable*.[914]

[912] Ibid
[913] Duffie D, Economy E (2022), pp 32ff
[914] Boar C, Holden H, Wadsworth A (2020)

5.7. Conclusions

Research into IoM dynamics requires a cross-disciplinary effort, and CBDC explorations provide a revolutionary insight into these interplays. This chapter provides an overview of key elements regarding digital fiat money, heeding a selection of debates elicited by publications by leading institutions, private actors, and monetary authorities. Although many central banks are not yet convinced that the benefits of issuing a CBDC outweighs risks and costs, they keep carrying out extensive research and elaborating PoCs. Along these lines, the chapter disambiguates the notion of "central bank money" and underlines the difference between wholesale and retail CBDC use-cases, as well as the main drivers underpinning the respective interest. It outlines the history of CBDC projects to value the various approaches and sketch the general trends, while addressing candidate designs (*e.g.*, token-based or account-based systems) and architectures (*e.g.*, direct, hybrid, intermediated or synthetic models) for retail CBDCs. Meanwhile, it focuses on *interoperability* and *standardisation*, and on the impact of public-private interplays and cross-border CBDC models. Later, it explores a set of regulatory issues raised by CBDCs from an AML/CFT/CPF perspective and contextualises the debate within the broader *anonymity problem* generated by physical cash and the establishment of limits to cash transfers. Furthermore, it tackles *privacy* and data protection concerns and the competence for AML/CFT/ CPF compliance in relation to different public-private designs.

Building on the previous sections of this work, in this Chapter I introduced the existence of trade-offs between *anonymity* and *transparency* in CBDCs, whose designs can embed various balances between individual *privacy* and AML/CFT/CPF interests to have identity-based services. In this respect, the majority of the available CBDC proposals offer some *privacy* to end-users and some *visibility* to authorities and/or other participants of the CBDC system. Relatedly, I showed in this chapter how trade-offs can be addressed from the perspectives of *confidentiality* and *auditability* and are correlated with AML/CFT/CPF *anonymity*. Further, I contextualised the role of *segregating*, *hiding* and *unlinking* PETs, exemplifying how they generate different balances between *privacy/confidentiality* and *accountability/auditability*. In this sense, the chapter elaborates on the arguments introduced in Chapter 3.

Finally, I provided details on how six examples of CBDC scheme can be classified in terms of their embedded trade-off between *privacy/confidentiality* and *transparency/auditability*. Relatedly, I underlined the concept of "mixed solutions" that provide for options tailored to given types of transactions and/or users – *e.g.*, higher *anonymity* for low-value transactions and low-balance wallets. In this context, I argue the large-scale interest in CBDC explorations provides

a revolutionary and almost unique insight into cross-disciplinary efforts. In this respect, my goal was to highlight the interplay of technology, regulation, and technical standardisation, and to provide preliminary benchmarks to think about *anonymity* and *transparency* in CBDCs in a way that enables the application of the methodologies addressed by the following chapter. In doing so, the need for techno-regulatory standards emerged vis-à-vis the current lack of *standardisation* in a form that allows automation – *e.g.*, for what concerns risk indicators and the implementation of M2M payments, that are both topics explored as use-cases in Chapter 6 –, also in relation to risk scores related to transactions and customers.

6. Techno-Regulatory Standards and Trade-Offs-[by/through]-Design

"*In the absence of cooperation between law and technology, these two aspects would battle to take the upper hand. One would have to succeed before the other takes over".*
Schrepel T (2021)

6.1. Introduction

The increasing complexity of the IoM and the diffusion of DLT-based use cases in the financial sector has drawn significant attention from law and policymakers. As a wide range of stakeholders explore these technologies on a global scale, risks and uncertainties arise with regard to regulatory approaches, both within the AML/CFT/CPF context and beyond it. While this is hardly unusual when it comes to innovation, in this field the urgency stems from the extensive reach and industry-altering impact of the combination of P2P mechanisms and tokenisation. Drawing on the findings of the previous chapters, I argue the difficulty in applying regulation to the IoM consists of a riddle generated by the concurrent presence of (i) *assets*, such as the different types of tokens outlined in Chapter 1; (ii) a set of *technologies* that can be used to different ends (*e.g.*, P2P technologies, distributed systems, tokenisation); (iii) *innovative actors* (*e.g.*, developers, miners, exchanges, FinTech companies, P2P platforms); (iv) *traditional actors*, such as traditional FIs; (v) different *scopes of application* of the technologies, at times overlapping or concurring (*e.g.*, financial applications, supply chain, self-sovereign identity, certification). The combination of these elements shapes the IoM and mirrors its nature of an ecosystem of socio-technical ecosystems, as argued in Chapter 2.

In addition, these categories are under constant development. The primary challenge lies in grasping the internal mechanisms of each socio-technical environment, often *non-centralised*, to understand the factors at play to devise appropriate rules and enforcement approaches. Against this backdrop, the relationship between the law, IoM ecosystems, *technologies* and *entities – i.e., assets* and *actors*, respectively – is complicated. Reportedly, different approaches are possible when the law meets new technologies. Regulators may decide to (i) do nothing, an attitude described as a permissive "wait and see" approach, (ii) introduce tight restrictions, such as outlawing certain activities or the provision and/or acquisition of certain products or

services, (iii) issue flexible "case by case" permissions, (iv) set up structured and restricted regulatory experiments such as "regulatory sandboxes", (v) devise new regulatory frameworks.[915] Evidently, these approaches and their possible combinations exert both positive and negative impacts on the targeted domains, and come with strings attached. Hence, a regulatory strategy should suit the given phase of the evolution of a technology. For instance, while a "wait and see" approach can be beneficial in the early days, over time it proves insufficient to handle the arising regulatory questions, which generates "case-by-case" decisions.[916]

As emerged in the previous chapters, the relationship between the IoM and AML/CFT/CPF rules is multi-faceted. In some ways, this mirrors usual issues generated by innovation, but the debate also entails more peculiar angles. In particular, the implementation of DLT-based solutions, tokenisation, and encryption, enables direct collaboration between individuals, but also creates *obfuscation* opportunities that challenge existing frameworks and allows the establishment of novel types of service providers. Notwithstanding the importance of averting overgeneralisations, it is not surprising the combination between (a) the lower degree of access control of (some) IoM ecosystems, (b) the *anonymity* levels of some of them, and (c) their cross-border character, originated the regulatory willingness to mitigate their vulnerability to endanger the financial system. As outlined in Chapter 4, international and domestic frameworks were established to fight the abuse of cryptoassets for illicit purposes and extended to a new domain the traditional approach to the prevention of criminal exploitation of institutions, solutions or technologies to cleanse ill-gotten money or fund illicit activities. Accordingly, frameworks leaned on gateway points (so-called "on- and off-ramps") resembling traditional intermediaries – *e.g.*, exchanges and providers of custodial wallet services. As emerged from the findings of Chapters 2 and 3, however, the developing concept of *disintermediation* challenges this traditional methodology, especially from an evolutionary perspective.

6.1.1. Technology- vs. individual case-based AML/CFT/CPF regulation

In Chapters 3 and 5 I highlighted how cryptocurrency ecosystems can enshrine different degrees of *anonymity* and *accountability*. Likewise, I outlined how red flag indicators point to specific risks generated by AECs and the implementation of given technologies. Evidently, not

[915] Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), p 5. Regulatory approaches to DLTs were classified as follows: (i) adoption of a "wait and see" approach, (ii) application of existing frameworks, (iii) issuing guidance (especially under (i)), (iv) establishment of sandboxes, (v) regulatory cooperation, (v) adoption of new legislation. Finck M (2019a) , pp 153ss. These methodologies are explored by Magnuson W (2020), pp 177-190
[916] Finck M (2019a), p 155

all cryptocurrencies and providers of related services pose the same challenges to the AML/CFT/CPF regime. Once again, the differences may pertain to all the components of these socio-technical ecosystems – *e.g.*, technologies implemented at application or platform level, by the actors involved, practices deployed by users, strategies developed by LEAs and analytics companies. Hence, I argue a suitable regulatory methodology should account for the different levels of risk, in compliance with the RBA, and appropriately distinguish between use-cases.

From this perspective, literature provides different types of regulatory approaches to new technologies, where rules are benchmarked either to the implementation of a technology (*e.g.*, a framework for DLT-based applications) or to a specific application (*e.g.*, a regime for cryptocurrencies, DLT-based or not). The first case is termed *technology-based* regulation, where the targeted applications are pinpointed based on the implemented technology, usually because the latter has an impact the regulator wants to address (*e.g.*, all DLT-based applications, targeting the effects exerted by some trait of DLTs). In the second case, efforts are benchmarked to the function of specific tools, in a *use case-based* fashion.[917] Use-case based regulation allows specificities to be accounted for and regulatory actions to be based on concrete cases – *e.g.*, cryptocurrencies, a subtype, even just one of them. Focusing on individual cases is beneficial when a technology can be exploited in many ways and originate diverse impacts. Besides these two categories, there are *mixed situations* where a regulatory regime is tailored to a set of use-cases implementing a specific technology – *e.g.*, cryptocurrencies embedding a given PET.

As I explore below, all these methods feature, to different extents, an inherent risk of over-fitting. Indeed, given the IoM's technological dynamism, there is an undeniable risk rules may be already outdated when they enter into force, or shortly after. I argue the goal should not be to avoid the risk altogether, but to establish frameworks that prove useful despite the changes.

6.1.2. Categorising impacts and the sandbox model

In the early stages of the IoM, scholars identified three types of interplay DLT-based applications can have with regulatory frameworks. I argue the reasoning is still relevant today, despite the increased complexities of the sphere, and that it is possible to extend its scope to the IoM. According to said analysis, a first set of instruments, usually implemented by regulated actors and overall compatible with existing frameworks, are placed in a *recycle box*. This is the

[917] *Technological neutrality* does not correspond to *use case-based* regulation. Strictly speaking, the latter does not require a neutral approach towards the implemented technology, nor that the goal is to set broadly applicable principles. However, the two concepts share the idea that regulation should not be drafted in technological silos.

case of blockchain-based interbank settlement systems (*e.g.*, the Ripple network, wholesale CBDCs) and blockchain-banking.[918] A second set of use-cases pursues objectives straightforwardly illegal, thus placed in a *dark box*. For instance, AECs arguably seek a level of *unaccountability* that clashes with AML/CFT/CPF and provisions grounded on the *transparency* of value exchanges. As a middle category, the *sandbox* collects innovations whose essence, despite not inherently illegal, is incompatible with compliance and involves risks that call for specific regulatory action. Illustratively, implementations that bypass regulated entities – *e.g.*, DEXes, some stablecoins, and perhaps the whole DeFi sphere.

The use-cases populating the *recycle box* often require tailoring existing rules to the new instruments, but usually the basic structure of the measures is not challenged. In principle, they do not require new policy trade-offs. For instance, wholesale CBDCs may rely on the *anonymity-transparency* trade-off deemed appropriate for interbank settlements by the international financial system. Hence, unless they put forward products and services with different societal spillovers, *recycle box* initiatives do not raise specific *anonymity-transparency* issues.

I argue the situation is similar, albeit opposite, for the *dark box* group. Even when these innovations stimulate a re-evaluation of what is illegal – *i.e.*, they can generate a shift in the societal attitude towards some activities, which may lead to reconsider their qualification –, said re-evaluation lies in policy-making choices rather than in the relationship between new instruments and existing frameworks. In other words, the technology may change societal perception, but it is still possible to apply existing frameworks to them. For instance, even if we argue cryptocurrencies changed the perception of the amount of *transaction privacy* society is willing to give up for the sake of regulatory oversight, DLTs are "just" the technology that prompted this change in perception towards *anonymous transactions*. Hence, if the current regulatory framework is applied, use-cases that make it impossible to complete KYC or that purposefully hinder transaction monitoring are breaching AML/CFT/CPF measures (*i.e.*, use-cases positioned towards the *anonymity* end of the *anonymity-transparency* spectrum).

On the contrary, the last category offers insights into how different types of cryptocurrencies challenge AML/CFT/CPF schemes under the *anonymity-transparency* lens. Not complying with existing frameworks, albeit without thwarting their rationale, is a frequent occurrence for blockchain-based applications, chiefly due to the interplay of new and traditional stakeholders. To confront these cases, especially in the domain of financial services, regimes of *regulatory sandbox* were established, where businesses are free to test their products and services without

[918] Maupin JA (2017)

immediate regulatory repercussions, in agreement with the authorities and implementing a set of safeguards.[919] The idea is to encourage innovation while allowing regulators to cooperate with the industry in understanding the specificities of new products and services.

In this respect, over time other regulatory solutions were developed to suit the blockchain space as a context of governance through software code – *i.e.*, safe harbours, modular contracts, information fiduciaries.[920] These regimes of "structured experimentalism" may replace reactive approaches that may hinder development by overburdening young industries.[921] With regard to DLT applications, four traits of an efficient sandbox were identified in global reach, cross-sectoral flexibility, start-up friendly structure, and use of case-tailored parameter-setting practices.[922] Although the sandbox approach has gained significant momentum in many jurisdictions (*e.g.*, EU Digital Finance Package), significant drawbacks suggests a shift towards more inclusive strategies.[923] Indeed, these regimes feature a few overarching frailties. For example, effective implementation requires a creative regulatory solution to be designed for all new cases, gathering the authorities of all sectors the innovation may impact on.[924] If the geographical scope is insufficient, the sandboxed activity would prove unfit in cross-border scenarios because the service, albeit regulated, is not standardised.[925] Additionally, given the wide application of DLTs, the different parameters of the sandbox should be tailored to "the underlying constellation of regulatory concerns raised in each case".[926] Empirically, this is not easy to guarantee.

The efforts to regulate the IoM mirror its multi-layered structure and different regulatory standpoints. In addition, the debate confronts innovations of increasing complexity, whose collocation within existing schemes is often unclear. The early scope limitation of regulatory initiatives grew into a more mature approach of specialised expertise, informed by a sensitivity to standardisation needs. In some cases, this turned into token-based frameworks, introduced in

[919] Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), p 13
[920] Werbach (2019), pp 204ss. A *safe harbor* regime "excludes certain activities from legal obligations. When firms can take sufficient steps to police themselves, a safe harbour incentivises them to do so" (Ibid, p 204). *Modular contracts* refer to making contract-drafting resemble coding, representing contractual clauses as components assembled into a digital document via a markup language, while templates establish agreements on common scenarios (Ibid, p 206). The application in blockchain-based environments of *information fiduciaries* arose from noticing how entities are often exposed to liability, and the challenge worsens the more the entity is decentralised and autonomous. Hence, *fiduciary duties* may develop for public blockchains, aligning "the locus of legal responsibility with the locus of code on blockchain networks" (Ibid, pp 208-211).
[921] Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), p 1
[922] Maupin JA (2017)
[923] Reportedly, effectiveness and efficiency of sandbox frameworks (i) depend on the expertise of regulators, (ii) may not be sufficient to guarantee success, (iii) may not provide sufficient societal safeguards and transparency levels, (iv) is influenced by the quality of the regulatory text, (v) may be challenged by concerns about the legitimacy of the regulatory interventions. Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), pp 58-61
[924] Maupin JA (2017), p 11
[925] Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), p 40
[926] Maupin JA (2017), p 12

Chapter 1, where the concept of token becomes a benchmark for regulation. On the contrary, technology-based approaches may not fully fit the fluidity of the IoM.

In the previous chapters I explored the presence of (i) a multi-layered AML/CFT/CPF framework (*e.g.*, global standards, EU law), (ii) technical and regulatory standardisation initiatives on DLTs and cryptocurrencies, (iii) the socio-technical nature of IoM ecosystems, including their *anonymity* and *transparency* levels, and the possibility to (iv) benchmark specific regulatory considerations (*e.g.*, *auditability, confidentiality*) to given socio-technical factors (*e.g.*, PETs, wallet types, public-private models), and finally to (v) apply the same reasoning in designing applications embedding given socio-technical aspects to reach regulatory goals.

When considering these concepts through the lens of the regulatory methodologies mentioned above, I argue it is possible to pinpoint a set of methodological features for future AML/CFT/CPF regulation that accounts for the array of trade-offs between *anonymity* and *transparency* in IoM ecosystems. Thus, in this chapter I outline the value of (a) deploying design-based compliance and regulatory techniques, (b) shifting from the concept of "code is law" to the compound notion of "[regulation/compliance]-[by/through]-design", exploring its essence and components, (c) establishing techno-regulatory standards adopted through *polycentric* co-regulatory models. Against this backdrop, I provide (d) a use-case of the proposed approach in terms of techno-regulatory integration, and (e) suggestions on methodological elements for the intervention of EU law, chiefly in terms of the legitimacy and effectiveness of any initiative.

6.2. A Regulatory Methodology for the IoM between Anonymity and Transparency

From a comparative and diachronic standpoint, the IoM has been targeted by various regulatory methodologies. While the earliest frameworks emerged in 2016-2017 in the US, and major hustles occurred in 2018-2019, only from 2020 regulatory actions have started mirroring a higher level of awareness of the complexities and specificities of this sphere. Notwithstanding specific exceptions,[927] early initiatives targeted securities and addressed ICOs to provide safeguards to investors.[928] Generally, lawmakers intervened upon identifying risks that could thwart financial integrity, and AML/CFT/CPF regulation was a key tool to mitigate the side effects of the "blockchain hype" in the financial domain. This is an example of *reactive* regulation, which responds to perceived threats, instead of addressing them *proactively*.

[927] *E.g.*, amendments to the Delaware General Corporation Law to record shares' ownership and issuance on DLTs
[928] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), p 1

In recent times, a two-fold scenario emerged: the understanding of expert communities increased significantly, and IoM ecosystems kept developing. Hence, scholars and regulators started grasping the value of *proactive* initiatives to help the relevant stakeholders (*e.g.*, authorities, LEAs, FIs, PSPs) navigate the ocean of cryptoassets. I argue a proactive regulatory approach requires a detailed understanding of the field and assumes its development can be positively influenced through regulation. This seems even more crucial in a socio-technical context, where IoM's characteristics are linked to the stakeholders involved. From this perspective, the participation of a large array of actors in regulatory processes may provide a substantial insight into the nuances between the risks the regulator wants to mitigate.

The previous chapters underlined how confused definitions affect regulation in its drafting, application, and enforcement. From a first perspective, a framework is based on normative considerations on the target to regulate: AML/CFT/CPF rules place duties on specific entities because they are deemed to be in a valuable position to mitigate a set of risks. Because *anonymity* is one of these risks, defining what it means in the IoM is pivotal to understand what the AML/CFT/CPF framework pursues to prevent in this context. The need to define an acceptable degree of *anonymity* (if any) arose from the illegal consequences of allowing unknown parties to transact. *Anonymity* is related to *opaqueness* vis-à-vis the difficulty to retrieve information on origin of funds, reasons for operations and beneficial owners' identity,[929] while the possibility to transact *anonymously* and reduce *transparency* of fund flows facilitates laundering.

Against this backdrop, I believe a regulatory methodology that can account for the *anonymity-transparency* trade-offs in IoM ecosystems should be tailored to their specificities, in terms of mirroring the nature of the target to be regulated. Accordingly, it should not only involve as many stakeholders as possible, but also heed variables bound to influence the *anonymity* risk or the concept of *transparency* useful for AML/CFT/CPF, *i.e.*, *auditability*. From this perspective, the IoM calls for a multi-stakeholder regulatory process that communicates with the industry to understand holistically its compliance needs. Meanwhile, it should heed the social factors, together with their influence on the *anonymity* level of a specific scenario. I define the latter as the combination between a given currency (or combinations thereof in case of cross-currency transactions), the platforms and the actors involved, also in terms of forensic strategies and user best practices that can be deployed vis-à-vis implemented technology. Accordingly, this section selects regulatory strategies highlighting suitable solutions.

[929] These aspects relate to AML/CFT/CPF obligations, and their specificities are outlined in Chapter 4.

6.2.1. (Lack of) accountability and the teleological approach

Anonymous transactions are tainted by the *unaccountability* of those performing them. The socio-technical nature of the IoM exerts impacts in this respect: cryptocurrency transactions are a multi-layered bundle of features, which spills into *anonymity* and *transparency*. In Chapter 2, I argued the two traits can be reconciled by pinpointing trade-offs and applying a teleological methodology. In this regard, an AML/CFT/CPF-specific approach to *anonymity* and *transparency* is key, and the literature shows a teleological reasoning when linking the notion of *transparency* to the retrievability of data on funds' origin and *identity* of clients and intermediaries. As outlined in Chapter 2, (some) blockchains are structurally incompatible with *financial transparency*, as the *transparency* of *non-centralised* systems is not the one useful for oversight.[930] This is another reason to apply a teleological approach focused on a definition's context.

In Chapter 2, I reported how *identification* (*i.e.*, establishing the *real-world identity*) and *identity verification* (*i.e.*, verifying its authenticity) are crucial in CDD. The threshold for *identification* is set by the framework, and *identifiability* depends on the entity trying to achieve *identification*. The goal is not public *retrievability* of data, which would infringe *confidentiality*. On the contrary, this notion of *identifiability* is subjective; in the IoM some actors try to achieve *identification* and others to avert it. Thus, since *anonymous data* is not related to *identifiable* individuals,[931] for AML/CFT/CPF purposes an *anonymous transaction* is one that the entity trying to reach *identification* cannot (or finds significantly hard to) relate to an *identifiable* individual – *i.e.*, CDD cannot be performed successfully, due to socio-technical aspects.[932]

In this respect, I outlined how AML/CFT/CPF rules does not distinguish between *anonymisation* and *strong pseudonymisation*, including both the impossibility and the significant difficulty of *linking* ledger data to (an) *identified* person(s). Operationally, the service may not be *identity-based* (*e.g.*, a distributor assigns an identifier not tied to the user's *real-world identity* and obscured from transactions), or the user can opt not to have the *real-world identity* known. From a teleological perspective, *anonymous* transactions were linked to the ones that are *untraceable* and defined as being performed between a sender and a receiver without third parties being able to identify the parties involved.[933] Said transaction is not effectively *auditable*, thus *anonymity* is dependent on the observer. These notions were explored in Chapters 2, 3 and 5.

[930] Quiniou M (2019), p 20
[931] ICO (2021)
[932] Karasek-Wojciechowicz I (2021), p 3
[933] Edmunds J (2020) d

New technologies provide new pathways to *accountability* but also to disrupt data retrievability. Although the simple fact that a cryptocurrency scheme is not immune to forensics does not make it AML/CFT/CPF compliant, it shows that not all *anonymity-oriented* cryptocurrencies are equally *anonymous*. As highlighted in Chapter 5, these schemes can be classified according to the impact of a given set of technologies on the *anonymity* risk and degree of *accountability*. Indeed, the implementation of various PETs (and combinations thereof) generates different trade-offs between *confidentiality* and *auditability*.[934] In Chapter 5, the analysis of CBDC designs displayed that *anonymity* and *transparency* do not only ordinarily coexist, but also embody internal ambivalences. *Transparency* is leveraged to generate or bypass trust but also generates loopholes that can aid *de-anonymisation*. *Online transparency* embodies a dichotomy between enabling *accountability* but also surveillance.[935] While in the IoM the issue is more pressing in public ecosystems, the issue mirrors a general feature of the Internet having a twofold impact on *anonymous* communication by providing ways to undermine *anonymity* but also enhanced techniques to *anonymise* relevant activities.[936]

The long-established debate between *financial privacy* and *transparency* shows how innovation only heightened a pre-existent complexity generated by opposing interests. Although the urgency to set balances between *anonymity* and *transparency* does not originate from DLTs, the IoM made it more pressing by unlocking new opportunities both for lawlessness and *accountability*. Thus, the interplay of the principles informing online communication, coupled with the non-binary nature of these principles, requires setting balances policy-wise also when "information" has a financial content. It follows that the only way to overcome clashes between *anonymity* and *transparency* traits is to agree on a desirable trade-off.

6.2.2. Managing the risk of overfitting: rules- and principles- based approaches

Recent literature on cryptocurrency regulation shows computer scientists, lawyers, economists, ethicists and sociologists trying to lay the foundation of a fruitful cooperation. Different knowledge domains often develop in silos, and they work together only when collaboration is perceived as a solution to a pressing risk. In this way, regulatory teamwork stems from urgency, which rarely prompts future-proof solutions. Likewise, *reactive* regulation is vulnerable to perceptive distortions and ideology-powered arguments, and the consequent regulatory process

[934] European Central Bank and Bank of Japan (2020)
[935] Herian R (2019), p 77
[936] Nicoll C, Prins JEJ, van Dellen MJM (2003), p v. Article 19 (2015)

may not adequately consider trade-offs and phenomenological differences. Current-day approaches should consider the diversity within the IoM and its ever-evolving character, to avoid establishing overfitting regimes structured in such an over-tailored fashion that there is no room for them to evolve if not by breaking the boundaries of the same framework. Differently put, especially in finance, "crisis-inspired rules should not become a dogma", and even if a sandbox provides interesting insights, it cannot replace regulatory reforms.[937]

The overall evolution of IoM-related regulation reflects the difficulties in fully grasping the deployed technologies and their socio-economic and legal impacts. It is complex to distinguish what is brought about by digital innovation and which disruptions are tied specifically to DLTs, just as it is not always easy to differentiate between the legal impacts of a DLT-based instrument and those of a similar one from a functional perspective but based on a different technology. The attention to taxonomy initiatives stemmed from leveraging the concept of token to bridge cross-disciplinary gaps. Although this could aid techno-legal communication through common references, the potential of cross-disciplinary initiatives is not (and should not be) limited to taxonomies. Growing attention is paid to the possibility to cooperate not only to define cryptoassets, but also to guide their development. In this context, expert techno-legal communities can have a *proactive* role in designing tools compatible with jointly agreed-upon values. Generally, this idea falls under the definition of "regulation-by-design", explored below.[938] The major opportunity offered by the token-based approach is the creation of a scheme for new ontological categories of assets, and ecosystems for their exchange, not limited to given domains. Appropriate structures must be devised for token creation and transfer, and they do not always correspond to (and/or are not considered) monetary and financial instruments.[939]

The issue of multiple regulatory approaches to cryptocurrencies is set within the broader context of different methodologies to mitigate risks and encourage innovation. A relevant distinction – well-known to the area of financial services regulation, albeit relatively new – is the one between *rules-based* and *principles-based* frameworks and compliance.[940] A rules-based regulatory style outlines detailed prescriptive provisions, while principles-based approaches focus on standards and rules stated broadly and oriented to the outcomes.[941] One could draw a parallel with the difference between Regulations and Directives under EU law. Nonetheless,

[937] Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), p 52
[938] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), p 2
[939] It is well-known that the widest types of information can be stored on DLTs (*e.g.*, value transactions, land titles, intellectual property rights) and this is to some extent mirrored by the token categories explored in Chapter 1.
[940] Carter RB, Marchant GE (2011), pp 157-165
[941] Black J, Hopper M, Band C (2007), p 191

even if the latter set goals that Member States choose how to reach, from a substantial perspective they often encompass detailed provisions as well. In real-world situations, frameworks usually feature a mix between the two approaches, and this is the case of the AMLD. Principles-based rules allow flexibility and are suitable when detailed schemes can generate a vicious cycle where gaps lead to new rules, which generate new gaps, prompting new rules, and so on.[942] This risk is rather a certainty in new technologies, and it is known as the risk of overfitting, where rules become technologically outdated soon after their entry into force or even before.[943] Hence, the idea of paying attention to the purpose behind a framework, rather than tailoring regulatory approaches to specific instances, could fit the IoM.

When considering the various and ever-evolving degrees of *anonymity* in the IoM, it seems unlikely a thoroughly rules-based scheme can be safe against the risk of overfitting. Measures to combat ML/TF/PF need to confront a variety of instruments and may only be unified by focusing on the objective the framework pursues (*e.g.*, forbid *anonymous* value exchanges by means of cryptocurrencies above a certain threshold, while cryptocurrencies feature different levels of *anonymity*). Nonetheless, it seems crucial to complement this methodology with more detailed and contextualised behavioural standards (*e.g.*, predefined ways to avert *anonymity*) to avoid loopholes and guarantee the *accountability* of the actors involved.[944] Against this backdrop, I argue a combination of rules-based and principles-based methodologies may prove conducive to meet the IoM both where it is now and where it will be in the forthcoming years.

In this respect, one of the goals of establishing cross-disciplinary collaboration mechanisms is to bridge the gap between the dynamism of innovative technologies and stringent rules-based approaches. Designing an efficient interplay of rules-based and principle-based reasoning, in fact, presents its shares of complexities. For instance, when regulators are asked to focus on their broader mandate, instead of deploying an "overly rule-based approach" that can hinder innovation and "overly stretch regulatory resources",[945] they are asked to develop a deep understanding of the process enabled by the given technology, which needs access to different types of expertise. Hence, while to foster harmonisation and limit overfitting one solution could be to adopt a mixed rules-based and principles-based methodology, this requires significant cross-disciplinary efforts to tie the framework to an actual understanding of the dynamics at hand.

[942] Ibid, p 193
[943] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), p 17
[944] Black J, Hopper M, Band C (2007), pp 200-201
[945] Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017), p 54

6.2.3. A critical outlook on the impacts of disintermediation on regulatory methodology

In Chapters 2 and 3 I argued a teleological analysis of IoM's *anonymity* in the intermediary-based AML/CFT/CPF sphere cannot overlook the notions of *accountability* and *auditability*. Although the IoM embodies the idea of "democratising" value exchanges, it has evolved into DeFi and techniques enabling *enhanced disintermediation* (*e.g.*, self-hosted wallets, DEXes). While DeFi is a non-technical term depicting an ecosystem of DLTs, smart contracts, *disintermediation* and open banking,[946] its applications pursue transparent and trustless financial services, without involving intermediaries.[947] Not surprisingly, DeFi and *enhanced disintermediation* disrupt traditional regulation, as *decentralisation* potentially "undermine[s] traditional forms of accountability and erode[s] the effectiveness of traditional financial regulation and enforcement".[948] Indeed, while regulated intermediaries are (arguably) "positioned so as to be able to prevent wrongdoing by withholding necessary cooperation or consent",[949] in P2P transfers no third-party cooperation or consent is needed. Thus, even without assuming these initiatives pursue illegal goals, they ostensibly do not fall within the recycle box, but rather within the sandbox category,[950] and sandboxes were set up in various jurisdictions.

In this respect, the nature of DEXes spurred regulatory suggestions that shift the methodology from CEX-based to more innovation-friendly scenarios. Arguably, in DEXes software is no longer "used" to run the exchange, but rather "is" the exchange. Indeed, DEX platforms consist of general-purpose open-source software and resemble more online service providers (OSPs) than CEXes. Since software sets prices and transfers assets between buyers and sellers, the system can be (mis)used as users wish: what happens on the protocol depends on the users. From this perspective, the question arises on how to counteract harmful effects, also in terms of tracking and fighting illicit activity.[951] To avoid the use of regulation designed for *centralised* FIs, it was suggested to apply the "safe harbour" approach of the DMCA's,[952] whereby under some conditions OSPs are not liable for the actions of users interacting on their platforms.[953] Likewise, the "notice and takedown" methodology could be used for illegal content listed on DEXes, instead of stimulating developers to avoid self-regulation out of fear of being

[946] Zetzsche DA, Arner DW, Buckley RP (2020), p 173
[947] BitKom (2020). Referenced by Zetzsche DA, Arner DW, Buckley RP (2020), p 173
[948] Zetzsche DA, Arner DW, Buckley RP (2020), p 172
[949] Brummer C (2019), p 384
[950] Maupin JA (2017)
[951] Altschuler S (2022), pp 92-94 and 99
[952] Digital Millennium Copyright Act: 17 U.S.C. § 512. The "safe harbor" regime offers immunity from claims of copyright infringement if OSPs block access to infringing materials when notified. Zimmerman M (2017)
[953] Altschuler S (2022), p 99

classified as exchanges. Decentralised protocols should be shielded from liability to allow them to delist blacklisted DeFi tokens when they are reported.[954]

Here, self-regulation is a component of a "regulation designed for DEXes". Reportedly, CEX-based AML/CFT/CPF regimes waste resources over problems solved by technology, while driving *traceable* activities towards *untraceable* worlds.[955] Accordingly, "direct legal regulation" could be used to ensure regulated entities deploy monitoring systems that, as outlined in Chapters 3 and 4, are provided by private companies. The regulatory goal is to establish a reporting and surveillance system, and the primary tool for regulating DEX protocols is "code", while the law supplements it when the architecture falls short. Indeed, while it is not possible for code alone to hinder the (mis)use of DEXes, the use of RegTech solutions can be ensured by regulators contracting directly with service providers. Hence, the role of regulators is to ensure technology is used and reports are filed when needed.[956]

Nonetheless, I previously argued how *disintermediation* in the IoM is not as clearcut as it may seem. The sphere is populated by both traditional and novel intermediaries, even if the latter are not always within the reach of regulatory efforts either by regulatory decision (*e.g.*, crypto-to-crypto exchanges in the 5AMLD) or forced by the circumstances such as (perceived or actual) lack of enforceability (*e.g.*, DEXes). Moreover, while a certain bewilderment is warranted by (some of) the *enhanced disintermediation* applications, I argue that when benchmarks have already been set in the AML/CFT/CPF domain, even when *disintermediation* clashes with active cooperation there might be no reason to overlook long-established principles.[957]

Illustratively, if the application of the RBA led to limit volume-wise transactions involving *anonymous* instruments, such as cash or bearer shares, the same reasoning can be applied to cryptocurrency transfers. A teleological approach – *i.e.*, focused on what risks the framework tries to mitigate – leads to establishing equivalences. An example of this concept can be found in the text of the upcoming MiCA Regulation, stating "Union legislation on financial services should be guided by the principles of 'same activities, same risks, same rules' and of technology neutrality".[958] Indeed, in the EU regulation of financial markets, the principle "same activity, same risks, same regulation" is typically accepted to minimize regulatory arbitrage.[959] Arguably, similar considerations inform FATF's position on non-custodial wallets and P2P transfers

[954] Ibid, p 102, which refers to Antonopoulos A (2021)
[955] Ibid, p 107
[956] Altschuler S (2022), p 110 and 112-113
[957] This may be different from a policy-making perspective, as different choices are always possible.
[958] Council of the European Union (2022a), Recital 6
[959] Katona T (2021), p 94

and the related unacceptably high risks in case of mass-adoption. Accordingly, national legislators may decide to ban or deny licenses to platforms operating with self-hosted wallets, or to set transactional/volume thresholds for P2P transfers, or also to mandate VASP/FI involvement.[960] Another possible equivalence concerns EU provisions on "e-money". Against the background of *anonymity* being a risk factor as per Annex III AMLD, the approach is to ease CDD for cases of low risk. While Member States can outlaw payments via *anonymous* prepaid cards, Article 12 AMLD provides conditions to simplify CDD duties for e-money. Among other provisions, it outlines a transaction limit of EUR 150, a maximum storage allowance and the impossibility of reloading the instrument via *anonymous* e-money, provided the transactions/business relationship are monitored adequately to detect suspicions.[961] The application of similar rules to IoM activity may reduce gaps between value exchanges.

Meanwhile, despite its overall *decentralised* layout, DeFi features power *reconcentration* in parts of its value chain, albeit less regulated and transparent.[962] Regulation may evolve according to phenomenological developments, and effective oversight and risk control would be provided if regulation were to target the part of the value chain that is *reconcentrated*.[963] While the context is not equal to that of the IoM, I argue this reasoning is relevant to the latter as well.

6.2.4. Identifying the risks: rules-based indicators

As emerged in Chapter 4, the RBA is the background against which AML/CFT/CPF measures are implemented. Its flexibility allows compliance strategies to be devised that are proportionate to the specificities of regulated entities, but thrusts on the latter cumbersome evaluations. To guide efforts and aid compliance, as addressed in Chapter 3 various layers of risk assessments and anomaly indicators are issued to clarify benchmarks. Chiefly, they provide instructions on the application of enhanced CDD measures in specific circumstances. These indicators are published by different stakeholders, such as international and supranational institutions (*e.g.*, FATF, EC, EBA), national legislators and regulators, supervisory, investigative and enforcement authorities (*e.g.*, FIUs). Building on the interpretation of these indicators, each regulated entity retains the obligation to apply RBA-based measures from a concrete perspective.

[960] Financial Action Task Force (2020), p 15
[961] Article 12(1) of the AMLD, as amended.
[962] Zetzsche DA, Arner DW, Buckley RP (2020), p 172. Indeed, among DeFi projects "the degree of decentralisation varies from protocol to protocol" (Zunzunegui F (2022), p 9).
[963] Ibid, p 172

In the IoM, just as in the traditional financial system, not all entities, tools, and stakeholders embody the same level of risk. According to the RBA, this consideration shall inform the design of regulatory and compliance responses not only from the standpoint of regulated entities. Indeed, the regulatory treatment must be tailored to the different degrees of danger to the integrity of the financial system, in line with the principle of proportionality.[964] Illustratively, EU Member States are required to consider the AMLD, EC's risk assessments and other supranational authorities' guidelines not only when transposing Union law into domestic legislation, but also when designing implementation strategies and drafting national risk assessments. In Chapters 3 and 4 I contextualised red flag indicators as an integral part of the RBA.

In this respect, as explored in Chapter 3 it is common practice for regulated entities to deploy RegTech solutions to screen their operations and detect anomalous activities in an automated way. Mandatory transaction monitoring procedures are often grounded on these tools, that in turn heed the red flags of regulators. For IoM-related operations, these software solutions are offered by blockchain analytics companies. Based on the alerts provided by these systems, the entity investigates the activities to decide whether to activate internal escalation procedures so that the competent person – usually, the Money Laundering Reporting Officer (MLRO) – can determine whether to submit an STR under the conditions outlined in Chapter 4. In this respect, RegTech applications perform the process of anomaly detection outlined in Chapter 3, to single out rare or suspicious events in terms of them being significantly different from the datasets.[965]

Red flag indicators are usually provided in rules-based format, which means they are phrased as templates of sequences of actions that suggest a suspicion, and are drafted in a way that is self-explainable, as required for auditing purposes. They are the basis of transaction monitoring solutions, whose alerts and hits are generated through a process of rule-matching – *i.e.*, they are produced when the system matches a given occurrence with one of the "rules" identified as suspicious. For instance, a rule may be set in a RegTech application to flag all transfers of an amount that exceeds by 30% the average amount of the previous transactions performed by the same customer. Thus, if a situation of the sort arises, the system would match the occurrence with the rule, and flag the transfer accordingly.

Indeed, transaction monitoring solutions were defined as "predominantly rules-based thresholding protocols tuned for volume and velocity of transactions with tiered escalation

[964] Zetzsche DA, Buckley RP, Arner DW, Barberis N (2017), p 53
[965] Kamišalić A, Kramberger R, Fister I (2021). Li Z, Xiang Z, Gong W, Wang H (2022). Shayegan MJ, Sabor HR, Uddin M, Chen CL (2022)

procedures".[966] Hence, the preliminary review of a flagged transfer usually relies on "suspiciousness heuristics" – *e.g.*, political exposure, geographical dynamics, round numbers, transaction type and properties, behavioural logic –,[967] as enshrined by the indicators. Chief reference is to those outlined in Chapters 3 and 4, issued by FATF in 2020 with regard to VAs. The indicators were developed from an analysis of more than 100 case studies dated from 2017 to 2020 and include a section of *anonymity* that depicts vulnerabilities related to the technologies embedded in the cryptocurrency or service provider, or to the ecosystem itself.

The debate on the respective merits of rules-based and principles-based standards is heated for accounting and auditing standards, where it was argued there is insufficient acknowledgment that the format of the standards affects their content. This is because the more effort is required, the more complex it is to comply without guidance and exceptions.[968] Likewise, rules-based auditing generates audit processes that are relatively uniform, unscalable and significantly redundant, while in principles-based audit efforts can be targeted to higher risks.[969] The debate chiefly concerns accounting standards and pivots on the difference between those issued by the FASB (more rules-based) and those issued by the IASB (more principles-based). In this context, rules-based standards are criticised because they encourage "check-box" thinking – *i.e.*, formal compliance with detailed criteria instead of substantial compliance, unsuitable to the complexity of the financial environment. On the other hand, the vagueness of principles-based standards requires expertise, leaving room for misinterpretation and inconsistencies.[970]

Against this backdrop, I argue that also in the AML/CFT/CPF the regulatory methodology and the style used to draft risk indicators are key elements. I provide here two examples of rules-based red flags: (i) with regard to transaction patterns: "incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency"; (ii) with regard to anonymity: "moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin".[971]

Red flag indicators, drafted by experts and reflecting their opinions, operate as empirical measures of AML/CFT/CPF risk. Likewise, they aim to provide a structure to think about these risks. In principle, they should provide clear benchmarks and their structure should be able to

[966] Weber M, Chen J, Suzumura T, Pareja A, Ma T, Kanezashi H, Kaler T, Leiserson CE, Schardl TB (2018), p 3
[967] Ibid, p 3
[968] Benson GJ, Bromwich M, Wagenhofer A (2006), p 185
[969] Sin YF, Moroney R, Strydom M (2015), p 282
[970] Ibid, p 283. In any case, the prescriptiveness of auditing standards was argued to be highly influential on the audit's procedure and results
[971] Financial Action Task Force (2020d)

accommodate the development of new indicators as the sphere evolves. Nonetheless, the content of rules-based indicators is often less straightforward and more ambiguous than what it seems. Moreover, depending on the link with empirical findings (*i.e.*, the phenomenological aspect highlighted in Chapter 1) they may feature little normative content, and be for the most part descriptive. In addition, there can be considerable gaps between the indicators and best practices deployed in the industry (*e.g.*, crypto travel rule debate).[972] In this respect, I believe the creation of a "transposition model" between red flag indicators and techno-regulatory standards could help clarify their meaning and streamline their application at the regulated entity-level. This could happen in the framework of the role of the AMLA. I argue their implementation could be eased by developing the standards with the private entities offering IoM-related analytics services and sharing them in an open-source format. I elaborate more on techno-regulatory standards and on a possible regulatory methodology below.

In practice, a considerable amount of time and human resources are needed to review the alerts generated by the rule-matching process. Tiered escalation procedures involve multiple layers of analysts deciding whether to escalate the item up to the MLRO. Because an alert can be a true or a false positive, rules-based systems have the advantage of interpretability, but their simplicity produces many false positives, estimated at around 95–98%.[973] Indeed, the discovery of patterns is demanding, and transaction datasets are massive, dynamic, high dimensional, complex from a combinatorial perspective, non-linear, as well as often fragmented, inaccurate, incomplete, or inconsistent, while the difficulty to automate the synthesis of information from different data streams leaves the task up to human analysts. Hence, a vicious circle stimulates over-reporting due to the cost asymmetry between false positives and false negatives.[974] The insufficiency of rules-based systems suggested the automation of an increasing array of processes, where machine learning-based methodologies are deployed and investigated in conjunction with forensic approaches.[975] Notably, as explored in Chapter 3 the combination between transaction graph analytics and machine learning is increasingly deployed in the AML/CFT/CPF domain for transaction classification purposes. Indeed, the supervised activities involve transaction flow relationships between entities, which creates a graph structure helpful for classification and to which specific algorithms can be applied.[976]

[972] In this regard, they share features with rules-based indicators in governance: Kaufmann D, Kraay A (2008)
[973] Eddin AN, Bono J, Aparício D, Polido D, Ascensão JT, Bizarro P, Ripeiro P (2021)
[974] Weber M, Chen J, Suzumura T, Pareja A, Ma T, Kanezashi H, Schardl TB (2018)
[975] Oad A, Razaque A, Tolemyssov A, Alotaibi M, Alotaibi B, Zhao C (2021)
[976] Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022)

6.2.5. Ranking the risks: the value of taxonomies

The evolution of the IoM calls for increasingly complex RegTech solutions due to the great quantity and complexity of transaction data to be processed. Considering the *enhanced disintermediation* trend, regulated entities and LEAs need to analyse a growing number of transactions vis-à-vis sophisticated *obfuscation* techniques and without the assistance of regulated counterparties.[977] In this context, it is important to devise tools to aid compliance and reduce over-reporting.[978] Building on the need to provide future-proof benchmarks to enable communication between regulation and technology, and possibly automatic application and enforcement, I argue a method worth exploring is a taxonomy that provides yardsticks to evaluate different levels of *anonymity* risk posed by different cryptocurrencies and/or ecosystems.

Although it may seem odd for a taxonomy to be future-proof and mitigate the risk of overfitting, I believe its design can merge principles-based and rules-based methodologies. This instrument comes to mind because of the use made for tokens, overviewed in Chapter 1, where taxonomisation showed its capacity to merge flexibility with precision. Indeed, the token is used as a benchmark to bridge cross-disciplinary gaps and merge different understandings to reduce regulatory uncertainty. One of the most compelling aspects of such a framework is to provide experts with different backgrounds with a common frame of reference to work on and build a body of knowledge. I believe a taxonomy that categorises cryptocurrencies and ecosystems according to their level of *anonymity-related* risk would prove useful. Nonetheless, because the concept of *anonymity* is socio-technical, it remains to be explored whether all – or a significant number of – these risks can be effectively modelled in a taxonomy fashion.

As outlined throughout this work, in the IoM the *anonymity-transparency* interplay pertains to different dimensions, and several ambivalences stem from the background against which the IoM has developed (*e.g.*, online communication, financial sphere). The multi-layered complexity of IoM socio-technical ecosystems suggests the adoption of a teleological approach to develop a conceptual understanding of both their nature and their regulatory consequences. Accordingly, I argue a valuable approach entails: (i) conceptualising the different trade-offs between, on one side of the spectrum, *anonymity* and *privacy* and, on the other side, *transparency* and *auditability*, that exist in the IoM; (ii) leveraging the RBA to develop an understanding of the AML/CFT/CPF risk featured by various use cases; (iii) designing a taxonomy-based

[977] *E.g.*, in the context of CDD or investigations on transactions originating from or destined to unhosted wallets or processed by DEXes
[978] Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022)

framework to classify IoM ecosystems according to this risk, in combination with techno-legal reasons that ground the classification (*i.e.*, parameterised criteria); (iv) leveraging the findings to establish a regime of techno-regulatory standards featuring a "[regulation/compliance]-[by/through]-design" approach. The next two sections explore the last element.

6.3. From "Code is Law" to "[Regulation/Compliance]-[by/through]-Design"

As outlined in Chapter 4, the AML/CFT/CPF approach to the IoM remains moulded on the gatekeeper-based model even after the advent of cases of *enhanced disintermediation*. Meanwhile, the implementation of the crypto travel rule raises multi-dimensional issues, and the industry declares to be lacking the technology to comply. In other words, despite the efforts of analytics companies, the sector has yet to develop an adequate RegTech solution. In this context, a key challenge is posed by transactions involving self-hosted wallets.

The idea that information on originators and beneficiaries must be collected and accompany cryptocurrency transfers – as it ordinarily happens for wire transfers – explicitly aims to avert *anonymity*. In this situation, a technology-powered solution (cryptocurrency transfers) is (purportedly) unable to comply with a piece of regulation (FATF's travel rule), because of a technological gap (no effective tool). This gap, however, stems from a (partial) misalignment between regulatory provisions and the phenomenology of the targeted domain. Evidently, other factors hinder the application of the crypto travel rule. Not only VASPs/FIs may not possess, or have adequate procedures to collect, the *identity*-related information to be submitted to the counterparty, but some of this data may not exist or it may not be possible to collect it.

But how can the growing cases of *non-centralisation* and *disintermediation* be addressed by AML/CFT/CPF? As outlined in the previous chapters, not only is the IoM permeated by methods to *obfuscate* flows, but intermediary-based regulatory efforts are hindered when transactions do not involve regulatable entities – *e.g.*, in a transfer between two self-hosted wallets what stands between the parties is just technology. In this context, the challenges in implementing the crypto travel rule shed a thought-provoking light on the interplay between technology and regulation. The effectiveness of active cooperation is vulnerable to criticism, and the value of tech-sensitive regulation was underlined.[979] Regulators shall develop ways to consider the features of these ecosystems and deploy a *proactive*, rather than *reactive*, model. I suggest a regulatory and compliance approach that is not new but modified to fit the IoM sphere.

[979] De Filippi P, Wright A (2018). Zetzsche DA, Arner DW, Buckley RP (2020), p 180

6.3.1. When the "law" meets "code", perhaps on a blockchain

The starting point is the widely known, and criticised, "code is law" maxim, put forward in 1999 by Lessig to depict the regulatory impact of "code" in the cyberspace as part of the founding arguments of the New Chicago School.[980] In his words, "the software and hardware (*i.e.*, the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is".[981] The concept was framed by Reidenberg under the label of "lex informatica", and soon extended into "law is code".[982] Accordingly, "code" complements law in its regulatory action, which leads to focus on how predefined regulatory elements can be built into technology.[983] This does not imply code "replaces" or "displaces" law, but that it exerts a "normative influence" on individual behaviours – *e.g.*, impact of software on user behaviour.[984] It does so in combination with other three factors: market dynamics, law itself, social norms.[985] The concept of regulation comes to include these four aspects.[986] In Lessig's words, it is possible to build the cyberspace to protect values deemed fundamental, or to design it not to uphold them. The issue is unavoidable as any choice includes "some kind of building. Code is never found; it is only ever made, and only ever made by us",[987] thus it is crucial to decide which values to embed.[988]

In this context, the idea of "code is law" developed towards the "law is code" argument that "law itself can be codified and defined as technological code".[989] The notion that code can control cyberspace behaviour *ex ante* or *a priori* (*i.e.*, before the fact) gave birth to notions such as "lex cryptographica" and "cryptolaw",[990] and originated a series of debates that evolved into

[980] Lessig L (1998). Lessig L (1999). Lessig L (2006)
[981] Ibid, pp 4-5
[982] Reidenberg J (1998). For an overview of related research: Werbach (2019), pp 149-173
[983] Hassan S, De Filippi P (2017)
[984] In this context, regulation was defined by Black as "the intentional use of authority to affect behaviour of a different party according to set standards, involving instruments of information-gathering and behaviour modification" Black J (2002), p 1, referenced by Finck M (2019a), p 145
[985] Lessig L (1998). Lessig (1999). Finck M (2019a), p 39. Lessig "did not say "Code always disrupts law" or "Code is superior to law." His point was that software code and legal enactments are both mechanisms that can govern human behavior. Code is a form of law…and not necessarily the best one" (Werbach (2019), p 153). Indeed, "one of the most important lessons from Lessig's analysis was that law and code are not binary alternatives" (Ibid, p 156).
[986] Lessig L (1999). This generates the theory of the "pathetic dot" (De Filippi P, Wright A (2018), p 173)
[987] Lessig L (2006) Books, p 6
[988] Brown I, Marsden Christopher (2003), p 303, referenced by Finck M (2019a), p 39. Accordingly, technology should be studied as a regulatory modality coexisting with the others (Werbach (2019), p 153). Following this reasoning, the role of the law expands, regulating behaviour both directly and indirectly (and modern regulation is a mix), by regulating other modalities of regulation (Lessig L (1998), p 666)
[989] Möslein F (2019), p 277, referring to De Filippi P, Hassan S (2016)
[990] Differences emerged among these notions. "Lex cryptographica" distances itself from Lessig's "code is law" and other code-based regimes because it inherently operates on an autonomous basis, independently from centralised authorities (De Filippi P, Wright A (2018), p 207). "Cryptolaw" is a new type of accessory legislation and jurisprudence emerged when DLTs implement and deliver law (Reyes CL (2017), p 399). Crepaldi M (2019)

the controversial "code as law".[991] Indeed, "regulation by code" was argued to allow the formalisation of contractual agreements into self-executing and self-enforcing predetermined code-based rules,[992] and blockchain technology, mostly through smart contracts, was seen as an enabler of an "order without law" built on private (self-)regulatory frameworks.[993]

It was argued "law" and "code" are in a synergic relationship of extraordinary complexity, where code can implement self-regulation and reinforce or undermine public regulation, while law can subvert or strengthen code. I believe it is interesting to focus on the intertwined and mutual relation between regulation and code,[994] as it perfectly exemplifies the way in which technology can interact, communicate, and evolve with regulation, as well as be designed accordingly. Evidently, negative impacts can be produced as well, and code can be leveraged to escape regulatory constraints, which reminds of cyberlibertarians. My argument pivots around the dynamic between code and regulation, and it allows me to argue in favour of the joint development of these two crucial building blocks of today's world, thus mitigating the risk of their siloed development. By no means do I support equating the concepts of code and law.[995] Indeed, what is relevant to this research is that, starting from "law is code" arguments, *design-based* techniques were devised to pursue socio-legal outcomes through embedding legal principles and values into technology, thus fostering cross-disciplinarity. Accordingly, even if hyperbolic statements such as "code is/as law" are not to be interpreted literally, the inter-relationship between "law" and "code" has laid the conceptual groundwork for valuable notions such as *embedded regulation* and *embedded supervision*, still explored to this day.[996]

Ostensibly, code – as a primary component of the broader concept of the "design" of a given application – enables regulation and compliance to be approached in a *proactive* way, replacing "command and control" techniques with a *design-based* methodology where compliance is *embeddable*.[997] Building on RegTech tools, these techniques require preliminary standard setting. Hence, the assumption is that regulators can convert obligations – and, as outlined in detail below, also the way and methods to achieve compliance with them – into code that can be used for a given application to *comply by design*.[998] The idea that compliance can be

[991] Hacker P, Lianos I, Dimitropoulos G, Eich S (2019), pp 22-23. Wright A, De Filippi P (2015). Yeung K (2019)
[992] Hassan S, De Filippi P (2017), pp 88-90
[993] In using these concepts in this work, I acknowledge the interplay between "rules", "code" and "law" generated considerable controversy, and that the legal and ethical challenges of "regulation by code" were widely explored with regard to blockchain and machine learning. These elements, however, fall outside the scope of this work.
[994] Finck M (2019a), p 39
[995] "The equation between code and law (and of law and Code) is debatable at best" Möslein F (2019), p 275
[996] Auer R (2019). Zetzsche DA, Arner DW, Buckley RP (2020)
[997] Nabilou H (2019). Pocher N, Veneris A (2022b). Yeung K (2017)
[998] Schrepel T (2021), pp 44-45. Pocher N, Veneris A (2022b)

streamlined into a design process developed from the concept of *privacy by design* put forward in 2011, later evolved into compliance "by" or "through" design explored below.[999] I believe that, provided a few important limitations are borne in mind, embedding compliance can be a fitting methodology in a situation of *enhanced disintermediation*.[1000]

Meanwhile, the possibility to exert impacts on these systems through technology relies on stakeholders to develop ways to do it effectively vis-à-vis the major power dynamics between the actors involved. In CBDCs, as highlighted in Chapter 5, a method is PPPs, where public entities cooperate with the industry that owns the skills to develop technological tools. CBDCs, however, are obviously not an example of *enhanced disintermediation*, which means any equation must be approached with care. In this sense, I believe the value of effective technology-based tools to comply with regulation is most noteworthy. It is seemingly a power of technology spilling into the regulatory world. This power, however, can pursue regulatory objectives through predefined procedures and an adequate understanding of the techno-legal context.

6.3.2. Placing the debate within the IoM domain

Lessig argues that governance and commerce are shaping the cyberspace in ways very distant from its original architecture, allowing control and efficient regulation, thus challenging essential liberties.[1001] In this sense, the argument is related to the IoM evolution, where the hype over time left room to *(re)centralisation* tendencies. In this respect, the DeFi space provides insights on how to extend regulatory safeguards to the IoM. A few methodologies appear disruptive because of their proactiveness in terms of interplay with technologies. In the early phase of the exploration, reference was to supervisory mechanisms, in the form of *embedded supervision – i.e.*, "an automated form of compliance, monitoring, and supervision, using the system itself to implement, monitor, and enforce compliance requirements".[1002] Going beyond supervision, the reasoning spilled into *embedded regulation*, and DeFi offers the chance to design regulation in a new way, where "regulatory approaches could be built into the design of DeFi, thus potentially decentralising both finance and its regulation, in the ultimate expression of RegTech".[1003] This methodology appears helpful in *non-centralised* systems.

---

[999] Casanovas P, González-Conejero J, De Koker L (2018). Cavoukian A (2011). Torra V (2017). Auer R (2019)
[1000] See below for an analysis of the interplay between *embedded regulation* and *embedded compliance*, as well between *regulation by design* and *compliance by design*
[1001] Lessig L (2006), pp 4-5
[1002] Zetzsche DA, Arner DW, Buckley RP (2020), p 202. Auer R (2019)
[1003] Zetzsche DA, Arner DW, Buckley RP (2020), p 172

Embedded regulation appears even more valuable when considering AML/CFT/CPF RegTech solutions,[1004] where the use of technology is well-established, and developments are promising. To fully reap the benefits of these efforts, regulators, partnering with the industry, could develop technology-based systems and *embed* regulatory objectives through *ad hoc* compliance strategies. The technology-based trait of a regulatory approach can refer to a type of regulation that either (i) uses a specific technology as benchmark (*i.e.*, it targets all implementations of a specific technology), or (ii) targets technology as regulatory tool (*e.g.*, regulation-by-design). The term is here used as sub (ii), which means I do not necessarily herald the use of DLTs as benchmarks without a complementary focus on other cases.

The way through this process is not straightforward. I believe a pivotal aspect is building on existing initiatives to capitalise on efforts to bridge gaps and discrepancies between terminologies and knowledge sets. Evidently, *proactive* regulation needs a dialogue with the industry that is hands-on developing projects based on these technologies, as well as with stakeholders that are already offering RegTech applications that leverage their extensive IoM-related datasets. Cross-disciplinary communication to set up common frameworks (*e.g.*, taxonomies, definitions of core concepts) and benchmarks (*e.g.*, tokens) can thus lead the way to approaching the regulation of technological evolution not only *ex post*. Evidently, this type of collaboration is viable when communication between different stakeholders is feasible – *e.g.*, it is hard to picture a co-operation between AML/CFT/CPF regulators, forensic companies, and AEC developer communities. Nonetheless, the establishment of common languages may lead to a techno-legal mutual awareness of the impacts of a specific implementation (*e.g.*, dark box, recycle box, sandbox), thus possibly informing more inclusive regulation and policy making.

6.3.3. Towards a flexible understanding of "code is/as law" and "law is/as code"

As mentioned above, experts elaborated on the "code is law" and "law is code" paradigms and developed the concepts of "code as law" and "law as code". Accordingly, governments tried to transpose regulation into smart contracts or embed it directly into information systems, to generate automated enforcement that does not need constant monitoring.[1005] Indeed, it was suggested to shift the regulatory focus from "code is law", where code is used to implement rules, to "code as law", that relies only on technology to define and implement law. Reportedly,

[1004] *E.g.*, Lootsma Y (2017). Yeung K (2019). Arner DW, Zetzsche DA, Buckley RP, Barberis JN (2019)
[1005] The "rules as code" movement took place from 2018 in Australia, Canada and France, and leverages computer languages to aid drafting and implementation of legal provisions. Other movements are "better rules" and "legislation as code". Casanovas P, de Koker L, Hashmi M (2022), p 66. Goldbarsht D, de Koker L (2022), p 7

this approach could ensure compliance by embodying requirements into code-based systems, through a mechanism that enables a transaction only if it satisfies the logic embedded into code.[1006] Although the strategy could seem efficient, from a conceptual standpoint I do not agree with a strict equation between "law" and "code" to promote interventions on code itself to reach technical *accountability*. As noted in the literature, the code-based approach is tainted by lack of flexibility, and the regulatory action of code is useful only for objectively verified rules that can be defined in the code itself, while the formality of translating legal rules into code-based rules can enable people to bypass regulation exploiting the rigidity of the system.[1007] It is for this reason I prefer referring more broadly to "design", although in the domain at hand design models usually include coding as a key component.

In this sense, among the manifold challenges posed by the combination of legal and technical trust in blockchain governance, the chief difference between cryptography and law stems from the distinction between human-to-human expression and computer programming. It is impossible to reduce the law to objective rules, but only portions of it. Reportedly, "hard-edged, cryptographically secured code can never fully encompass human intentions".[1008] Indeed, law is dynamic and does not only consist of reading predefined codes, while DLTs' cryptography is inherently expressed in finite systems.[1009] From this perspective, "the world is often too complex to be put into code", and the value of automation lies more in simplifying a contract's execution than in trying to automate all complexities.[1010]

Nonetheless, I believe successful IoM regulation requires a combination between the law and the mechanisms underlying technologies.[1011] In the IoM, architecture shapes behaviour or grants the power to shape it, which means "poorly designed code can be as harmful as poorly designed law".[1012] Hence, I believe code plays a role worth exploring within design models, but I see no need to even try to pursue an equation with the regulatory role of the law. While I cherish the concept of embedding compliance with rules, and thus the value of devising rules that can be complied with through embedded mechanisms, the focus of my argument is on the

[1006] De Filippi P, Wright A (2018), pp 196-199
[1007] Ibid, p 200
[1008] Werbach (2019), pp 221-222. In this context, "some rules and regulations are particularly suitable for formalisation into the language of code. This is particularly true with laws containing rules that are both straightforward and unambiguous […]" (De Filippi P, Wright A (2018), pp 195-196)
[1009] Werbach (2019), p 222
[1010] Auer R (2022), p 19
[1011] Werbach (2019), p 203. As argued by the author, the fact that smart contracts do not require legal enforcement (if this is the case) does not render the law irrelevant, rather calls developers to study the law to understand where code and cryptographic solutions can match the functions of legal practice. Both "governance by code" and "law" have their own flaws; there is a need to draw from both.
[1012] Ibid, p 233

communication and mutual influence between technology and regulation, and less on their respective regulatory traits. The relationship between the two was explored in many ways. The "ex-ante law is code" approach – based on converting legal rules into code to have users comply by design – is risky because it affects smart contracts directly. Thus, the less intrusive "ex-post law is code" was suggested, while ways are investigated to make "law more code-like" and "code more law-like".[1013] Indeed, "the simplest way to make blockchain-based systems more consistent with legal enforcement is literally to connect the two".[1014]

In this sense, a valuable reference can be made to Ricardian Contracts, that proposed to "identify and describe issues of financial instruments as contracts".[1015] They are text files readable by people and parsable by programs and define a type of value for its issuance over the Internet, by identifying issuer/signatory, terms and clauses.[1016] Their background is that smart contracts are used "to translate certain legal contractual terms and conditions of services they offer into safe-to-execute code".[1017] However, the specificities of legal contracts and the multi-layered (*e.g.*, domestic, supranational, international) and cross-disciplinary (*e.g.*, civil, criminal, administrative) set of regulations they have to comply with challenges their deployment as such. Indeed, "contract" is a specific notion in the legal world, specified by the different legal systems and jurisdictions, and legal wording references implicitly and explicitly to elements of the broader legal framework(s). On the contrary, a smart contract consists of software executed automatically when programmed conditions are met, translating "fragments of the legal prose of a contract into an executable piece of code".[1018] Although the extensive literature on the legal status of smart contracts and their regulatory impact falls outside the scope of this work,[1019] the role of standardisation in the establishment of a common techno-regulatory methodology emerges from analysing how the *intelligibility* of the legal wording must be safeguarded not to incur claims of the contract being void or voidable.[1020]

A Ricardian Contract has three components: (i) legal code, a human-readable text of the contract, (ii) computer code, the executable smart contract, (iii) parameters/variables affecting

[1013] Schrepel T (2021), pp 44-45. Werbach (2019), pp 203-223
[1014] Ibid, p 212
[1015] Ibid, p 212. The author refers to Werbach K, Cornell N (2017), pp 101–170. Grigg I (2004). The concept was introduced by Grigg I (2019-2000)
[1016] Grigg I (2004) *Parsable* means "programs can convert it into internal forms for searching for name-value pairs"
[1017] Cervone L, Palmirani M, Vitali F (2020), p 1. Murphy S, Cooper C (2016)
[1018] Cervone L, Palmirani M, Vitali F (2020), p 1782
[1019] Some jurisdictions provide them with a clear legal status and enforce their life-cycle. They can be enforced internationally if compliant with UNCITRAL's conditions (Cervone L, Palmirani M, Vitali F (2020), p 1782)
[1020] The key issue of the unequivocal and free willingness to accept the terms of smart contracts shows the value of intelligibility and readability by humans and machines. Ibid, p 1782

its execution. To properly link legal and computer code the cryptographic hash of the computer code is included into the legal code, and that of the legal text is included into the computer code.[1021] Weaknesses of Ricardian Contracts were addressed by initiatives such as the "Smart Contracts Templates" and the "Intelligible Contract", where the latter maps into the operational code the whole text of the legal contract.[1022] Relatedly, a recent study analyses smart contract challenges under the lens of their deployment in the EU and impacts on the Digital Single Market.[1023] It puts forward the "Law + Technology" methodology to encourage their development, and I believe it can be useful to handle IoM challenges, dynamics and value exchanges.

In this field, a branch of legal informatics known as "computational law" ("Complaw") focuses on bridging the gap between legal knowledge/reasoning, natural language, and machine-readable formats (*e.g.*, through formal semantic representation).[1024] Its primary focus is "compliance management", that aims to develop computer systems that can assess, facilitate, or enforce, compliance; Complaw pursues to apply regulations without additional human input.[1025] In particular, experts focused on trying to solve the problem of using standard technologies for the implementation of the abovementioned Intelligible Contract leveraging solutions already exploited in the legal domain – *e.g.*, the Akoma Ntoso standard, an XML OASIS standard for modelling legal resources, and the LegalRuleML standard, an OASIS standard that consists of an interchange language for legal rules both human- and machine-readable.[1026]

6.3.4. "[Regulation/compliance]-[by/through]-design" in the IoM

A literature review of *design-based* methodologies shows a dichotomy between "regulation by design" and "compliance by design". Indeed, the notions refer to two distinct perspectives.

[1021] Werbach (2019), p 212. The author refers to Werbach K, Cornell N (2017). Grigg I (2004)

[1022] Cervone L, Palmirani M, Vitali F (2020). An Intelligible Contract is "a unique collection of linked machine-readable resources describing a legal contract, its legal prose, its legal context, and information on which parts of it can be automatically processed and how to do it". Mandatory components are (i) identification and referencing, (ii) document, (iii) context, (iv) process. Legal documents must be structured to preserve the logical and semantic structure of the text, serialised through standard technologies and linkable to other resources (Ibid p 1784).

[1023] Schrepel T (2021)

[1024] Athan T, Governatori G, Palmirani M, Paschke A, Wyner A (2016). Cervone L, Palmirani M, Vitali F (2020). Genesereth M (2015). Surden H (2012)

[1025] Genesereth M (2021)

[1026] AkomaNtoso was applied in legal and non-legal contexts (*e.g.*, modelling laws, legal changes, documents). It comprises an XML vocabulary to structure legal documents and a naming convention to identify legal resources; it supplies an informal ontology to identify entities and link them to portions of the legal text. The LegalRuleML standard allows to re-express legal prose and connect business rules to automatic legal reasoners. Cervone L, Palmirani M, Vitali F (2020) p 1785. The authors cite: Palmirani M, Vitali F (2011). Palmirani M (2011). Peroni S, Palmirani M, Vitali F (2017). Dimyadi J, Governatori G, Amor R (2017). Palmirani M, Sperberg R, Vergottini G, Vitali F (2018). Vitali F, Palmirani M, Parisse V (2019). Vitali F, Palmirani M, Sperberg R, Parisse V (2018). Palmirani M, Governatori G, Athan T et al (2017). Athan T, Governatori G, Palmirani M, et al (2014).

On the one hand, "regulation by design" focuses on shaping *regulation* starting from a *design-based* perspective. On the other hand, "compliance by design" refers to a compliance process grounded on *embedding compliance* into the design of a given tool.[1027] Hence, the wording "regulation by design" is imprecise when used to refer to compliance measures and not to the regulatory process at the roots of compliance. It follows that it is important to ponder whether in certain cases *embedded regulation* may be more correctly rephrased as *embedded compliance*, when it pinpoints the elements embedded into the given application as a set of tools that aid, and aim to ensure by design, compliance with the regulation.

Nonetheless, regulation can be drafted (or reformed) considering the need to comply with it through embedded procedures, as well as existing rules can be equipped with implementing acts that aid the embedding process. Hence, despite the overarching conceptual value of distinguishing the two phases (*i.e.*, design of the regulatory framework and subsequent implementation through compliance measures) in practice they are two sides of the same coin. It is for this reason that, while they are distinct concepts, in this work I focus on conceiving a regulatory approach that can aid its implementation by means of "compliance by design" methods. I call this joint analysis "[regulation/compliance] by design".

From a parallel perspective, in addition to "by design" methodologies the concept of "compliance through design" was put forward.[1028] Indeed, "compliance by design" has been extending its scope of application, and different approaches, meanings and fields of applications have been reviewed – *i.e.*, "regulatory compliance", "compliance by detection", "compliance by design", "legal compliance by design". Relatedly, four concepts were identified: (i) "compliance by design", referring to formalised rules heeded in the design phase of a business or regulatory process;[1029] (ii) "legal compliance by design", focused on the legality of the whole process, encompassing approaches based on business processes and legal knowledge (*i.e.*, properties of normative and legal systems);[1030] (iii) "compliance through design", including social and

[1027] In broad terms, compliance is the "conformity in fulfilling requirements, or demonstrating conformity with regulatory constraints", which denotes a set of requirements are previously selected – *e.g.*, laws, regulations, standards, best practices (Casanovas P, González-Conejero J, de Koker L (2017), p 34). From this perspective, compliance is a granular concept not fully translatable into binary requirements (Hashmi M, Casanovas P, de Koker L (2018), pp 60-61), and is increasingly automated to optimise the use of resources (Casanovas P, González-Conejero J, de Koker L (2017), p 34). It was argued the advantages of "compliance by design" include the flexibility of the approach, that can adjust to additions or changes in the rules.
[1028] Ibid. Hashmi M, Casanovas P, de Koker L (2018). Goldbarsht D, de Koker L (2022), p 7
[1029] Hashmi M, Casanovas P, de Koker L (2018), pp 60-61. In compliance-by-design a set of rules is assessed and compliance is embedded into business practice. Casanovas P, González-Conejero J, de Koker L (2017), p 34
[1030] Ibid, p 35. Hashmi M, Casanovas P, de Koker L (2018), pp 60-61.

institutional aspects not (explicitly) included in the traditional approach;[1031] (iv) "legal compliance through design". The latter recognises a broader array of social, political, economic aspects, as well as governance and ethical elements, crucial to the design of legal compliance. In principle, compliance encompasses technical, practical, and theoretical elements, and the "through design" approach acknowledges the relation between different meta-models, and the impossibility to comprehensively automate it by normative and linguistic tools.[1032] Although it seems possible to formalise aspects of legal compliance, this requires regulatory models that can bridge machine and human interfaces, as well as professional and institutional experiences.[1033] Indeed, (semi-)automation does not only refer to compliance with a text. Whenever there are contrasting or contending rights, obligations and policies, a compliance strategy does not only respond to regulatory requirements but also to a broader set of variables.[1034]

While I find the referenced literature most thought-provoking, I believe the specific features of my field of research warrant the choice to refer jointly to "by design" and "through design" approaches. Indeed, I argue that several aspects – *i.e.*, (i) the AML/CFT/CPF framework, (ii) its compliance impacts, (iii) the socio-technical features of IoM ecosystems, (iv) the dynamics between the regulatory field and IoM phenomenology – exemplify the crucial role of social, political, economic, governance and ethical elements whose importance led to formulating "through design" methodologies. Nonetheless, to fall in line with the portion of the literature that refers to "embedded regulation/compliance" as "regulation/compliance by design", I merge the two perspectives into a joint compound concept, and I refer to it as "[by/through]-design". Hence, my work focuses on "[regulation/compliance]-[by/through]" design.

6.4. "[By/through]-Design" Techno-Regulatory Standards in the IoM

As argued in Chapter 4, FATF's Recommendations are instruments of soft law. Despite giving rise to powerful expectations within the international community, they are not directly

[1031] These are defined as interpretation processes, institutionalisation, modelling-coordination interface, citizens-law relation. Casanovas P, González-Conejero J, de Koker L (2017), p 35
[1032] Ibid, pp 45-46. Hashmi M, Casanovas P, de Koker L (2018), pp 60-61, 63, 68-70. The notion was conceptualised to ground models to represent and (semi-)automate compliance. The authors addressed differences/similarities between "legal compliance by design" and "regulatory compliance", and factors hindering (semi-)automation. A later publication describes it as intermediate, semi-automated, hybrid, modular, adaptive and scalable, partial, flexible (Casanovas P, de Koker L, Hashmi M (2022), p 80)
[1033] Hashmi M, Casanovas P, de Koker L (2018), pp 68-70. For instance, the KYC practices deployed by a regulated entity can either foster or hinder a financial inclusion policy, depending on whether the latter is considered when responding to its AML/CFT/CPF duties (Casanovas P, González-Conejero J, de Koker L (2017), pp 46-47).
[1034] Ibid, pp 46-47. Casanovas P, de Koker L, Hashmi M (2022), p 71

binding. This remains true even if participating jurisdictions committed to transposing them into domestic law and enforcement measures are imposed in case of non-compliance. Soft law and standardisation are fundamental in the global financial domain, where the regulatory framework consists of a compound mix of rules, standards, and best practices, and are increasingly important as regulatory instruments.[1035] Because there is a tendency to turn to domestic implementations to protect national sovereignty, an important goal of global standards has been to avoid or mitigate the so-called "forum shopping" or "jurisdiction shopping".

In addition, in Chapter 4 I overviewed the extent to which technical standardisation has addressed DLTs beyond the specific AML/CFT/CPF action of the FATF. When analysing these initiatives, one can notice how technical standards usually do not refer to existing regulatory frameworks and do not pursue the establishment of regulatory standards, even when they are seen as drivers for mitigation of regulatory risks,[1036] and are at times advertised as such. Nonetheless, technical and regulatory standardisation features common aspects, chiefly pertaining to the interplay between regulatory agencies and the expertise held by the private sector. The lines are easily blurred between standards set by regulatory agencies and self-regulatory initiatives, and standardisation is often used to mitigate problems of information asymmetry between the industry and regulators. This asymmetry can be tackled by involving experts in regulatory processes or by adopting standards that can act as minimum safeguards.

6.4.1. "Embedded compliance" between (dis)intermediation and institutional adoption

The value of embedded compliance in a sphere such as the IoM, with its cases of *enhanced disintermediation*, appears relatively straightforward. Given the array of stakeholders and platforms (perceived as) difficult or impossible to control, the idea of doing it so "by design" can be tempting. This reasoning, however, may give rise to misunderstandings. In the same way it is difficult or impossible to enforce regulation on and within *non-centralised* ecosystems, it can be difficult or impossible to ensure they embed compliance into their design (*e.g.*, by adopting a specific RegTech tool) and monitor their compliance strategies. Hence, this approach is far from not generating challenges. As argued above, it may not be always possible or easy to reach the internal dynamics of the relevant ecosystems to the point of being able to exert an

[1035] Casanovas P, de Koker L, Hashmi M (2022), p 78
[1036] König L, Korobeinikova Y, Tjoa S, Kieseberg P (2020), p 1. World Economic Forum (2020)

influence on the protocol. Indeed, a certain degree of *(re)centralisation* may be needed for players to be able to actually embed compliance measures into a given technological solution.

Nonetheless, from a conceptual perspective I do not see this argument as a hindrance to advocating for a "[regulation/compliance]-[by/through]-design" approach. On the one hand, part of the IoM responds to socio-technical queries other than those of traditional market dynamics; on the other hand, a portion of these ecosystems will continue to lie outside the scope of regulation. *Embedded compliance* provides a key to unlock new opportunities, to be welcomed by players pursuing recognition within regulated environments, while it is not feasible to define measures that will be implemented by every IoM platform, tool, service provider. Meanwhile, as repeatedly argued, for now the IoM remains more *centralised* and intermediary-based than advertised, and the "decentralised label" is elusive.[1037]

In this context, IoM intermediaries are exponentially offering their services not only to retail clients but also to institutional players such as investment funds. From a methodological perspective, this requires cross-sectoral and forward-looking regulation and supervision. From a substantive perspective, arguably they should be subject to the same type of regulation and oversight as intermediaries operating with traditional and economically (*i.e.*, functionally) equivalent assets, also in terms of consumer/investor protection and AML/CFT/CPF.[1038]

Relatedly a growing connection can be witnessed between cryptocurrency ecosystems (and relevant platforms and stakeholders) and the mainstream financial system. The growth of the IoM and related activity performed by conventional intermediaries are factors that are increasingly interlinking traditional intermediaries (*e.g.*, banks, PSPs, institutional investors) with nodes of IoM ecosystems (*e.g.*, exchanges, trading platforms). Hence, conventional intermediaries may be exposed to an unregulated "shadow" financial system, either directly or indirectly.[1039] Illustratively, from a direct perspective there are instances of regulated entities that started interacting with the market of DeFi services to offer this type of products.[1040] Given the amount of "lightly regulated shadow crypto" entities, the need arises for technology-neutral rules.[1041] Indeed, the IoM's (purported) *decentralised* nature does not eliminate the need to safeguard public policy objectives, and technology can be leveraged to enforce AML/CFT/CPF

[1037] Auer R (2022), p 2
[1038] Auer R, Farag M, Lewrick U, Orazem L, Zoss M (2022), pp iii, 3 and 16. For an insightful analysis of the benefits of applying the notions of *functional equivalence* and *regulatory equivalence* to the blockchain context, please see De Filippi P, Mannan M, Reijers W (2022), p 368
[1039] For this reason, the need arises to apply a comprehensive risk assessment and risk mitigation approach. Auer R, Farag M, Lewrick U, Orazem L, Zoss M (2022), pp 3-4
[1040] Katona (2021), p 93
[1041] Auer R (2022), p 2

standards. In this context, the concept of *embedded supervision* was put forward to enhance data quality for supervisors and reduce compliance costs for firms.[1042] The term "regulatory automata" depicts a framework that enables automated supervision, where monitoring systems can use *decentralised* trust-creating mechanisms.[1043]

However, these mechanisms need an effective underpinning legal system and supporting institutions. For instance, DLTs provide evidence of a transfer of an asset-backed token, but the legal system must guarantee the link between the asset and the digital token,[1044] and frameworks must be developed to deal with the responsibility for financial crime. In this way, DLTs can improve the quality of compliance and lower the costs, improving the current situation that sees stakeholders lobbying for lighter regimes and supervisors struggling to apply AML/CFT/CPF standards to the IoM. While one operational aspect of *embedded supervision* is for regulators/supervisors to contribute to the design of the market (*e.g.*, standardisation to ensure *interoperability*), another important element is the development of an open source set of monitoring tools to clarify the application of regulatory requirements.[1045]

6.4.2. From "regulated self-regulation" to "polycentric co-regulation"

As outlined in Chapter 4, the global regulation of finance heavily relies on "voluntary compliance", with low institutionalisation,[1046] and its standardisation mirrors the evolution of the industry. Usually, *self-regulation* arises in a situation of minimal regulation, and it is introduced out of necessity: industry members self-regulate for the sake of growth and survival.[1047] In this context, self-regulation may guide technological change, especially in the form of standardisation.[1048] In a second phase, *oversight regulation* is generally driven by flaws of self-regulation,[1049] whose notion is debated, notably regarding the relationship between "regulation" and

[1042] Auer R, Farag M, Lewrick U, Orazem L, Zoss M (2022), pp iii, 3 and 16. *Embedded supervision* "is distinct from other forms of "suptech" or "regtech", which aim to use machine learning or artificial intelligence to more efficiently monitor the financial industry. The key principle of embedded supervision is to rely on the trust-creating mechanism of decentralised markets for regulatory purposes too" (Ibid, p 19)
[1043] Embedded supervisory systems could automatically verify compliance with Basel III standards of an entity holding asset-backed tokens. They could be designed for supervisors to access all transaction-level data or selected parts, while firms would define access rights instead of collecting/delivering data (Auer R (2022), pp 2-3, 9).
[1044] It is crucial "asset tokenisation" is validated by the legal system. Likewise, additional institutions could be required to guarantee the accuracy of external elements relevant to smart contracts' payoffs. Ibid, p 4
[1045] Ibid, pp 6 and 19-20
[1046] Newman A, Bach D (2014), p 432. Chapter 3 provides details on dynamics and actors
[1047] *E.g.*, hacks can drive market actors to establish self-regulatory schemes. Tsuchiya Y, Hiramoto N (2021), p3
[1048] Standardisation may even replace law in some domains. Finck M (2019a), p 169
[1049] Johnstone S (2021), p 136

"governance", and "self-regulation" and "co-regulation".[1050] A deep analysis of the topic falls outside the scope of this work, but an overview contextualises its methodology.

Even if regulation is often equated with governance,[1051] one distinctive trait of the former is the involvement of public institutions. Hence, governing actions within market regulatory systems – *e.g.*, corporate governance or industry standards/practices, if agnostically viewed by the law – are excluded.[1052] Counterintuitively, these instances of self-regulation may not be labelled as regulation;[1053] in this sense, self-regulation consists of "non-binding norms of action, process, and behaviour, for whom sanctions of the formal regulatory type play no part".[1054] By contrast, if there is a formal institutional involvement there is co-regulation, featuring interactions between general legislation and a self-regulatory entity.[1055] In these instances, self-regulatory efforts of the private sector are granted legitimacy by being framed within legislative/governmental regulation. The interactions between regulatory forces may occur with higher or lower intensity: institutional intervention may be indirect – *e.g.*, sanctions for failures to adopt standards/codes of practice (*i.e.*, enforced self-regulation).[1056] The legislator may also lay out principles to be implemented by private actors, which are best positioned to give them practical application – *e.g.*, principles-based regulation, of which both the AML/CFT/CPF regime (so far) and the GDPR are prominent examples.[1057]

Moving to the IoM domain, "top-down" legislation could appear a natural approach. However, in line with the findings of the previous chapters, the literature accounts for four problems: (i) the information asymmetry generated by technological evolution stimulates ill-advised fact-selection and the adoption of ill-suited terminology; (ii) a framework can be onerous to enforce when there are misunderstandings on the technology and its limitations; (iii) specific rules run the risk of adding excessive burdens; (iv) "command-and-control" methods tend to be rigid and lack flexibility.[1058] Hence, also in the IoM sphere there are attempts to apply AML/CFT/CPF methodologies informed by approaches other than "command and control", "hard law" and

[1050] For context-specific analyses: Pagallo U, Casanovas P, Madelin R (2019). Borrás S, Edler J (2020). Trubek DM, Trubek, LG (2007). Hofmann J, Katzenbach C, Gollatz K (2017)
[1051] This is Black's position, ref. by Hofmann J, Katzenbach C, Gollatz K (2017), p 1411. Finck M (2019a), p 145
[1052] Marsden C (2011)
[1053] "Regulation" and "self-regulation" may be difficult to differentiate: Bennett C, Raab C (2020), p 454
[1054] Marsden C (2008), p 118
[1055] Marsden C (2011), p 1, Pagallo U, Casanovas P, Madelin R (2019), p 2
[1056] Terminological choices vary: "enforced self-regulation" was labelled as "meta-regulation" in Black J (2012)
[1057] Regarding the GDPR: Bennett C, Raab C (2020), p 453
[1058] Finck M (2019a), pp 166-167

"top-down" methods. These approaches are focused on dialogue, principles, and incentives.[1059] However, in the field at hand these initiatives have been rare.

From a first perspective, certain stakeholders have engaged in self-regulatory efforts. Notably, cases were reported of voluntary application of CDD measures for the sake of acquiring commercial and competition advantages, responding to market dynamics. To the same end, some intermediaries have opted out of accepting AECs.[1060] Indeed, the diversity among IoM stakeholders emerges once again as a relevant aspect, with some actors cherishing freedom from any centralised control and others actively seeking to regulate themselves to legitimise their activities and be perceived by the market as legitimate players. In other words, the second group pursues to be accepted into commercial activities, to drive the industry's applications towards social benefit, but other stakeholders may also view regulatory compliance as a competitive advantage over those that cannot handle the attached burdens.[1061]

Meanwhile, the concept of "scheme governance authority" was put forward in 2014,[1062] in the early days of IoM's regulation. This can be a described as a "self-governance" initiative, but because it is mandated it becomes a form of direct regulation – namely, of "regulated self-regulation", equated by the literature to "co-regulation".[1063] In this respect, a twofold argument was raised. If there is no voluntary centralised scheme it is difficult to apply these rules, since the mandatory set up is feasible for centralised schemes only.[1064] Nonetheless, such establishment could ensure *accountability* to regulators and supervisors and could lay out the conditions to interact with regulated financial services.[1065] Around the same time, the EC mentioned the option of a central database to register users' identities and cryptocurrency addresses, coupled with a system of user registration via a self-declaration form. Experts have voiced doubts as to its efficacy when it comes to users engaging in illicit activities.[1066]

These approaches were not successful, and recent initiatives bear no mention to them. This is not to say innovative methodologies are to be ruled out, and indeed "[regulation/compliance]-[by/through]-design" may change the paradigm. However, the need arises to decide on a regulatory methodology to implement it. To assess the possible means of application of such a regime, its establishment can be imagined in a self-regulatory fashion. In these scenarios, as

[1059] Ibid, pp 144-145
[1060] Houben R (2019)
[1061] Johnstone S (2021), p 21
[1062] European Banking Authority (2014), p 14. It was an entity accountable to the regulator, to be established internally by a cryptoasset scheme.
[1063] Finck M (2018), p 686
[1064] Nabilou H (2019), pp 272-274
[1065] European Banking Authority (2014), pp 39-40
[1066] Houben R (2019)

underlined by Finck, isolated instances of self-regulation lack the transparency to safeguard diverse public and private interests, and fail to consider the positions of external actors, while it is necessary to handle information asymmetry. Accordingly, pure self-regulation is inappropriate, while co-regulation may combine flexibility with public policy goals. In other words, there is no single best regulatory technique, and a combination between designs was praised.[1067]

In line with these arguments, I find co-regulation particularly interesting in designing an AML/CFT/CPF regime that is suitable to the specifics of the IoM. In EU law, in co-regulation the objectives are defined by the legislator and their attainment is conferred to specific parties such as economic operators, social partners, NGOs.[1068] Co-regulation reflects innovative governance traits, including a shared exercise of power, the possibility to experiment and create knowledge through various insights into the application of standards.[1069] Indeed, co-regulation shows considerable advantages, as (i) it mirrors the need to involve private actors in a regulatory process while guaranteeing public oversight; (ii) it ensures the initiative's *reflexiveness*;[1070] (iii) its flexibility enables "regulatory experimentalism"; (iv) it identifies best practices; (v) it allows early intervention, and for regulators and regulated entities to engage in early dialogue and develop technology in a way that is compatible with public policy objectives.[1071]

In the domain at hand, co-regulation reconciles the *centralising* and *decentralising* forces of the blockchain, that is inherently both local (node-wise) and global (network-wise), and possibly *decentralised* at the infrastructure level and *centralised* at the governance level. Co-regulation mirrors the fact that governance is influenced by legal, social, technical, economic standards. The approach is process-oriented and can involve many stakeholders (*i.e.*, more than authorities and firms).[1072] Thus, "polycentric co-regulation" was put forward by Finck as an enhanced version of co-regulation, involving a wide array of stakeholders (polycentric) and tailored to technology (it can rely on code). In particular, authorities involve a diverse set of actors in drafting, implementing, and enforcing regulation, relying on the potential of code. This collaboration heeds technological requirements without unduly delegating regulatory authority or abandoning public policy objectives.[1073] The benefits of code emerge in different

[1067] Finck M (2019a), pp 170-171
[1068] European Commission (2003) (repl. by European Commission (2016)). Ref by Finck M (2019a), pp 172-173
[1069] Ibid, pp 172-173. These elements were identified in new governance by Scott J, Trubek D (2002)
[1070] *i.e.*, for it to be understood by the regulated autonomous social systems
[1071] Finck M (2019a), pp 174-175. Ranchordás S (2015)
[1072] Finck M (2019a), pp 175-176
[1073] Ibid, pp 144-145 and 165

phases, such as in (i) law making, where technology fosters polycentric participation and deliberation,[1074] (ii) implementation,[1075] and (iii) enforcement of regulatory constraints.[1076]

6.4.3. From "law + technology" to techno-regulatory standards

An interesting take on the way to have a cross-disciplinary evolution of technology at the EU level was provided by Schrepel, who termed the "law + technology" approach and contextualised it in relation to smart contracts.[1077] Within this framework, law and technology interact in a cooperative and complementary fashion, pursuing a preservation of their spheres of influence while building on their strengths. The approach respects the features of a technology (that in this case is the blockchain), as this is viewed as a key element to ensure the survival of the ecosystem, but allows enforcement. Accordingly, the characteristics of smart contracts and their environment are analysed through the "law + technology" lens to detect influential aspects and understand how to safeguard the evolution of the Digital Single Market.[1078]

The need to combine the two perspectives originates from the fact that a blockchain application has both legal and technical aspects, and if they do not cooperate "one would have to succeed before the other takes over", which generates unbalanced development of the applications.[1079] Accordingly, it is pivotal to establish a stable line of communication between law and technology, the latter mostly in terms of stakeholders holding knowledge and influence on the given domain. As argued in Chapter 4, regulators access industry expertise in different ways. In some cases, they rely on private sector authorities (self-regulatory organisations) for technical advice and/or policy execution, and major regulatory authorities receive suggestions on regulatory strategies from stakeholder groups and private actors. However, the extent to which

[1074] Technology can support polycentricity with new ways to influence specific laws, while aiding disorganised groups to exert political influence (Wu T (2003). Ref. by Finck M (2019a), pp 178-180). However, online participation raises issues of legitimacy, effectiveness, accountability (Ibid, ref. Brown I, Marsden C (2013), p 3)
[1075] For implementation, the model of "endogenous regulation" was suggested, similar to co-regulation, for regulators to leverage collaboration with core developers to incorporate regulation into the DLT and applications running on top of it. Reyes C (2016), p 195. Referenced by Finck M (2019a), pp 178-180
[1076] Reference was made to the methodologies introduced by Reidenberg and Lessig (Reidenberg J (1998). Lessig L (1996). Ref. by Finck M (2019a), pp 178-180), and to the fact new techniques can provide real-time feedback and allow regulators to react swiftly (Kaal W, Vermeulen E (2017). Ref. by Finck M (2019a), pp 178-180)
[1077] Schrepel T (2021)
[1078] The methodology opposes "technical fundamentalism". The latter "consists of designing technology without relying on legal rules, and sometimes is a way of avoiding it" and leads to "temporary autonomous zones" where law is not enforced. It threatens the survival of the technology, as outside the "temporary autonomous zone" the application of the law can lead to its extinction. "Technical fundamentalism" also includes the attitude of rejecting "any technical modification under the pretext that it contradicts some founding principles, such as those extolled by Satoshi Nakamoto" (Schrepel T (2021), p 14)
[1079] Ibid, p 14

the private sector is formally involved in the decision-making process varies significantly. When self-regulatory organisations play a crucial role, their involvement can go beyond self-regulation.[1080] This type of involvement is the one in "polycentric co-regulation".

As argued in Chapter 4, regulatory and technical standardisation are not detached. Two topical examples are (i) the ongoing debates on the crypto travel rule and on CBDC *interoperability*, explored in Chapter 5, and (ii) from a conceptual standpoint, the notion of "polycentric co-regulation", exemplifying how embedded processes are at the heart of valuable methodologies today. From this perspective, cross-disciplinarity could be a step forward from cross-functionality – *i.e.*, presence of members with different experiences and responsibilities – currently praised in FATF's architecture.[1081] In this context, an interesting reflection is sparked by the section of the AML Package that entrusts the drafting of RTSs, ITSs, guidelines, recommendations for regulated entities, supervisors or FIUs to the AMLA, to improve clarity of the rules, ensure consistency with standards, promote supervisory convergence.[1082]

RTSs and ITSs are delegated instruments adopted by the EC to ensure consistency in the application of the AMLR. They are technical by nature, do not imply strategic decisions or policy choices. Their content is limited by the delegating act, as provided for by Article 290 TFEU. As reported in Chapter 4, they are not a new concept. In the AML Package, RTSs are chiefly targeted to enhancing the application of an RBA-based CDD, and namely they shall:

i. specify: (a) entities, sectors and transactions with higher ML/TF risk; (b) related thresholds for occasional transactions; (c) criteria to identify linked transactions. The RTSs must build on the inherent risk levels of business models and the EC's SRA (Article 15(5) AMLR).
ii. set out (i) minimum data to collect in standard, simplified and enhanced CDD, depending on the customer's risk level, (ii) simplified measures applicable to lower risk situations; (iii) reliable and independent sources to perform *identity* verification; (iv) list of attributes for an eID scheme and relevant trust services to fulfil the requirements (Article 22 AMLR).
iii. provide a common EU template for reporting suspicious transactions, to ease compliance but boost the effectiveness of FIUs' analyses and cooperation (Article 50(3) AMLR).
iv. concerns group policies, branches, and subsidiaries (Articles 13-14 AMLR).

The rules-based nature of the AMLR is expected to provide a consistent framework for the AMLA to supervise its application.[1083] If multi-stakeholder participation is ensured in decision-

[1080] Brummer C (2015), pp 18 and 32
[1081] *I.e.*, combination of financial authorities and LEAs (Ibid, p 106).
[1082] European Commission (2021b), pp 11-12, Recital 9, Articles 5-6
[1083] European Commission (2021a), p 3

making, for instance as provided by the model of "polycentric co-regulation", I believe this type of regulatory forum – and the underlying regulatory methodology – could fit the need for an innovative AML/CFT/CPF approach to the IoM sphere.

6.5. Use Case: CBCD-Based Machine-to-Machine Payments [1084]

Considering the foregoing, this section describes a preliminary model of application of a methodology that belongs to the "[regulation/compliance]-[by/through]-design" sphere. The use case concerns the interaction between the worlds of Consumer Internet of Things (CIoT), machine-to-machine (M2M) communication, and retail CBDCs. While the integration of digital fiat money into M2M dynamics may unlock a novel layer of socio-economic synergy, it also generates complex regulatory questions mirrored by trade-offs. This section portrays the interplay between technological features and regulatory options, showcasing an embryonic example of cross-disciplinary dialogue. The background of the analysis consists of two pillars. On the one hand, the last decade has brought into our life *smart* objects that leverage connectivity to provide innovative services. CIoT is a subset of these items: an interconnected system of ubiquitous digital devices used by consumers on a personal basis – *e.g.*, wearable watches, home assistants, smart vehicles.[1085] On the other hand, as explored in Chapter 5 central banks are increasingly investigating retail CBDCs for public use.[1086]

Since interactive e-devices can communicate in the M2M fashion, a future was foreseen where smart machines can (inter)act autonomously also from an economic perspective.[1087] This concept gives birth to a "M2M economy", that is decentralised and grounded on the autonomy of its participants (*i.e.*, (C)IoT devices). The literature underlines the benefits of integrating DLTs into (C)IoT projects, where they are conducive to improvements in scalability and smart contracts increase communication efficiency and security by predefining conditions for transfers of data and assets.[1088] Accordingly, DLTs and programmability could reportedly contribute in a substantial way to the "M2M economy" reaching its full potential. Among the challenges arising from enabling smart devices to exchange data and services without (or with limited)

[1084] *Contents and parts of this section have already appeared in the following co-authored publication*: Pocher N, Zichichi M (2022)
[1085] Mercan S, Kurt A, Erdin E, Akkaya K (2021). The acronym (C)IoT signals the argument is deemed applicable to the broader complex of IoT devices.
[1086] Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021). Pocher N, Veneris A (2021b)
[1087] Prasad R, Rohokale V (2020). Schweizer A, Knoll P, Urbach N, von der Gracht HA, Hardjono T (2020)
[1088] Taubenheim J (2019). Barbosa AC, Oliveira TA, Coelho VN (2018)

human intervention, however, the need emerges for them to handle payments.[1089] In this sense, M2M payments consist of integrating payment processes into an automated processing of business transactions. Without M2M payments, (C)IoT runs the risk of remaining a siloed fragment of the bigger picture. Integration needs to rely on information exchanges performed without interruptions dependent on human actions such as manual confirmation.[1090]

6.5.1. Applying "trade-offs-[by/through]-design"

The deployment of CBDCs in a (C)IoT scenario generates regulatory hurdles, including the current lack of a normative framework for device-to-device transactions, adequate standardisation measures, frameworks of *machine identities* to support the legal effects of the activities they perform, and the need to re-design transaction safeguards that may hinder a true M2M scenario.[1091] In this context, the large-scale interest in CBDCs can provide the opportunity to define normative goals at the beginning of the design process, tackling technical and legal aspects jointly. This is in line with the "[regulation/ compliance]-[by/through]-design" approach. Against this backdrop, it can be argued that the automation featured by (C)IoT solutions requires a payment system that is *compliant by design*.

If one assumes, within the limits outlined above, that design and code can become regulatory instruments, a crucial role is played by the analysis of the specific features to be tuned. This applies also to the integration between (C)IoT and CBDCs. Since (C)IoT devices are used in large economic sectors and their core functionalities consist of sensing and collecting data, surveillance issues arise when privacy and data protection are not adequately safeguarded.[1092] When financial transactions are placed into the equation, risks increase consistently, and a chief trade-off concerns the concurrent presence of *privacy* and *transparency* requirements – *e.g.*, data protection and AML/CFT/CPF. While, as argued in Chapter 2 and investigated in Chapter 5, the *privacy-transparency* tension is found in all means of payments, programmability generates new forms of control and disclosure of sensitive information,[1093] and the added value of CBDCs is to embed from the start a specific trade-off. The main examples reviewed in Chapter 5 are (i) full *transparency*; (ii) unlimited *privacy*; (iii) nuanced solutions. The last option is

[1089] Schweizer A, Knoll P, Urbach N, von der Gracht HA, Hardjono T (2020). Mercan S, Kurt A, Erdin E, Akkaya K (2021)
[1090] PPI AG (2020)
[1091] *E.g.*, two-factor authentication. Forster M, Gross J, Kamping AK, Katilmis S, Reichel M et al (2021)
[1092] Ahlgren B, Hidell M, Ngai ECH (2016). Mercan S, Kurt A, Erdin E, Akkaya K (2021). Jabbar R, Fetais N, Kharbeche M, Krichen M, Barkaoui K, Shinoy M (2021)
[1093] Allen S, Capkun S, Eyal I et al (2020)

deployed by the majority of CBDCs projects, offering some *privacy* to consumers, in the form of *confidentiality*, and some *visibility* to authorities, in terms of *auditability*.[1094]

Relatedly, a CBDC scheme can deploy different types of wallets (or combinations thereof), that serve the function of authenticating users and interacting with the system.[1095] Digital wallets store private and public keys used to sign transactions digitally, and their features influence the autonomy of (C)IoT devices and the *non-centralisation* of M2M communications. There are at least five wallet design options that can be highlighted:[1096]

i. When choosing between account-based and token-based wallets,[1097] one must consider that in an M2M scenario an account-based wallet limits the device's access to the payment process because human authentication is required. However, it is not mandatory to use only one wallet type within a CBDC ecosystem – *i.e.*, there is no need for a CBDC architecture to deploy only token-based wallets, and there could be an account-based main wallet and several token-based wallets dedicated to devices.
ii. With regard to hardware-based vs. software-based wallets,[1098] the choice will likely depend on the operation scenario of the device and on the required degree of security – *e.g.*, the implementation of hardware-based solutions may be feasible for some CIoT devices, and more complex in other scenarios.
iii. When it comes to custodial or non-custodial wallets,[1099] the main point is that while token-based CBDCs *can* be held by custodians on behalf of end-users, account-based CBDCs are intrinsically based on the relationship with a custodian.[1100] Hence, non-custodial wallets are suitable for CIoT devices and resonate better with distributed structures. It is possible to combine the two types to suit different needs within the same ecosystem.
iv. The distinction between parent wallets and sub-wallets may provide a fruitful combination in a M2M scenario.[1101] Indeed, it is possible for the (human) holder to have a main wallet as parent wallet and open several sub-wallets, controlled by the parent wallet, to

[1094] Pocher N, Veneris A (2022b)
[1095] Allen S, Capkun S, Eyal I et al (2020)
[1096] Pocher N, Zichichi M (2022), pp 7-8
[1097] In account-based wallets access is tied to an identity system and authentication is performed via identity verification (*e.g.*, a security code), while in token-based wallets via a cryptographic scheme (*e.g.*, a digital signature).
[1098] The security of a hardware-wallet relies on chips and other technologies built in the device, while a software-based wallet makes use of cryptography and security protocols at the software level.
[1099] As outlined in the previous chapters, wallets are custodial when a third party operates the wallet and holds the private keys on the user's behalf, while in "non-custodial wallets" end-users hold the private keys directly.
[1100] Goodell G, Al-Nakib HD, Tasca P (2021)
[1101] The distinction concerns authorisation. A main parent wallet can be compared to a generic bank account for the use of fiat currency, while sub-wallets are comparable to prepaid cards linked to the account and with a limited amount of fiat.

set payment limits or conditions, thus also controlling privacy protection and other features. A CIoT device could use this type of sub-wallet to have autonomy in its payments.

v. As mentioned in Chapter 5, one of the requirements for a CBDC model is to provide for (a certain degree of) offline usability. Some CIoT devices are likely to run into this situation on a frequent basis – *e.g.*, a smart vehicle needing to pay at a tollbooth, but no connection is available when passing through the gates. In Chapter 5 I explored related hardware- and software-based design options.

In terms of embedded *privacy-transparency* trade-off, as outlined in Chapter 5 CBDC research is heeding "mixed solutions" to offer certain *anonymity* and a desirable level of *privacy*.[1102] These models are designed to provide multiple wallet options tailored to different types of transactions and users – *e.g.,* higher degrees of *anonymity* for transactions of low value. To do so, they may offer *anonymity-oriented* wallets – *i.e.*, transactions may not require the acquisition of *identity* data – allowing only selected types of transactions. Ostensibly, albeit not necessarily, an *anonymity-oriented* CBDC is usually token-based. In this respect, it was argued users should be able to hold their CBDC tokens in a non-custodial fashion, thus the latter should not be linked to addresses/identifiers (*e.g.*, users or other tokens) in compliance with the principle of "privacy by design".[1103] This idea, combined with the mentioned limits in terms of amounts and types of transactions, appears suitable to the operational specifics of smart devices. However, the model below shows this argument can also be nuanced, without being disregarded, within a scheme of tiered wallets with a main account-based wallet controlling token-based sub-wallets, thus implementing a different trade-off.

6.5.2. A preliminary model of techno-regulatory integration

As anticipated, the deployment of DLTs in a scenario populated by billions of economically autonomous smart devices was deemed conducive to handle the necessary techno-regulatory requirements.[1104] Seemingly, native DLT-based means of payment are significantly suitable to integrate payments into the CIoT, thus streamlining the value chain and avoiding (at the time of the operation) human involvement, manual confirmations and/or the need for exchanges between tokens. Nonetheless, beside the value of DLTs, it is the nature of retail CBDCs as fiat

[1102] Pocher N, Veneris A (2022b)
[1103] Goodell G, Al-Nakib HD, Tasca P (2021)
[1104] Schweizer A, Knoll P, Urbach N, von der Gracht HA, Hardjono T (2020). Forster M, Gross J, Kamping AK, Katilmis S, Reichel M, Sandner P, Schröder P (2021)

money that plays a key role in merging the physical and digital worlds in a seamless fashion, grounding the possible model for a two-tier retail CBDC system based on a DLT.

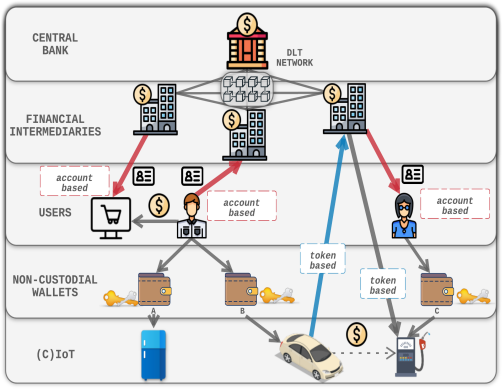

Figure 8: preliminary model of techno-regulatory integration
From: Pocher N, Zichichi M (2022)

The integration between a two-tier retail CBDC and CIoT is multi-layered, and a set of structural options must be tailored to the needs and constraints of smart devices. A preliminary model is displayed in Figure 8 above. Within this system, smart machines are equipped with non-custodial token-based sub-wallets loaded with a given budget to pay automatically and independently, while (human) end-users hold custodial account-based parent wallets that rely on authentication and control the devices' wallets. The combination of the two wallet types safeguards *privacy* and allows the trade-off outlined above to be designed in a more flexible way.

As argued in Chapter 5 with regard to CBDC implementation, the integration between retail CBDCs, M2M payments and CIoT also requires multi-stakeholder-based standardisation, and CBDC projects seem to provide an invaluable opportunity to develop it. Accordingly, the relevance emerges of applying "by design" techniques to address regulatory concerns, especially when they generate seemingly opposing requirements. In this context, the deployment of DLTs in a CBDC design is conducive to reaching and embedding desired trade-offs.

6.6. The Intervention of EU Law: Notes on Legitimacy and Effectiveness

As outlined in Chapter 4, a considerable portion of the EU activity in the AML/CFT/CPF domain consists of transposing FATF Standards. Accordingly, the measures adopted at the EU level are closely intertwined with the Recommendations, also because the increasingly cross-border and international nature of ML/TF/PF would make siloed Union actions largely ineffective. Hence the value of international coordination and cooperation and of adopting rules

compatible with, or at least as stringent as, international ones.[1105] This consideration underpins this work when addressing the AML/CFT/CPF regulation of IoM ecosystems starting from international standardisation, which links the methodology to the broader sphere of global financial regulation as a compound of rules, standards, best-practices.

Although the concrete value of the tie between EU and international measures is undisputed, their formal relationship is more complex. Transposition into EU law arguably alters the diffusion dynamics of global standards, as EU law exerts a "legalisation" effect that transforms soft law and informal best practices into embedded rules.[1106] This EU-based cryptocurrency-oriented research on AML/CFT/CPF is inherently challenged by the interplay between FATF Standards, the technical nature of compliance in the IoM, the mechanisms of EU law, the dynamics between regulatory and technical standards. Evidently, the IoM is constantly evolving and will develop in ways difficult to foretell. These circumstances call for a regulatory methodology that is "flexible-by-design", from the standpoint of being applicable to new instruments, networks, ecosystems, as they emerge. In my opinion, this is a major value of establishing a cross-disciplinary working group. Indeed, the process of laying out benchmarks to construe a cryptocurrency taxonomy that accounts for the relevant trade-offs between *anonymity* and *transparency* should be conducted in a way that is as future-proof as possible.

As mentioned above, I believe a valuable regulatory approach to the AML/CFT/CPF challenges of the IoM entails the design of a taxonomy framework to classify IoM ecosystems and their elements from a functional perspective (*i.e.*, according to their risk), in combination with the techno-legal reasons that ground the classification (*i.e.*, parameterised criteria). Indeed, the taxonomy instrument has already showcased its capacity of combining flexibility with precision in cross-disciplinary endeavours. An inter-disciplinary body of knowledge can then be leveraged to establish a regime of techno-regulatory standardisation as per a "[regulation/compliance]-[by/through]-design" methodology. Likewise, to create a future-proof instrument I believe the design of the taxonomy should embody a combination of principles-based and rules-based approaches and include an analysis on whether it is feasible to model in a taxonomy fashion the socio-technical elements influencing *anonymity* in IoM ecosystems.

The final objective is to develop regulatory and compliance decisions that draw from the findings of the taxonomy– *e.g.*, use its benchmarks as criteria on which to ground decisions – to shape a framework to apply AML/CFT/CPF to the IoM. Illustratively, when a given use case

[1105] European Commission (2021a). Recital 4
[1106] Newman A, Bach D (2014), pp 430-432

is at the extreme end of the *anonymity* scale, the given transactions – in the given cryptocurrency or processed by a given entity – could be outlawed or limited if risks are deemed too high to be addressed by regulated entities. Limitations pertaining to e-money testify that trade-offs have already been established in the sphere of digital payments, thus there is no reason to use different standards for the IoM. Concurrently, the cross-disciplinary collaboration and development of common references (*e.g.*, the taxonomy) could give rise to "[regulation/compliance]-[by/through]-design" mechanisms. The parameterisation of the risk levels could spur an application of these criteria to ensure compliance of a specific tool with the framework.

6.6.1. Legitimacy and the need for uniformity

The overarching role of global financial regulation, and notably the activity of the FATF, and the inherent cross-border nature of IoM ecosystems, may challenge the EU involvement in cryptoasset regulation also in the AML/CFT/CPF domain. However, the mentioned complexities and the integration of the (Digital) Single Market warrant the involvement of EU law as the prime means to address the type of regulation foreseen in this work. As outlined in Chapter 4, AML/CFT/CPF measures are not a stand-alone framework in the EU, rather they interact with other areas such as payments and transfer of funds, financial services, criminal law, the eIDAS regime. To a varying degree of intensity, depending on the specificity of the regimes, managing AML/CFT/CPF regulatory issues at the EU level also safeguards their interplays with other frameworks. In this context, EU-level integration can provide a powerful playing field to the regulatable portion of the IoM, while I argue that the considerable literature, policy and regulatory documents pertaining to AML/CFT/CPF harmonisation provides an extensive array of arguments defending the role of EU law.

Since the application of DLT-based solutions to the financial sphere (later encompassing IoM tools not necessarily DLT-based) emerged as a disruptive techno-economic phenomenon, the latter calls for EU institutions to adopt an innovation-friendly approach combined with a critical analysis of relevant developments, to design sensible regulatory responses that can safeguard public policy objectives.[1107] To this end, "the cooperation of law and technology requires a uniform approach across the European space".[1108] Indeed, the cross-border nature of (public permissionless) blockchain applications makes it difficult for developers and users to decide to

[1107] Decisions to be made go way beyond banning or allowing a use case. Sensible frameworks that balance innovation with public policy are needed and require a deep understanding of the technology. Finck M (2019a), p 144
[1108] Schrepel T (2021), p 15

comply only with the regulation of a given jurisdiction. For this reason, the effects of a national regime would not necessarily be limited to it, and a strong "Brussels effect" was foreseen.[1109] It is for this reason that "law + technology" methodologies argue EU members could coordinate their actions and subsequent implementation strategies, especially when targeting the "layer 1" of blockchains, thus influencing the architecture of the given blockchain, its core software.[1110]

From this perspective, "polycentric co-regulation" allows a technology-enabled expansion of the actors involved in the regulatory process. This could play a role in meeting the needs of consistency with values of democracy, participation, representation, and pluralism, and of de-centralisation and experimentation required by the IoM. Accordingly, provided transparency is ensured within the co-regulation procedures, the approach could mitigate the accusations of democratic and legitimacy deficits currently tainting the activities of EU institutions.[1111]

Evidently, specific controversies could arise in terms of legitimacy and legal basis regarding specificities of the taxonomy-based "[regulation/compliance]-[by/through]-design" approach. I argue these problems may depend significantly on the results of the taxonomy effort, which could suggest addressing them at a later stage. In any case, as explored in Chapter 4 one can witness an increasing opening of EU law towards the adoption of regulation-based regimes not only in the AML/CFT/CPF domain. From the perspective of regulatory methodology, one may focus on the legal instrument's shift in recent EU proposals from the long-established directive-based approach of minimum harmonisation, to a regulation-based that aims to achieve uniformity for the foundational aspects of the regulatory frameworks.[1112] As outlined in Chapter 4, the methodology underpins both the AML and the Digital Finance Packages, the latter including the MiCA proposal. In the case of both proposals the legal basis is Article 114 TFEU on the approximation of laws, as it is necessary to the functioning of the internal market. The choice of legal basis is justified, respectively, to remove establishment obstacles and improve the functioning of the internal market for financial services,[1113] and because ML/TF/TP can generate cross-border economic losses, functional disruption, reputational damage.[1114]

[1109] *I.e.*, the type of unilateral regulatory globalisation by the hands of which rules originally adopted in a jurisdiction expand to the economic life of the marketplace at a global level
[1110] Schrepel T (2021), p 15. "Layer 2", instead, includes the technology and the applications that are deployed on top of the underlying blockchain protocol (*e.g.*, it is the layer where smart contracts work).
[1111] Verbruggen P (2009). Finck M (2019a), pp 177-178. "Indeed, while the Union never regulates in isolation and is influenced by industry views even outside co-regulatory contexts, the latter technique can make such engagement explicit and add transparency" (Ibid)
[1112] European Commission (2021a), p 2
[1113] European Commission (2020b), p 4
[1114] European Commission (2021a), p 4

6.6.2. Effectiveness: standards and flexibility "[by/through]-design"

The concrete ways to move from the process of devising a taxonomy, which can subsequently inform a "[regulation/compliance]-[by/through]-design" regime, to embedding measures into technology are yet to be explored. Similarly, the specific method to combine the application of rules-bases and principles-based methodologies in the building stage of the taxonomy entails specific complexities that are be addressed, especially since the link between the two frames of reference is not as clear as one could hope. In this respect, I believe the AML/CFT/CPF regime offers an interesting field of experimentation because its measures are inherently shaped by the RBA – thus, their application is by nature tailored to the principle of proportionality, which demands a preliminary assessment of the levels of risk – and the RBA is in turn moulded on a multi-level variety of risk indicators that contribute to shaping final compliance outputs. Hence, I think a taxonomy-based "[regulation/compliance]-[by/through]-design" approach, within the meaning argued above, is inherently consistent with an RBA-based regime, and provides a degree of flexibility that can attempt to mitigate the mentioned risk of overfitting.

In this context, I argue an important role is played by red flag indicators and the possibility to transpose them, leveraging a "transposition model" to be devised, into techno-regulatory standards to clarify and benchmark their meaning and streamline their application. Notably, I think this "regulatory experimentation" could take place within the framework of the responsibilities and competences thrust on the AMLA within the AML Package. Their implementation could be eased by developing the standards directly with the private sector offering IoM-related analytics services and sharing them in an open-source format. Among indicators, I believe *anonymity* risks are among the most relevant given their role as drivers underpinning the regulation of the IoM space. Indeed, the first concerns of cryptocurrency misuse stemmed (purportedly) *anonymous* cryptocurrency transfers aiding illicit transactions.

In terms of effectiveness of this regulatory methodology, at least two other problems emerge. On the one hand, embedded regulation still needs an opening into (*i.e.*, access to) these ecosystems. Considering the increasing tendencies of the IoM towards *disintermediation*, one cannot forget that this type of access is remarkably difficult to obtain (or even impossible to achieve) when there is no *centralisation* of power of any kind at the socio-technical level. On the other hand, the enforcement of any regulatory provision in the IoM is susceptible to generating controversies related to the origin and ideologic roots of this sphere, as well as to the privacy and data protection elements outlined throughout this work. Foreseeably, a fruitful

cross-disciplinary and cross-industry cooperation, also in the form of PPPs, could aid the establishment of a fit-for-purpose enforcement strategy.

6.6.3. The role of the EU in setting techno-regulatory standards

As mentioned above and explored in Chapter 4, the EU AML Package not only introduces a new domain-specific and EU-wide supervisory authority, the AMLA, but also entrusts it with a comprehensive drafting of operational specifications. The latter are addressed to a wide array of stakeholders, and arguably cover the foundational aspects of the AML/CFT/CPF regime from a compliance perspective. Indeed, among its manifold competences, the AMLA is expected to adopt RTSs, ITSs, guidelines and recommendations for regulated entities, supervisors and/or FIUs,[1115] to improve the degree of clarity of AML/CFT/CPF rules, ensure the consistency of EU measures with international standards, promote supervisory convergence.[1116]

In this context, I argue the AMLA framework could provide a suitable institutional and procedural background against which to implement regulatory solutions that blend the need for flexibility with that of ensuring an EU-wide common approach to the combination between law and technology. From a content perspective, however, I believe that these RTSs could be shaped in a more innovative fashion also in terms of drafting style. This would mirror in a more detailed way the dynamics between technical and regulatory provisions in a way that goes beyond what was done so far in the available examples of RTSs referenced above. To this end, the AMLA regime and its links with the procedures to adopt RTSs' proposals could be explored further, in combination with the impacts on EU law legitimacy. In broad terms, I argue large-scale stakeholder involvement may mitigate most concerns.

Relatedly, Finck highlighted the risk of intra-EU fragmentation stemming from different national regimes, and an even more worrisome risk of "race to the bottom". In this regard, the usual EU response – *i.e.*, issuance of a supranational framework – may not be viable in the IoM because of the insufficient capability of performing comprehensive assessments on the legal implications of blockchain technology and related innovation capacities.[1117] Although from an AML/CFT/CPF perspective a supranational framework is already underway, I believe these considerations can be applied to its specifications and implementing measures, such as those to be included in RTSs and ITSs. Indeed, AML/CFT/CPF rules affect socio-economic and legal

[1115] European Commission (2021b), pp 11-12 and Articles 5-6
[1116] Ibid, Recital 9
[1117] Finck M (2019a), pp 180-181

areas perceived as sensitive to the sovereignty of the Member States. Hence, the latter could argue against EU-level detailed rules adopted by the EC.

Indeed, going back to Finck's reasoning, when it comes to certain complex technology-related matters even when there is consensus on the appropriateness of a regulatory reform, there may be no certainty as to the principles to include and no political consensus on over-hauling (supra)national values. For this reason, she mentions the possibility to devise a "28th regime", that consists of an EU-framework that is alternative to national rules but does not replace them.[1118] An example could be, in the case at hand, a set of techno-regulatory standards the industry can comply with on a voluntary basis. The goal would be to give an additional opportunity to stakeholders active in a cross-border fashion, fight the "race to the bottom", and possibly lead to the adoption of standard secondary legislation.[1119]

In my opinion, however, the choice of pursuing the establishment of a 28th regime instead of pursuing regulatory uniformity through an institutionalised techno-regulatory model would not be a suitable methodology to adequately address the specifics of the AML/CFT/CPF sphere and IoM ecosystems. This is largely due to the nature of the AML/CFT/CPF framework, in terms of protected values and interests, in the realm of financial system integrity, especially taking into consideration the inherently cross-border dynamics explored throughout this work for what concerns IoM-related activities. Indeed, I believe that without a uniform approach the framework would still suffer from the significant fragmentation that drove the drafting of the AML Package, and in a broader sense also that of the Digital Finance Package. Moreover, the procedural specificities of "polycentric co-regulation" and its combination with the taxonomy-based and "[regulation/compliance]-[by/through]-design" methodologies are elements that precisely aim to solve, or at least mitigate, some of the issues that usually arise when establishing a supranational regime that is perceived as too intrusive at a national level.

6.7. Conclusions

Against the backdrop of the increasing complexity of IoM-related regulation, in this chapter I explored key aspects of a possible methodology to be applied at the EU level in the AML/CFT/CPF sphere. Mainly, the chapter considered (i) the concurrent and ever-evolving presence

[1118] The "28th regime" is a concept put forward by Monti M (2010). Referenced by Ibid, pp 180-181. A key example of this approach, also known as "optional instrument", is the regime of the *Societas Europaea* introduced by Council Regulation (EC) No 2157/2001

[1119] In the meantime, the approach could offer a context in which to reflect on the process to adapt regulation to technological innovation, to serve both private and public interests (Ibid, pp 180-181)

of multiple assets, technologies, innovative and traditional stakeholders in the socio-technical ecosystems that compose the IoM; (ii) the diverse approaches put forward over recent years with respect to the regulation of new technologies; (iii) their interplay with the elements that, as outlined in the previous chapters, inform the AML/CFT/CPF regime. The analysis set out by overviewing the impacts of technology-based and individual-based regulation, as well as of mixed solutions, on the domain at hand. Accordingly, it underlined how, instead of aiming to eliminate IoM-related risks once and for all, the goal can be to establish flexible and teleologically oriented frameworks that evolve with technology and provide useful results despite the constant changes. Relatedly, I outlined the types of interplay DLT-based applications can have with regulatory frameworks and focused on the *proactive* instances of "structured experimentalism" (*e.g.*, regulatory sandboxes) that could replace *reactive* regulatory approaches.

Furthermore, I provided an overview of a set of methodological features of AML/CFT/CPF regulation, tailoring the analysis to *anonymity-transparency* trade-offs. Accordingly, I proposed the creation of a taxonomy to evaluate the levels of *anonymity* risk posed by cryptocurrencies and/or ecosystems, possibly leveraging a combination between principles-based and rules-based methods, claiming the participation of a large array of actors in regulatory processes may provide a substantial insight into the risks to be mitigated. Meanwhile, I suggested the creation of a "transposition model" between red flag indicators (*e.g.*, the ones of the FATF) and techno-regulatory standards, and I explored the effects of *enhanced disintermediation*. In the third section of the chapter I investigated the possible shift from the widely known and criticised "code is law" to a compound concept of "[regulation/compliance]-[by/through]-design", focusing on the communication level between technology and regulation, while I overviewed the underlying concepts of *embedded regulation* and *embedded compliance*, as well as related evolutions. I underlined the importance of tech-sensitive regulation and how the effectiveness of "active cooperation" is vulnerable to criticism, while a *proactive* approach is needed. I underlined the importance of focusing on the mutual relation between regulation and code, without the need to equate or compare the two concepts. In this context, a key aspect is building on existing cross-disciplinary initiatives and furthering multi-stakeholder dialogue.

In the following, the chapter elaborated on the value of techno-regulatory standards and of placing their adoption within a polycentricity-based model of co-regulation. Accordingly, it assessed the role of techno-regulatory standards and elements of a possible methodology, exploring the differences between "self-regulation", "co-regulation" and the recent concept of "law + technology". Later, I provided an embryonic use-case of the proposed approach, to exemplify the content of a model of techno-regulatory integration as an example of the type of

communication to be institutionalised. Finally, I reviewed methodological elements for the intervention of EU law in the AML/CFT/CPF regulation of IoM ecosystems in terms of legitimacy and effectiveness, overviewing the role of EU institutions in the design and implementation of such an innovative methodology. I considered the relationship of EU law with FATF Standards and global financial regulation, and the substantial and procedural value of establishing cross-disciplinary frameworks in line with the "polycentric co-regulation" model. In particular, I suggested exploring the implementation of the regime within the competences of the AMLA proposed by the AML Package. Notable reference is to the AMLA's proposed role in drafting RTSs, albeit possibly considering experimentation with innovative drafting styles, to go beyond what was achieved by past instances of these instruments.

7. Concluding Remarks

"*There is no disagreement as to the importance of stopping money laundering, the financing of terrorism, or the proliferation of weapons; the question is rather if these goals can be achieved with a new balance between the competing interests of privacy and surveillance, while facilitating the nascent promises of new technologies.*"
Kyles DL (2022)

7.1. Anonymity and an Unwarranted Double Standard

From a general perspective, two opposing elements emerged from my investigation into the interplay between the AML/CFT/CPF regime and the IoM, that in this work includes payment-type cryptoassets. On the one hand, when it comes to cryptocurrency ecosystems the complexity of the underlying technologies has over time generated ambiguities concerning the specifics of relevant platforms and stakeholders. Preliminarily, the phenomenological picture of the IoM appears blurry regarding the degree of *disintermediation* and *non-centralisation* featured in different cases. Clearly, this goes to the detriment of any idea of *accountability* one may wish to establish. On the other hand, the "blockchain hype" informed an overall perception that everything about the IoM is disruption, and that any regulatory framework – AML/CFT/CPF measures in particular, given their intermediary-based nature – is unravelled by the innovations brought about in this sphere. Often, *disintermediation* and *non-centralisation* are (mis)interpreted not only in terms of whether they are indeed featured by a given scenario, but also in terms of their consequences. Illustratively, on the one hand CEXes are treated like traditional financial intermediaries, and on the other one DEXes are portrayed as an unreachable underworld, often without considering key differences among them.

I do not mean to argue these positions are completely unfounded. As explored in this work, it is challenging to grasp the possible combinations of traits that can be featured by an IoM ecosystem or even by only one of its many stakeholders and components. At times it may be even impossible, before enough information is released about a specific project (*e.g.*, in the relevant whitepaper, CBDC design report). Likewise, many of the concepts that underpin the IoM and its *enhanced disintermediation* evolution are indeed disrupting the *centralisation* paradigm that is at the heart of traditional intermediary-based *accountability* mechanisms.

Nonetheless, I challenge the twofold reasoning above, and the assumptions behind it, and I underline below how it gives rise to a very odd outcome.

Indeed, although the IoM is not understood in full, and there is often a lack of clarity when discussing the activities taking place within these ecosystems – *e.g.*, in terms of identifying entities to be entrusted with regulatory duties –, there is somehow a sense of certainty that traditional regulatory principles and approaches must be changed entirely to address the challenges arising in this sphere. In this sense, I argue there is a widespread confusion between the need to find the appropriate approach for handling IoM regulatory issues and the need to re-evaluate previous regulatory policy decisions because of the advent of cryptocurrencies. I do not mean to say that policy decisions should not be changed or updated, but that adjusting the regulatory approach does not entail *per se* changing any determination concerning the values to protect and the objectives of the given framework. In other words, these elements are obviously related but should remain separate and treated accordingly when regulating new spheres.

I think *anonymity* in cryptocurrencies is a perfect example of this tendency to use a double standard when it comes to the IoM. For instance, as explored in Chapter 6 the prohibition of *anonymous* bearer shares or prepaid cards seems to originate fewer controversies than the regulatory treatment of self-hosted wallets or privacy coins. The same is true for the trait of *disintermediation* and its interplay with the enforcement phase – *e.g.*, different types of limits are placed on cash transactions, even if it is still possible to pass on a bag full of cash in a dark alley. The point is making this occurrence more difficult, by hindering any exploitation of financial operators in the endeavour to fill the bag of cash and/or make use of its content by disguising its origin, and to make it easier to detect these situations. By contrast, we debate – and I include this work – on whether the (supposed) impossibility of enforcement of limitations on self-hosted wallets or DEXes should restrain any proposals for limitations.

Arguably, this double standard stems from the fact that in recent years cryptocurrencies, in combination with the increasing amount of personal data collected every day and the possibility to exploit it very efficiently for a vast array of purposes, created a heightened sensitivity to the importance of privacy and data protection. This, in turn, had an impact on the public perception as to the acceptable trade-off between *anonymity* and *transparency*, between *privacy* and the risks of *surveillance,* also in terms of financial transactions. Despite the importance of these considerations, I argue that this issue should not be confused or merged with the impossibility of implementing current regulatory frameworks in innovative spheres.

The cryptocurrency space is complex, but its dynamics are not impossible to understand. Since the endeavour requires a less traditional form of interdisciplinary knowledge, it is likely

that legal experts cannot sufficiently understand it with their own background. This means they must engage in cross-disciplinary endeavours and establish new forms of collaborations to grasp and address the challenges at stake. At the same time, the simple fact that a new scenario alters dynamics and benchmarks does not necessarily unravel regulation, and the need for new approaches does not mean that nothing can be saved. It does, however, require phenomenological analyses on which to structure new regulatory methodologies and processes.

Against this backdrop, these conclusions pivot on four pillars, addressed by the following sections. These pillars mirror the multi-layered approach deployed throughout this work and pertain to different levels of reasoning. The final output of this dissertation consists of their combination. In particular, in the remainder of these concluding remarks I outline findings concerning: (a) the *anonymity-transparency* trade-offs featured by IoM socio-technical ecosystems, (b) the application of a holistic approach to drafting a risk-based taxonomy, (c) the value of establishing a polycentric techno-regulatory standardisation model in the EU, methodologically grounded on (d) "[regulation/compliance]-[by/through]-design".

7.2. Anonymity-Transparency Trade-Offs in IoM Socio-Technical Ecosystems

In this work I explored the interplay between the IoM and AML/CFT/CPF regulation from the viewpoint of *anonymity* risks vis-à-vis the *transparent* nature featured by some DLT implementations. *Anonymity* and *transparency* are pivotal notions in the world of DLTs and are considered inherent features of the IoM. In the development of the latter, *encryption* and ledger *transparency* played a key role. *Anonymity* and *transparency* are also key notions in the AML/CFT/CPF sphere, where *anonymity* generates risks of misuse of financial systems, while *transparency* aids compliance, supervision, investigation, and enforcement. This twofold perspective has long populated *online communication* and *financial transactions*, where *anonymity* is double-edged: it fosters illegality, but its absence violates human rights, posing AML/CFT/CPF and privacy concerns. Cryptocurrencies are a prime example of this dynamic.

While disambiguating the notions of *anonymity* and *transparency*, I argued in favour of a teleological methodology. In other words, the analysis was informed by the specifics of the context, composed of the IoM and the AML/CFT/CPF framework. The latter regulatory domain is anchored to a domain-specific vision of mitigating risks generated by *unaccountable* transactions. The consequent understanding of *anonymity*, albeit not clearly defined, is tied to the intermediary-based nature of the regime. When applied to the IoM, this approach generates

problems mirrored by challenges such as the crypto travel rule, transfers involving self-hosted wallets, and difficulties in linking transactions to *real-world identities.*

The complexity that informs the IoM as an ecosystem of socio-technical ecosystems is another element that warrants the adoption of a teleological approach to the definitions of *anonymity* and *transparency*, to develop a conceptual understanding of both their nature and regulatory consequences. Indeed, the socio-technical essence of the IoM generates a granularisation of the concepts of *anonymity* and *transparency.* Since the characteristics of an ecosystem depend on technical and social elements, and on their interaction, cryptocurrency features are inevitably multi-layered and can vary significantly. Transactions take place within and/or across ecosystems populated by many stakeholders, services, technical layers, where the concept of *anonymity* comes into play in different forms. Accordingly, a "dynamic" approach is needed for its analysis. On the basis of the traits identified and explored in this research, chiefly at the core of Chapters 2 and 3, when IoM specifics meet the AML/CFT/CPF regime the concept of *anonymity* displays the features listed in Table 3 below.

Conceptually granular	*Anonymity* is composed of different features. Their individual importance depends on the given perspective. Several elements are used as benchmarks to evaluate the *anonymity* of a cryptocurrency scheme – *e.g.*, they encompass notions of *traceability*, *linkability*, *identifiability, pseudonymity*, *confidentiality*, and *privacy.* These terms are often used imprecisely, also equated with *anonymity*, and their definitions are not always consistent – *e.g.*, studies may anchor their assessments to the same metrics, but rely on different interpretations of them, thus giving different meanings to the same benchmarks.
Context specific	*Anonymity* is a context-specific notion, which means its definition is bound to vary depending on the context. In the AML/CFT/CPF sphere, an *anonymous* transaction is one that cannot be related to an *identified* or *identifiable* individual. Relatedly, a subject is *identifiable* for a specific purpose when the entity in charge of the *identification* process can access the required data. Thus, *anonymity* can be evaluated only with respect to specific requirements against which to determine if *identification* has been reached.

Observer dependent	*Anonymity* can be assessed only with respect to a specific actor trying to reach *identification*. A subject is *identifiable* if the entity in charge of *identification* can access the required data. A subject is *identifiable* or *non-identifiable* only with reference to a specific actor.
Broader understanding than other frameworks	In AML/CFT/CPF, *anonymity* has a broader meaning than in other regulatory frameworks (*e.g.*, data protection). It does not distinguish between *anonymisation* and *strong pseudonymisation.* It encompasses both the impossibility to link data to an *identified* person, and cases where the link is (only) significantly hampered. It follows that the same data can qualify as *pseudonymous* for data protection purposes and *anonymous* for those of AML/CFT/CPF.
Different from *privacy*	*Anonymity* (better, *anonymisation)* is only one of the available techniques for enhancing *privacy*. In particular, *anonymity* requires the absence of *identifiers*. If there are *identifiers*, there is *pseudonymity*. Hence, both *anonymity* and *pseudonymity* relate to *identity*. *Privacy* is a broader concept and can be safeguarded in ways other than *anonymity*, and to different extents. Thus, techniques to enhance *privacy* do not necessarily exert impacts on *identification.*
Ranging on a spectrum	*Anonymity* and *transparency* are not a zero-sum game. There is no perfect dichotomy between *irresponsible anonymity* and *accountable identification*. Along a spectrum ranging from complete *anonymity* to full *transparency*, at any given point the two features coexist in a specific balance. A subject/item is not *identified* or *anonymous*: these traits are combined into a specific trade-off.
Linked to *disintermediation* and *obfuscation*	The IoM is more intermediated than expected, but disruptive new trends of *enhanced disintermediation* pose substantial *anonymity* risks. Meanwhile, *anonymity* can be linked to cases of transaction *obfuscation* and *opaqueness* of financial flows. These categories can be tied to traits of *untraceability, unidentifiability* and *unlinkability*, depending on the specifics.

Influenced by the interplay between forensics and *anonymity enhancements*	*Anonymity* is influenced by the interplay of forensics and *anonymity enhancements*. Since they benchmark the level of *traceability*, forensic techniques operate as a *trait d'union* between *pseudonymity* and *(un)accountability*. Their role is defining the possibility and likelihood of linking a *real-world identity* to a (set of) IoM transaction(s). This depends on their efficacy vis-à-vis *privacy*-enhancing methods. At the same time, the quality and efficacy of forensics influence *anonymity* enhancements, by prompting new means of *obfuscation.*
Mirroring *unaccountability*	Cyber-libertarians advocate for a cyberspace where everyone operates *anonymously* in an *unaccountable* fashion. Technology can be leveraged to reach opposing goals, and the IoM is a prime example of how it can generate pathways to *accountability (e.g.*, forensics) but also to *unaccountability* (*e.g.*, *anonymity*-enhancing methods). *Anonymous* transactions are tainted by the *unaccountability* of those performing them, while *enhanced disintermediation* and *obfuscation* are tied with (and at times pursue as a direct or indirect goal) *unaccountability*.

Table 3: socio-technical features of anonymity at the crossroads between the IoM and AML/CFT/CPF

Meanwhile, the understanding of *transparency* relevant to this work required a twofold analysis, as exemplified in Table 4 below, between the notions of ledger *transparency* and financial *transparency*, which is tightly tied to the concepts of *auditability* and *accountability*.

Ledger *transparency*	The goal of many public blockchains is to combine *user anonymity* (better, *pseudonymity)* with *transparency of operations*. The ledger is *transparent,* and the complete transaction history is available to everyone. Network participants, however, are not related to their *real-world identities*, but to *addresses* that act as *pseudonyms*. *Transparency of operations* is a type of *transparency* that does not ensure *accountability* and differs from *financial transparency.* The type of *transparency* offered by public blockchains it is a type of *transparency* useful for user interaction, not for oversight bodies.

Financial *transparency*	*Financial transparency* is grounded on the connection to *real-world identities – i.e.*, it relies on *identifiability.* From a regulatory perspective the notion of *transparency* is the one that aims to fight ML/TF/TP, and this understanding is focused on the information on the origin of funds and on the *identification* of clients and intermediaries.
Auditability	*Financial transparency* is tied to the concept of allowing *auditability*. While *auditability* assumes that access to a certain type of information is allowed in certain circumstances and by specific actors, it does not breach *confidentiality* of cryptocurrency transactions.
Mirroring *accountability*	The quest for *transparency* to ensure *accountability* is a commonplace goal not only in the financial context, but also in information networks. The goal of ensuring *auditability* is to hold users *accountable* for their activities. *Accountability* is ensured by *auditability*.

Table 4: the twofold nature of *transparency* in the public blockchains and financial regulation

Against this backdrop, the alleged paradox of public blockchains featuring both *anonymity* and *transparency* traits can be reframed as a combination of features whose interplay can be measured and reconciled by using benchmarked trade-offs and a teleological methodology. From the perspective of this research, the goal is the identification of specific benchmarks to differentiate between the various degrees of *anonymity* enshrined by IoM ecosystems. The approach of this work starts from conceptualising the existing trade-offs between, on the one hand, *anonymity* and *privacy* and, on the other hand, *transparency* and *auditability*.

As highlighted in Chapter 5, the current large-scale interest in CBDCs offers an invaluable chance to understand the way their features are influenced by technical and social factors. When devising the design of a CBDC model, a trade-off is chosen between *privacy*, *anonymity*, and *transparency*, which sheds a light on how these characteristics play out in cryptocurrency ecosystems as well. Most CBDC proposals offer some *privacy* to end-users and some *visibility* to authorities and/or other participants of the system. These "mixed solutions" provide options tailored to given types of transactions and/or users (*e.g.*, higher *anonymity* for low-value transactions and low-balance wallets). These trade-offs can be addressed from the perspectives of *confidentiality* and *auditability*, with direct impact on AML/ CFT/CPF *accountability*. Relevant schemes can be classified as per these embedded trade-offs.

In this context, *accountability* emerges as a key conceptual link. Both *obfuscation* and *dis-intermediation*, hampering *traceability*, generate a situation where users are not *accountable* for their activities (*e.g.*, transactions). While some stakeholders are trying to avoid regulatory constraints and surveillance, others are trying to re-establish it by applying different techniques, thus engaging in a never-ending race. On the ground of the socio-technical nature of IoM ecosystems, the activities performed by this plethora of actors influence the overall character of the domain. Against this backdrop, I believe the added challenge brought by the IoM when addressing the trade-offs between *anonymity* and *transparency* is not the presence of this interplay, but rather its peculiar and ever-evolving socio-technical composition.

7.3. A Holistic Approach to a Risk-Based Taxonomy Effort

A methodological outcome of this work concerns the value of taxonomies to enable cross-disciplinary cooperation, as introduced in Chapter 1. I argue the approach has already proven conducive to balancing flexibility with precision in the realm of tokens. Provided it leverages both principle-based and rules-based methodologies, it can mitigate the risk of overfitting. Taxonomising allows the levels of *anonymity* risk posed by different cryptocurrencies and/or ecosystems to be evaluated and categorized accordingly. This can be done after having pinpointed the benchmarks of AML/CFT/CPF *anonymity* risk – emerged as chiefly linked to *enhanced intermediation* and *obfuscation* – and requires that the assessments be accompanied by details justifying the classification – *e.g.*, criteria should be parameterised.

Such a taxonomy effort mirrors an interrelation exercise between empirical phenomena and theoretical schemes, which is grounded on selecting yardsticks on which to ground techno-regulatory reasoning. This approach is deployed in the preliminary taxonomy of CBDC designs provided in Chapter 5. The model is based on embedded *privacy-transparency* trade-offs, grounded on the possibility to link regulatory considerations (*e.g.*, *auditability, confidentiality*) to socio-technical factors (*e.g.*, PETs, wallet types, public-private models). However, since concepts of *anonymity* and *transparency* are socio-technical, it remains to be explored whether all AML/CFT/CPF risks can be effectively modelled in a taxonomy fashion and, if not, scope limitations and complementary approaches must be provided.

From a regulatory perspective, the value of the socio-technical concept and of deploying a "system approach" lies in embracing the elements at play when devising a strategy to approach these ecosystems, thus avoiding reaching conclusions that are refuted by phenomenology. In this respect, I argued in this work that the difficulty in applying regulation to the IoM stems

from the concurrent presence of (i) *assets*, such as the different types of tokens, (ii) a set of *technologies* deployable to different ends (*e.g.*, P2P technologies, distributed systems, tokenisation); (iii) *innovative actors* (*e.g.*, developers, miners, exchanges, FinTech companies, P2P platforms); (iv) *traditional actors*, such as traditional FIs; (v) different *scopes of application* of the technologies, at times overlapping or concurring (*e.g.*, financial applications, supply chain, self-sovereign identity, and certification). The combination of these elements shapes the IoM and mirrors its nature of an ecosystem of socio-technical ecosystems.

Accordingly, the socio-technical nature of the IoM ecosystems requires that the modelling of *anonymity* and *transparency* deploys a methodology that is both suitable to measure AML/CFT/CPF risk and able to encompass a holistic perspective. Indeed, IoM ecosystems feature a given *anonymity-transparency* trade-off for multiple reasons, including the way the systems generating and exchanging payment tokens are construed and governed. Hence, it is necessary to focus on the landscape in which cryptocurrencies are transferred through an *accountability*-based approach. This entails focusing on the evolution of *non-centralisation* and *disintermediation* scenarios, and on the interplay between the different socio-technical dimensions – *e.g.*, interplay between forensics and *anonymity enhancements*.

In particular, as explored in Chapters 3 and 4 the AML/CFT/CPF domain makes use of "red flag indicators" where empirical elements suggesting suspicious activities are described to guide compliance responses and supervision. Chief reference is to the indicators published by the FATF, that substantially inform national and institutional guidance. These indicators are a key feature of RBA-based frameworks, and are usually provided in rules-based format, phrased as templates of sequences of actions that suggest a suspicion. I argue a pivotal aspect concerns the methodology and style used to draft risk indicators to help detecting anomalous activities.

Red flag indicators operate as empirical measures of risks, and they provide a structure to think about them. In principle, they should provide clear benchmarks and their structure should be able to accommodate new indicators as the sphere evolves. The content of rules-based indicators, however, is often less straightforward than desired. Moreover, depending on the link with empirical findings – *i.e.*, the phenomenological aspects highlighted in Chapter 1 – they may feature little normative content, and be for the most part descriptive. Furthermore, there can be considerable gaps between the indicators and industry best practices (*e.g.*, crypto travel rule debate). Further, although rules-based systems have the advantage of interpretability, their simplicity produces an outstanding number of false positives – *i.e.*, reportedly, more than 95% of the alerts generated from the rule-matching process are false positives.

While RegTech tools embedding machine learning are innovating this sphere, I believe other initiatives may aid and support the development of more effective and efficient applications. In this respect, I argued in favour of the creation of a "transposition model" between red flag indicators and techno-regulatory standards. The concept is detailed below. This model could help clarify the meaning of the indicators, streamline compliance at the regulated entity-level and would enshrine the holistic approach outlined above with regard to *anonymity-transparency* trade-offs. Indeed, as exemplified in Figure 9 below, the model would draw directly from the mentioned taxonomy. Ideally, the findings included in the taxonomy could allow it to be used directly as a source of risk indicators, and the transposition process could happen in the framework of the competences entrusted to the proposed AMLA. In particular, I believe both their drafting and their implementation could be eased by developing standards with the private entities offering analytics services and sharing them in an open-source format.

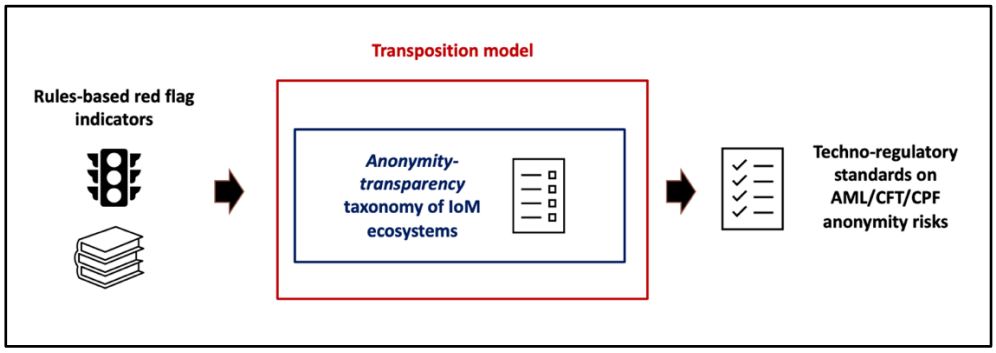

Figure 9: interplay between the proposed taxonomy and the proposed transposition model between red flag indicators and techno-regulatory standards

7.4. A Polycentric Techno-Regulatory Standardisation Model in the EU

The mentioned taxonomy should be grounded on the establishment of an institutionalised regime of techno-regulatory standards featuring the participation of a large array of actors in the regulatory process. This approach may provide a substantial insight into the risks to be mitigated and would leverage inputs from both AML/CFT/CPF efforts and technical standardisation on DLTs and cryptoassets. Indeed, IoM-related technical and regulatory standardisation is currently siloed, and in the AML/CFT/CPF domain there is a lack of the type of standardisation that allows automation of the compliance process for what concerns risk indicators. In this context, the design of AML/CFT/CPF compliance in CBDC systems can inspire a broader discussion on the value of standardisation in the broader IoM space.

One of the goals of establishing cross-disciplinary collaboration is to bridge the gap between the dynamism of technologies and stringent rules-based regulatory approaches. Indeed, as outlined in Chapter 6, embedding cross-disciplinarity into regulatory processes is at the heart of innovative methodologies. Designing an efficient interplay of rules-based and principle-based reasoning, however, presents its complexities, and requires significant cross-disciplinary efforts. To this end, I suggest an EU-level institutionalised model of techno-regulatory standardisation can provide for a legitimate and effective response. The model is to be established as a multi-stakeholder scheme of co-regulation, bearing in mind the impact of global financial regulation on Union-level strategies and the technical nature of compliance in the IoM. In other words, I suggest devising techno-regulatory standards through *polycentric* co-regulation.

In particular, I suggest implementing the regime within the competences of the AMLA as proposed by the AML Package. The AMLA is expected to draft RTSs related to almost all parts of AML/CFT/CPF compliance. These RTSs are to be drafted as per Article 290 TFEU, which means they are submitted to the EC for adoption, they are technical, do not imply strategic or policy choices. If multi-stakeholder participation is ensured in decision-making according to the model of "polycentric co-regulation", I believe this type of regulatory forum could fit the IoM sphere. I argue the AMLA framework could provide a suitable scenario to blend the need for flexibility with that of ensuring an EU-wide approach. In my opinion, however, the content of RTSs could be shaped as to blend technical and regulatory provisions in a way that goes beyond what has been done so far. The regime and its links with the procedures to adopt RTS proposal could be explored further, in combination with the impacts on EU law legitimacy. In broad terms, large-scale stakeholder involvement may mitigate most concerns.

In this context, I believe AML/CFT/CPF is a valuable field for *proactive* regulatory experimentation because its measures are inherently shaped by the RBA. Thus, their application is by nature tailored to the principle of proportionality, which demands a preliminary assessment of risk levels. Meanwhile, the RBA requires consideration of a multi-level variety of risk indicators that must contribute to shaping final compliance outputs. Hence, I believe a taxonomy-based approach, within the meaning detailed above, is consistent with an RBA-based regime, and provides a degree of flexibility that mitigates the risk of overfitting.

7.5. A "[Regulation/Compliance]-[by/through]-Design" Regime

The first three pillars of these conclusions enshrine an underlying *proactive* approach to the management of techno-regulatory dynamics. Indeed, the way they elaborate on the interlink

between technical and regulatory compliance assumes the latter can be embedded into technology. This concept is at the root of *design-based* techniques, in contrast to traditional *command and control* approaches. In particular, the suggestions outlined above are informed by a methodology that I labelled "[regulation/compliance]-[by/through]-design", as contextualised in Chapter 6. This approach entails a shift from the controversial concepts of "code is/as law" and "law is/as code" to a more comprehensive and flexible notion, focused on the mutual relationship between regulation and technology, without the need to equate or even compare the two.

The notion is anchored to the need of leveraging existing cross-disciplinary initiatives to further multi-stakeholder dialogue in a way that is suitable to the dynamics of the target to regulate. In particular, Table 5 below outlines the different components of "[regulation/compliance]-[by/through]-design". The ordering of the concepts displayed by the table responds to reasons of logical narrative, following the arguments presented in Chapter 6, while the numbering highlights their position within the mentioned expression.

3	**Design**	The possibility to evaluate and taxonomise *anonymity-transparency* trade-offs inspires the establishment of AML/CFT/CPF techno-regulatory standards. The same reasoning can be applied to design from the start applications that embed given socio-technical aspects to reach regulatory and compliance goals. Indeed, in the same way a cryptocurrency scheme can be assessed in terms of its embedded *anonymity-transparency* trade-off by referring to specific benchmarks (e.g., implementation of certain PETs, presence in the system of both private and public actors), technology can be leveraged to embed *by design* a specific balance into a given application. Implementing design options often includes coding, but "code" is only one element of "design".
1	**Regulation/ Compliance**	A *proactive* approach to managing the interplay between technology, compliance and regulation is enshrined by *design-based* techniques – *i.e.*, *compliance by design, regulation by design*. Operationally, they are labelled *embedded compliance* and *embedded regulation*, at times used interchangeably in an imprecise fashion. In principle, *regulation by design* focuses on shaping *regulation* starting from a *design* perspective, while *compliance by design* refers to a process grounded on

		embedding compliance into the design of a tool. Despite the importance of distinguishing the two phases (*i.e.*, design of the framework, compliance measures), in practice they are two sides of the same (crypto-)coin. Indeed, in this work I focused on how to conceive a regulatory approach to aid *compliance by design*. To include the two aspects, I call this approach "[regulation/compliance] by design".
2	**By/Through**	The concept of *compliance through design* includes social, political, institutional, governance and ethical aspects not (explicitly) included in *by design* approaches. In the addressed research domain, there is a concurrent presence of several elements – *i.e.*, (i) AML/CFT/CPF framework, (ii) compliance impacts, (iii) socio-technical features of IoM ecosystems, (iv) dynamics between the regulatory field and IoM phenomenology. Arguably, this interplay is directly tied to the aspects whose value led to formulating *through design* methodologies. Because part of the literature does not make this distinction explicit while referring to *embedded regulation/compliance* as *regulation/compliance by design*, however, in this work the two perspectives are merged into the compound concept of "[by/through]-design".

Table 5: [regulation/compliance]-[by/through]-design

As interpreted in this work, the notion of "[regulation/compliance]-[by/through]-design" underpins (at least) three specific operational scenarios, outlined in Table 6 below. These different aspects are mutually reinforcing and are included in the transposition dynamics outlined in Figure 9 above. Indeed, I argue the underlying concept is the same, albeit interpreted and analysed from different viewpoints. In broad terms, the notion concerns the way to addressing the mutual interplay between regulation and technology.

Benchmarking *anonymity* and *transparency* to socio-technical elements, to evaluate risks posed by IoM ecosystems and categorise these risks accordingly, thus linking regulatory considerations to socio-technical factors	*Anonymity-transparency* **taxonomy** of IoM ecosystems in terms of ML/FT/PF risk

"Translating" regulatory provisions, often drafted in a rules-based fashion to describe empirical phenomena, into embeddable technical specifics with regulatory content	**Transposition model** between the risk indicators and techno-regulatory standards that can be complied with by design
Drafting regulation starting from the assumption that it will be complied with by/through design, hence providing techno-regulatory benchmarks to comply with it by/through design	**Techno-regulatory standardisation**

Table 6: "[regulation/compliance]-[by/through]-design" dynamics

To exemplify the approach from an operational perspective, in Chapter 6 I provided a use-case that addresses the interplay of M2M dynamics and retail CBDCs. In doing so, I displayed a preliminary process of modelling techno-regulatory integration, as an embryonic example of the type of cross-disciplinary communication and reasoning to be institutionalised.

7.6. Final Remarks

While the substantial components of these conclusions were outlined above, two more general remarks arose from this investigation. Indeed, I believe the interplay between the IoM and AML/CFT/CPF measures, interpreted through the lens of *anonymity* and *transparency*, provides valuable insights into the relationship between law and technology. In particular, I focus on two examples concerning the value of standardisation, and the way to think about the IoM as one of the possible examples of innovative technologies that alter traditional dynamics.

On the one hand, the value of standardisation is increasingly pivotal when regulating new technologies. This is because this type of normative structure aids the establishment of regulatory mechanisms that foster cross-disciplinarity. Indeed, it provides stakeholders with different expertise with a common playing field and common references to start building new frameworks. In particular, standardisation is key in the domain of financial regulation, as it is almost inherently composed of a mix of rules, standards, and best practices. Because the importance of standards as regulatory instruments is constantly increasing, I believe in the upcoming years it will be crucial to make sure the relevant processes feature an actual multi-disciplinary approach. Meanwhile, the interplay between the nature of standardisation initiatives as instruments of soft law and the consequences of their transposition into hard law should be carefully addressed. Despite the value of soft law, I believe efforts should be exerted towards the

implementation of cross-disciplinary standardisation models into hard law systems. This is what is suggested by the EU model of techno-regulatory standardisation proposed in this work.

On the other hand, I believe the understanding and the interpretation of the IoM have so far been informed by an excessive rigidity. To face the challenges posed by the socio-technical specifics of this domain, I argue we should deploy a more flexible reasoning. The IoM, but the same could be relevant to other fields of new technologies, is a notion that encompasses different scenarios. It features growing connections with the mainstream financial system, where traditional intermediaries (*e.g.*, banks, institutional investors) are interlinked with nodes of IoM ecosystems (*e.g.*, exchanges), but also displays thriving cases of *enhanced disintermediation*. Some of the latter end up having more ties with the traditional system than expected, giving rise to a process that tends to look more like a cycle than a spectrum. From a methodological perspective, this requires cross-sectoral and forward-looking regulation and supervision. From a substantive perspective, it requires diversified regulatory approaches, and possible equations between certain IoM activities and those involving equivalent traditional assets, to avoid exposing the regulated world to unregulated risks, either directly or indirectly.

Against this backdrop, it is important to think dynamically about this domain, without placing it into a specific category, but rather acknowledging existing differences between various instances and applications. In the years to come, the IoM is bound to house an ever-growing number of nuances between *anonymity* and *transparency*, *privacy* and surveillance, *centralisation* and *non-centralisation*, *disintermediation* and control. This is because the IoM, when interpreted as an ecosystem of socio-technical ecosystems, emerges as a new sphere of activities, not as a single concept. In my opinion, understanding the impacts of this consideration is crucial in the endeavour to regulate it in the most effective and legitimate way, trying to balance regulatory safeguards with the desire to foster advanced innovation and development.

Bibliography

1. Books and Book Chapters

Akhgar B, Gercke M, Vrochidis S, Gibson H (2021) Dark Web Investigation. Springer

Allen JG, Rauchs M, Blandin A, Bear K (2020) Legal and Regulatory Considerations for Digital Assets. University of Cambridge

Amarasinghe N, Boyen X, McKague M (2021) The Complex Shape of Anonymity in Cryptocurrencies: Case Studies from a Systematic Approach. In: Borisov N, Diaz C (eds) Financial Cryptography and Data Security. FC 2021. LNCS, vol 12674. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-64322-8_10

Antonopoulos AM (2016) The Internet of Money - Volume One. Merkle Boom

Antonopoulos AM (2017a) Mastering Bitcoin, 2nd Edition. O'Reilly Media

Antonopoulos AM (2017b) The Internet of Money - Volume Two. Merkle Boom

Arner D et al (2019) Policy and Regulatory Challenges of Distributed Ledger Technology and Digital Assets in Asia. In: Brummer C (ed). Cryptoassets: Legal, Regulatory, and Monetary Perspectives. Oxford University Press

Ashmarina SI, Horák J, Vrbka J, Šule\vr P (2020) Economic Systems in the New Era: Stable Systems in an Unstable World. Springer

Bancroft A (2020) The Darknet and Smarter Crime: Methods for Investigating Criminal Entrepreneurs and the Illicit Drug Economy. Palgrave Studies in Cybercrime and Cybersecurity. Palgrave Macmillan

Barbereau T, Sedlmeir J, Smethurst R, Fridgen G, Rieger A (2022) Tokenization and Regulatory Compliance for Art and Collectibles Markets: From Regulators' Demands for Transparency to Investors' Demands for Privacy. In: Lacitt MC, Treiblmaier H (eds) Blockchains and the Token Economy. Technology, Work and Globalization, Springer

Bevir M (2009) Key Concepts in Governance. SAGE Publishing

Bexell M, Moerth U (2010) Introduction: Partnerships, Democracy, and Governance. In Bexell M, Moerth U (eds) Democracy and Public-Private Partnerships in Global Governance. Palgrave Macmillan

Borreguero Belntrán Á (2019) A Forensics Approach to Blockchain. Master Thesis in Telecommunications Engineering. Universitat Politècnica de Catalunya

Brown I, Marsden C (2013) Regulating Code. MIT Press

Brummer C (2015a) Soft Law and the Global Financial System: Rule-Making in the 21st Century. Cambridge University Press

Brummer C (2015b) The Perils of Global Finance. In Brummer C. Soft Law and the Global Financial System: Rule-Making in the 21st Century. Cambridge University Press

Brummer C (2015c) The Architecture of International Financial Law. In Brummer C. Soft Law and the Global Financial System: Rule-Making in the 21st Century. Cambridge University Press

Brummer C (2015d) Territoriality and Financial Statecraft. In Brummer C. Soft Law and the Global Financial System: Rule-Making in the 21st Century. Cambridge University Press

Brummer C (2019) Introduction. In: Brummer C (ed) Cryptoassets: Legal, Regulatory, and Monetary Perspectives. Oxford University Press

Campajola C, Cristodaro R, De Collibus FM, Yan T, Vallarano N, Tessone CJ (2022) The Evolution of Centralisation on Cryptocurrency Platforms. Available at: http://arxiv.org/abs/2206.05081

Carter RB, Marchant GE (2011) Principles-Based Regulation and Emerging Technology. In Marchant GE, Allenby BR, Herkert JR (eds). The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight. The International Library of Ethics, Law and Technology. Springer

Crepaldi M (2019) The Authority of Distributed Consensus Systems: Trust, Governance, and Normative Perspectives on Distributed Ledgers. PhD Thesis University of Bologna

Dannen C (2017) Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners. Apress

De Filippi P, Wright A (2018) Blockchain and the Law: The Rule of Code. Harvard University Press

Edmunds JC (2020) Rogue Money and the Underground Economy. An Encyclopedia of Alternative and Cryptocurrencies. Greenwood

Finck M (2019a) Blockchain Regulation and Governance in Europe. Cambridge University Press

Furneaux N (2018) Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence. Wiley

Geva B (2019) Cryptocurrencies and the Evolution of Banking. In Brummer C (ed) Cryptoassets. Legal, Regulatory, and Monetary Perspectives. Oxford University Press

Goldbarsht D, de Koker L (2022) From Paper Money to Digital Assets: Financial Technology and the Risks of Criminal Abuse. In Goldbarsht D, de Koker L (eds) Financial Technology and the Law. Combating Financial Crime. Law, Governance and Technology Series, Volume 47. Springer

de Koker L, Goldbarsht D (2022) Financial Technologies and Financial Crime: Key Developments and Areas for Future Research. In Goldbarsht D, de Koker L (eds) Financial Technology and the Law. Combating Financial Crime. Law, Governance and Technology Series, Volume 47. Springer

Hacker P, Lianos I, Dimitropoulos G, Eich S (2019) Regulating Blockchain: Techno-Social and Legal Challenges. Oxford University Press

Herian R (2019) Regulating Blockchain: Critical Perspectives in Law and Technology. Routledge

Johnstone S (2021a) Responses from the Centre. In Johnstone S. Rethinking the Regulation of Cryptoassets. Cryptographic Consensus Technology and the New Prospect. Rethinking Law. Elgar

Johnstone S (2021b) Regulatory Building Blocks and Other Concerns. In Johnstone S. Rethinking the Regulation of Cryptoassets. Cryptographic Consensus Technology and the New Prospect. Rethinking Law. Elgar

Johnstone S (2021c) An Emerging Market. In Johnstone S. Rethinking the Regulation of Cryptoassets. Cryptographic Consensus Technology and the New Prospect. Rethinking Law. Elgar

Johnstone S (2021d) Complexities in a developing technology. In Johnstone S. Rethinking the Regulation of Cryptoassets. Cryptographic Consensus Technology and the New Prospect. Rethinking Law. Elgar

Johnstone S (2021e) Acquiring the Tradition. In Johnstone S. Rethinking the Regulation of Cryptoassets. Cryptographic Consensus Technology and the New Prospect. Rethinking Law. Elgar

Kavallieros D, Myttas D, Kermitsis E, Lissaris E, Giataganas G, Darra E (2021a) Understanding the Dark Web. In Akhgar B, Gercke M, Vrochidis S, Gibson H (eds) Dark Web Investigation. Springer

Kavallieros D, Myttas D, Kermitsis E, Lissaris E, Giataganas G, Darra E (2021b) Using the Dark Web. In Akhgar B, Gercke M, Vrochidis S, Gibson H (eds) Dark Web Investigation. Springer

Kermitsis E, Kavallieros D, Myttas D, Lissaris E, Giataganas G, (2021) Dark Web Markets. In Akhgar B, Gercke M, Vrochidis S, Gibson H (eds) Dark Web Investigation. Springer

Kestemont L (2018) Handbook on Legal Methodology. Intersentia.

King C et al (2018) The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan

Kyles DL (2022) Centralised Control Over Decentralised Structures: AML and CFT Regulation of Blockchains and Distributed Ledgers. In Goldbarsht D, de Koker L (eds) Financial Technology and the Law. Combating Financial Crime. Law, Governance and Technology Series, Volume 47. Springer

Lessig L (1999) Code and Other Laws of Cyberspace. Basic Books

Lessig L (2006) Code v. 2.0. Basic Books

Magnuson W (2020) Blockchain Democracy: Technology, Law and the Rule of the Crowd. Cambridge University Press

Marchant GE, Allenby BR, Herkert JR (2011) The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight. The International Library of Ethics, Law and Technology. Springer

Marthews A, Tucker C (2019) Blockchain and Identity Persistence. In Brummer C. Cryptoassets: Legal, Regulatory, and Monetary Perspectives. Oxford University Press

Maurushat Alana, Halpin D (2022) Investigation of Cryptocurrency Enabled and Dependent Crimes. In Goldbarsht D, de Koker L (eds) Financial Technology and the Law. Combating Financial Crime. Law, Governance and Technology Series, Volume 47. Springer

Möslein F (2019) Conflicts of Laws and Codes. Defining the Boundaries of Digital Jurisdictions. In In Hacker P, Lianos I, Dimitropoulos G, Eich S (eds) Regulating Blockchain: Techno-Social and Legal Challenges. Oxford University Press

Nicoll C, Prins CJEJ, van Dellen MJM (2003) Digital Anonymity and the Law: Tensions and Dimensions. Information Technology & Law Series. T.M.C. Asser Press

Pocher N, Veneris A (2022a) Central Bank Digital Currencies. In Tran DA, Thai MT, Krishnamachari B (eds) Handbook on Blockchain. Springer Optimisation and Its Applications. Springer Cham

Quiniou M (2019) Blockchain: The Advent of Disintermediation. ISTE Ltd

Riccardi M, Levi M (2018) Cash, Crime and Anti-Money Laundering. In: King C et al (2018) The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan

Schrepel T (2021) Blockchain + Antitrust. The Decentralisation Formula. Elgar Publishing

Sidorenko EL, Sheveleva SV, Lykov AA (2021) Legal and Economic Implications of Central Bank Digital Currencies (CBDC). In Ashmarina SI, Horák J, Vrbka J, Šule\vr P (eds) Economic Systems in the New Era: Stable Systems in an Unstable World. Springer

Swartz L (2020) New Money: How Payment Became Social Media. Yale University Press

Tamò-Larrieux A (2018) Designing for Privacy and its Legal Framework. Data Protection by Design and Default for the Internet of Things. Law, Governance and Technology Series. Springer.

Torra V (2017) Data Privacy: Foundations, New Developments and the Big Data Challenge. Springer

Walch A (2019) Deconstructing 'Decentralisation'" In Brummer C (ed) Cryptoassets: Legal, Regulatory, and Monetary Perspectives. Oxford University Press

Werbach K (2019) The Blockchain and the New Architecture of Trust. Information Policy Series. The MIT Press

2. Journal Articles and Conference Proceedings

ABA Bank Compliance (1999) Privacy Crossfire: Money Laundering Hearings Refocus Privacy Debate. ABA Bank Compliance 20 (10)

Abimbola K (2001) Abductive Reasoning in Law: Taxonomy and Inference to the Best Explanation. Cardozo Law Review. 22(5-6), 1683-1690

Adler D (2018) Silk Road: The Dark Side of Cryptocurrency. Fordham Journal of Corporate & Financial Law Blog. Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/

Ahlgren B, Hidell M, Ngai ECH (2016) Internet of Things for Smart Cities: Interoperability and Open Data. IEEE Internet Computing 20, 6, 52-56.

Al Jawaheri H, Al Sabah M, Boshmaf Y, Erbad A (2019) Deanonymising Tor Hidden Service Users Through Bitcoin Transactions Analysis. Computers & Security, 2020, 89

Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys Tutorials, 17(4), 2347–2376

Altschuler S (2022) Should Centralized Exchange Regulations Apply to Cryptocurrency Protocols. Stanford Journal of Blockchain Law & Policy, 5(1), 92-113

Amarasinghe N, Boyen X, McKague M (2019) A Survey of Anonymity of Cryptocurrencies. ACSW 2019, ACM

Amler H, Eckey L, Faust S, Kaiser M, Sandner P, Schlosser B (2021) DeFi-ning DeFi: Challenges & Pathway. IEEE 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)

Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S (2013) Evaluating User Privacy in Bitcoin. LNCS 7859, 34–51

A**rner DW, Zetzsche DA, Buckley RP, Barberis JN (2019)** The Identity Challenge in Finance: From Analogue Identity to Digitized Ident. to Digital KYC Utilities. European Business Organisation Law Review 20 (1), 55–80

Arruñada B (2018) Blockchain's Struggle to Deliver Impersonal Exchange. Minnesota Journal Law Science & Technology 19 (1), 55–105

Athan T, Governatori G, Palmirani M, Paschke A, Wyner A (2016) LegalRuleML: Design principles and foundations. In Faber W, Paschke A (eds) Reasoning Web. Web Logic Rules (LNCS, 9203), Springer, 151-188. Available at: https://doi.org/10.1007/978-3-319-21768-0_6

Athan T, Governatori G, Palmirani M, Paschke A, Wyner AZ, et al (2014) Legal interpretations in legalruleml. In SW4LAW+ DC@ JURIX

Athanassiou PL (2019) Tokens and the Regulation of Distributed Ledger Technologies: Where Europe Stood in the Last Quarter of 2018. Journal of International Banking Law and Regulation 34 (3), 105–14

Avarikioti Z, Pietrzak K, Salem I, Schmid S, Tiwari S, Yeo M (2021) Hide & Seek: Privacy-Preserving Rebalancing on Payment Channel Networks. Cryptology ePrint Archive, Paper 2021/1401. Available at: https://eprint.iacr.org/2021/1401

Barbereau T, Smethurst R, Papageorgiou O, Rieger A, Fridgen G (2022) DeFi, Not So Decentralized: The Measured Distribution of Voting Rights. Proceedings of the 55th HICSS

Barbosa AC, Oliveira TA, Coelho VN (2018) Cryptocurrencies for smart territories: an exploratory study. International Joint Conference on Neural Networks (IJCNN), IEEE, 1-8. Available at: https://ieeexplore.ieee.org/document/8489299/

Barresi RG, Zatti F (2020) The Importance of Where Central Bank Digital Currencies Are Custodied: Exploring the Need of a Universal Access Device. Available at: https://ssrn.com/abstract=3691263

Bartoletti M, Carta S, Cimoli T, Saia R (2020) Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact. Future Generation Computer Systems 102: 259–77

Baxter G, Sommerville I (2011) Interacting with computers. Elsevier, 23

Bennett C, Raab C (2020) Revisiting the governance of privacy: Contemporary policy instruments in global perspective. Regulation and Governance 14(3), 447-464

Benson GJ, Bromwich M, Wagenhofer A (2006) Principles- Versus Rules-Based Accounting Standards: The FASB's Standard Setting Strategy. ABACUS, 42(2)

Berberich M, Steiner M (2016) Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers? Technical Core Features and Use Cases of the Blockchain Technology. European Data Protection Law Review, 2(3), 422–26.

Béres F, Seres IA, Benczúr AA, Quintyne-Collins M (2021) Blockchain is Watching You: Profiling and Deanonymising Ethereum Users. Proceedings of the 3rd IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2021

Berg A (2019) The Identity, Fungibility and Anonymity of Money. Economic Papers, November, 1–16. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211011

Biryukov A, Tikhomirov S (2019) Deanonymisation and Linkability of Cryptocurrency Transactions Based on Network Analysis. Proceedings - 4th IEEE European Symposium on Security and Privacy, 172–84

Black J (2002) Critical Reflections on Regulation. 27 Australian Journal of Legal Philosophy

Black J (2012) Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis. Modern Law Review 75 (6), 1037–63, 1045

Black J, Hopper M, Band C (2007) Making a Success of Principles-Based Regulation. Law and Financial Markets Review, 191-206

Bodó B, Giannopoulou A (2019) The Logics of Technology Decentralisation: The Case of Distributed Ledger Technologies. In Blockchain and Web 3.0: Social, Economic, and Technical Challenges. Routledge

Bolt W, Lubbersen V, Wierts P (2021) Getting the balance right: Crypto, stablecoin and central bank digital currency. Journal of Payments Strategy & Systems, 16(1)

Borrás S, Edler J (2020) The roles of the state in the governance of socio-technical systems' transformation. Research Policy 49(5), 103971

Bossone B (2020) Money and customer funds in the world of digital finance: Who really owns what? Journal of Payments Strategy & Systems, 15(1)

Brenner M, Christin N, Johnson B, Rohloff K (2015) Financial Cryptography and Data Security. Springer Berlin Heidelberg

Brunnermeier MK, Niepelt D (2019) On the equivalence of private and public money. Journal of Monetary Economics, 106, 27-41

Capaccioli S (2020) Blockchain, Bitcoin and Stigmergy: An Explanation and a New Perspective for Regulation. BioLaw Journal 2020 (2), 467–76

Capraz S, Ozsoy A (2021) Personal Data Protection in Blockchain with Zero-Knowledge Proof. In Patnaik S et al (eds) Blockchain Technology and Innovations in Business Processes, Smart Innovation, Systems and Technologies, 219. Springer Nature Singapore Pte Ltd

Casanovas P, de Koker L, Hashmi M (2022) Law, Socio-Legal Governance, the Internet of Things, and Industry 4.0: A Middle-Out/Inside-Out Approach. Multidisciplinary Scientific Journal, 5, 64-91. MDPI

Casanovas P, González-Conejero J, de Koker L (2017) Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey. Proceedings of the 1st Workshop on Technologies for Regulatory Compliance.

Cavoukian A (2011) Privacy by design. Office of the Information and Privacy Commissioner

Cervone L, Palmirani M, Vitali F (2020) The intelligible contract. Proceedings 53rd Hawaii International Conference on System Science

Chamon M (2021) The legal framework for delegated and implementing powers ten years after the entry into force of the Lisbon Treaty. ERA Forum 22,21-38

Chaum DL (1983) Blind Signatures for Untraceable Payments. Available at: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF

Chaum DL (1985) Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM. 28(10) Available at: https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf

Chaum DL, Fiat A, Naor M (1990) Untraceable Electronic Cash. Available at: http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf

Chaum, DL (1981) Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communication of the ACM. 24(2). Available at: https://dl.acm.org/doi/10.1145/358549.358563

Chen W, Zheng Z, Ngai ECH, Zheng P, Zhou Y (2019) Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum. IEEE Access 7 (c), 37575–86

Clarke R (1999) Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice. User Identification & Privacy Protection Conference

Covolo V (2020) The EU response to criminal misuse of cryptocurrencies: The young, already outdated 5th anti-money laundering directive. European Journal of Crime, Criminal Law and Criminal Justice. 28(3), 217-251

Danezis G, Meiklejohn S (2016) Centrally banked cryptocurrencies. Network and Distributed Systems Security Symposium. Available at: http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf

Dashkevich N, Counsell S, Destefanis G (2020) Blockchain Applications for Central Banks: A Systematic Mapping Study. IEEE Access 8, 139918–52

De Domenico M, Baronchelli A (2019) The Fragility of Decentralised Trustless Socio-Technical Systems. EPJ Data Science 8 (1), 4–9

De Filippi P, Hassan S (2016) Blockchain Technology as a Regulatory Technology: from Code is Law to Law is Code. First Monday. Available at: https://firstmonday.org/ojs/index.php/fm/article/view/7113

De Filippi P, Mannan M, Reijers W (2022) The alegality of blockchain technology. Policy and Society, 41(3), 358-372, doi: https://doi.org/10.1093/polsoc/puac006

De Haro-Olmo FJ, Varela-Vaca AJ, Álvarez-Bermejo JA (2020) Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. MDPI Sensors, 20, 7171, doi:10.3390/s20247171

De Koker L (2015) Anonymous Clients, Identified Clients and the Shades in between Perspectives on the FATF AML/CFT Standards and Mobile Banking. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2634305

Defferrard M, Bresson X, Vandergheynst P (2016) Convolutional Neural Networks on Graphs with Fast Localized Spectral Filtering. 30th Conference on Neural Information Processing Systems (NIPS 2016)

Desmond DB, Lacey D, Salmon P (2019) Evaluating Cryptocurrency Laundering as a Complex Socio-Technical System: A Systematic Literature Review. Journal of Money Laundering Control 22 (3): 480–97

Dimyadi J, Governatori G, Amor R (2017) Evaluating legaldocml and legalruleml as a standard for sharing normative information in the aec/fm domain. In Proceedings Lean and Computing in Construction Congress.

Distefano B, Pocher N, Zichichi M (2020) MOATcoin: Exploring Challenges and Legal Implications of Smart Contracts through a Gamelike DApp Experiment. Cryblock 2020

Eddin AN, Bono J, Aparício D, Polido D, Ascensão JT, Bizarro P, Ripeiro P (2021) Anti-money laundering alert optimisation using machine learning with graphs. Available at: https://arxiv.org/abs/2112.07508

Eikmanns BC, Mehrwald P, Sandner PG, Welpe IM (2023) Decentralised Finance Platform Ecosystems: Conceptualisation and Outlook. Technology Analysis and Strategic Management, 1–13.

Fanti G, Pocher N (2022) Privacy in Cross-border Digital Currency: A Transatlantic Perspective. Atlantic Council GeoEconomics Center and Atlantik Brücke. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf

Fanti G, Venkatakrishnan SB, Bakshi S, Denby B, Bhargava S, Miller A, Viswanath P (2018) Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees. Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2-2, 1-35. DOI: https://doi.org/10.1145/3224424

Fanusie YJ (2020) Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them. The Digital Social Contract: A Lawfare Paper Series, November, 1–23

Ferretti S, D'Angelo G (2019) On the Ethereum blockchain structure: a complex networks theory perspective. Concurrency and Computation, 32(12), Wiley

Finck M (2019b) Blockchain and the GDPR: Can Distributed Ledgers Be Squared with European Data Protection Law? European Parliamentary Research Service

Fleder M, Kester MS, Pillai S (2015) Bitcoin Transaction Graph Analysis. Available at: https://arxiv.org/abs/1502.01657

Freni P, Ferro E, Moncada R (2020) Tokenisation and Blockchain Tokens Classification: A Morphological Framework. IEEE ISCC 2020

Froomkin AM (1995) Anonymity and Its enmities. Journal of Online Law. http:// articles.umlaw.net/froomkin/Anonymity_Enmities.htm

Gelemerova L (2009) On the Frontline against Money-Laundering: The Regulatory Minefield. Crime, Law and Social Change 52 (1): 33–55

Goforth CR (2020) Crypto Assets: A Fintech Forecast. Banking & Finance Law Review, 37

Golubova A (2021) BIS backs central bank digital currencies: Their time "has come". Available at: https://www.kitco.com/news/2021-06-23/BIS-backs-central-bankdigital-currencies-Their-time-has-come.html

Gonsalves T, Vaidyanathan L, Jhunjhunwala A (2012) Prototyping Socio-Technical Systems for Banking Services for Rural India. 2012 Computer Supported Cooperative WorkConference – Companion volume

González Galli LM, Meinardi EN (2011) The Role of Teleological Thinking in Learning the Darwinian Model of Evolution. Evo Edu Outreach 4, 145–152

Goodell G, Al-Nakib HD, Tasca P (2021) A Digital Currency Architecture for Privacy and Owner-Custodianship. Future Internet, 13. Available at: https://arxiv.org/abs/2101.05259

Goodell G, Aste T (2019) Can Cryptocurrencies Preserve Privacy and Comply With Regulations? Frontiers in Block. 2 (4)

Grigg I (2004) The Ricardian Contract. First IEEE Workshop on Electronic Contracting. Available at: https: //www.researchgate.net/publication/4085229_The_Ricardian_contract.

Grigg I (2019-2000) Financial Cryptography in 7 Layers. Available at: https://iang.org/papers/fc7.html

Grijpink J, Prins C (2001) Digital Anonymity on the Internet: New Rules for Anonymous Electronic Transactions? An Exploration of Private Law Implications of Digital Anonymity. Computer Law and Security Report 17 (6), 379–89

Gross J, Sedlmeir J, Babel M, Bechtel A, Schellinger B (2021) Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. SSRN Electronic Journal. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891121

Harrigan M, Fretter C (2016) The Unreasonable Effectiveness of Address Clustering. 2016 International IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress

Harvey J, Branco-Illodo I (2020) Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in "Privacy Coin" Whitepapers, Journal of Political Marketing, 19:1-2, 107-136, DOI: 10.1080/15377857.2019.1652223

Hashmi M, Casanovas P, de Koker L (2018) Legal Compliance Through Design: Preliminary Results of a Literature Survey. Proceedings of the 2nd Workshop on Technologies for Regulatory Compliance (TERECOM 2018) co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018)

Hassan S, De Filippi P (2017) The Expansion of Algorithmic Governance: From Code is Law to Law is Code. Special Issue 17: Artificial Intelligence and Robotics in the City. 3. Will we Succeed in Making AI Revolution Work for Everyone? Field Actions Science Reports, 88-90. Available at: https://journals.openedition.org/factsreports/4518

Helms SC (2001) Translating Privacy Values with Technology, 7 Boston University Journal of Science and Technology Law, 288, 301

Herlihy M (2018) Atomic Cross-Chain Swaps. PODC'18, July 23-27, 2018, Egham, UK, 245–54

Hofmann J, Katzenbach C, Gollatz K (2017) Between coordination and regulation: Finding the governance in Internet governance. New Media and Society 19(9), 1406-1423

Houben R (2019) Cryptocurrencies from a Money Laundering and Tax Evasion Perspective. International Company and Commercial Law Review 30 (5): 261–71

Hustinx P (2010) Privacy by design: delivering the promises. Identity in the Information Society, 3(2)

Ince P, Liu JK, Zhang P (2018) Adding Confidential Transactions to Cryptocurrency IOTA with Bulletproofs. LNCS 11058, Springer, 32-45

Inozemtsev MI (2021) Taxonomy and Typology of Crypto-Assets: Approaches of International Organisations. Lecture Notes in Networks and Systems 139, 122–33

Irwin ASM, Dawson C (2019) Following the cyber money trail. Global challenges when investigating ransomware attacks and how regulation can help. Journal of Money Laundering Control, 22(1), 110-131, Emerald

Jabbar A, Geebren A, Hussain Z, Dani S, Ul-Durar S (2022) Investigating individual privacy within CBDC: A privacy calculus perspective. Research in International Business and Finance, Elsevier. DOI: https://doi.org/10.1016/j.ribaf.2022.101826

Jabbar R, Fetais N, Kharbeche M, Krichen M, Barkaoui K, Shinoy M (2021) Blockchain for The Internet of Vehicles: How to use Blockchain to secure Vehicle-to-Everything (V2X) Communication and Payment? IEEE Sensors Journal 21, 14, 15807–15823

Jardine E (2021) Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. American Journal of Criminal Justice, 46, 980-1005

Jiaxuan Y, Ying R, Jeskovec J (2020) Design Space for Graph Neural Networks. 34th Conference on Neural Information Processing Systems (NeurIPS 2020)

Jung H, Jeong D (2021) Blockchain Implementation Method for Interoperability between CBDCs. Future Internet, 13(5)

Kaal W, Vermeulen E (2017) How to Regulate Disruptive Innovation – From Facts to Data. 57 Jurimetrics 169

Kamišalić A, Kramberger R, Fister I (2021) Synergy of blockchain technology and data mining techniques for anomaly detection. Applied Sciences (Switzerland), 11(17)

Karasek-Wojciechowicz I (2021) Reconciliation of Anti-Money Laundering Instruments and European Data Protection Requirements in Permissionless Blockchain Spaces. Journal of Cybersecurity, 1–28

Katona T (2021) Decentralized Finance: The Possibilities of a Blockchain 'Money Lego' System. Financial and Economic Review 20(1)

Kaufmann D, Kraay A (2008) Governance Indicators: Where Are We, Where Should We Be Going? The World Bank Research Observer, 23(1), Oxford University Press

Kerwer D (2005) Rules that Many Use: Standards and Global Regulation. Governance: An International Journal of Policy, Administration, and Institutions, 18(4), 611-632

Kipf TN, Welling M (2016) Semi-supervised Classification with Graph Convolutional Networks. Available at: https://arxiv.org/abs/1609.02907

Kirimhan D (2023) Importance of Anti-Money Laundering Regulations among Prosumers for a Cybersecure Decentralized Finance. Journal of Business Research, 157

Klarin A (2020) The Decade-Long Cryptocurrencies and the Blockchain Rollercoaster: Mapping the Intellectual Structure and Charting Future Directions. Research in International Business and Finance 51

Kochergin D, Dostov V (2020) Central Banks Digital Currency: Issuing and Integration Scenarios in the Monetary and Payment System. Lecture Notes in Business Information Processing, 394, 111–119

König L, Korobeinikova Y, Tjoa S, Kieseberg P (2020) Comparing Blockchain Standards and Recommendations. 12, 222, Future Internet, MDPI

Kopackova H, Libalova P (2017) Smart city concept as socio-technical system. Proceedings of the International Conference on Information and Digital Technologies

Koshy P, Koshy D, McDaniel P (2014) An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In Int. Fin. Crypt. Ass. 2014, 8437, 469–85

Kranzberg M (1986) Technology and History: Kranzberg's Laws. 27 Technology and Culture 544, 545

Kuch P (2022) Teleology - the Missing Piece to Solving the GDPR Puzzle. Journal of Data Protection & Privacy, 5 (1) Henry Stewart Publications

Le Nguyen C (2018) Preventing the Use of Financial Institutions for Money Laundering and the Implications for Financial Privacy. Journal of Money Laundering Control 21 (1), 47–58

Leavitt H (1965) Applied organisationalchange in industry: Structural, technological and humanistic approaches. Handbook of organisations, 1144-1170

Leibbrandt G, Goldscheider D (2021) Building a global digital identity infrastructure. Journal of Payments Strategy & Systems, 16(1)

Lessig L (1996) The Zones of Cyberspace. 48 Stanford Law Review 1403, 1408

Lessig L (1998) The New Chicago School. Journal of Legal Studies 27, S2, 661–691

Li Y, Susilo W, Yang G, Yu Y, Du X, Liu D, Guizani N (2019) Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies. IEEE Network 33 (5), 111–17

Li Y, Yang G, Susilo W, Yu Y, Ho Au M, Liu D (2021) Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. IEEE Transactions on Dependable and Secure Computing 18 (2), 679-691

Li Z, Xiang Z, Gong W, Wang H (2022) Unified model for collective and point anomaly detection using stacked temporal convolution networks. Applied Intelligence, 52(3), 3118-3131

Lin L (2019) Deconstructing Decentralized Exchanges. Stanford Journal of Blockchain Law and Policy 2 (1): 58–77

Linder S (1999) Coming to Terms with the Public-Private Partnerships. A Grammar of Multiple Meanings. American Behavioural Scientistic 43(1), 35-51

Lindsey LB (1999) The Money-Laundering Conundrum: Mugging Privacy in the Assault on Crime? The Future of Financial Privacy, Nov, 164–73

Lischke M, Fabian B (2016) Analyzing the Bitcoin Network: The First Four Years. Future Internet 8 (1)

Lootsma Y (2017) Blockchain as the Newest Regtech Application - the Opportunity to Reduce the Burden of KYC for Financial Institutions Banking & Financial Services Policy Report 36 (8) 16–21

Lorenz J, Silva IS, Aparício D, Ascensão JT, Bizarro P (2021) Machine Learning Methods to Detect Money Laundering in the Bitcoin Blockchain in the Presence of Label Scarcity. Proceedings of the First ACM International Conference on AI in Finance

Mabunda S (2018) Cryptocurrency: The New Face of Cyber Money Laundering. In IcABCD 2018, 1–6. IEEE

Marsden C (2011) Internet Co-regulation and Constitutionalism: Towards a More Nuanced View, 10. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1973328

Maupin JA (2017) Mapping the Global Legal Landscape of Blockchain Technologies. CIGI Papers. Available at: https://www.cigionline.org/sites/default/files/documents/Paper%20no.149.pdf

May TC (1988) The Crypto-Anarchist Manifesto. Available at: https://nakamotoinstitute.org/authors/timothy-c-may/

Meijer A, Thaens M (2018) Urban Technological Innovation: Developing and Testing a Sociotechnical Framework forStudying Smart City Projects. Urban Affairs Review 54(2), 363-387

Meiklejohn S, Orlandi C (2015) Privacy-Enhancing Overlays in Bitcoin. In Brenner M, Christin N, Johnson B, Rohloff K (eds) Financial Cryptography and Data Security. Springer Berlin Heidelberg

Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S (2016) A Fistful of Bitcoins: Characterising Payments among Men with No Names. Research Highlights. The ACM. 59-4

Mercan S, Kurt A, Erdin E, Akkaya K (2021) Cryptocurrency Solutions to Enable Micro-Payments in Consumer IoT. IEEE CEM

Merchant GE, Allenby B (2017) Soft law: New tools for governing emerging technologies. Bulletin of the Atomic Scientists, 73(2), 108-114

Moreno-Sanchez P, Zafar MB, Kate A (2016) Listening to whispers of ripple: Linking wallets and deanonymising transactions in the ripple network. Proceedings of Privacy Enhancing

Technology, 2016(4). Available at: https://www.researchgate.net/publication/305423583_Listening_to_Whispers_of_Ripple_Linking_Wallets_and_Deanonymizing_Transactions_in_the_Ripple_Network

Murphy S, Cooper C (2016) Can smart contracts be legally binding contracts? White paper, R3cev and Norton Rose Fulbright. Available at: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/norton-rose-fulbright--r3-smart-contracts-white-paper-key-findings-nov-2016.pdf

Nabilou H (2019) Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies. Journal of Banking Regulation, 21(4), 299-314.

Nadler M, Schär F (2023) Tornado Cash and Blockchain Privacy : A Primer for Economists and Policymakers. 1–15. Federal Reserve Bank of St. Louis Review

Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash Systems. Available at: https://www.bitcoin.org.

Nerurkar P, Patel D, Busnel Y, Ludinard R, Kumari S, Khan MK (2021) Dissecting bitcoin blockchain: Empirical analysis of bitcoin network. Journal of Network and Computer Applications, 177, 102940. Elsevier

Neudecker T, Hartenstein H (2017) Could Network Inf. Facilitate Address Clustering in Bitcoin? 10323 LNCS: 155–69

Newman A, Bach D (2014) The European Union as hardening agent: soft law and the diffusion of global financial regulation. Journal of European Public Policy, 21(3), 430-452

Oad A, Razaque A, Tolemyssov A, Alotaibi M, Alotaibi B, Zhao C (2021) Blockchain-enabled transaction scanning method for money laundering detection. Electronics, 10 (15)

Ober M, Katzenbeisser S, Hamacher K (2013) Structure and Anonymity of the Bitcoin Transaction Graph. Future Internet 5 (2)

Ojo M (2021) Balancing public-private partnerships in a digital age: CBDCs, central banks and technology firms. Munich Personal RePEc Archive. Available at: https://mpra.ub.uni-muenchen.de/107716/

Oliveira C, Torres J, Silva MI, Aparício D, Ascensão JT, Bizarro P (2021) Guiltywalker: Distance to Illicit Nodes in the Bitcoin Network. Available at: https://arxiv.org/abs/2102.05373

Oliveira L, Bauer I, Zavolokina L, Schwabe G (2018) To token or not to token: Tools for understanding blockchain tokens. ICIS 2018

Opare EA, Kim K (2020) A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures. IEEE Access, 8, 810–847

Orr DA, Lancaster DM (2018) Cryptocurrency and the Blockchain: A Discussion of Forensic Needs. International Journal of Cyber-Security and Digital Forensics, 7(4), 420-435. SDIWC

Pagallo U, Casanovas P, Madelin R (2019) The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. Theory and Practice of Legislation 7(1), 1-25.

Palmirani M (2011) Legislative change management with akoma-ntoso. In Legislative XML for the semantic Web, 101-130

Palmirani M, Governatori G, Athan T, Boley H, Paschke A, Wyner A (2017) Legalruleml core specification version 1.0. OASIS standard.

Palmirani M, Sperberg R, Vergottini G, Vitali F (2018) Akoma ntoso version 1.0 part 1: Xml vocabulary. OASIS standard

Palmirani M, Vitali F (2011) Akoma-ntoso for legal documents. In Legislative XML for the semantic Web, 75-100

Patnaik S et al (2021) Blockchain Technology and Innovations in Business Processes, Smart Innovation, Systems and Technologies, 219. Springer Nature Singapore Pte Ltd

Peroni S, Palmirani M, Vitali F (2017) Undo: the United Nations system document ontology. In International Semantic Web Conference, 175-183

Pfitzmann A, Hansen M (2010) A Terminology for Talking about Privacy by Data Minimisation: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. T. U. Dresden, 1–98. Available at: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf

Poblet M, Allen DWE, Konashevych O, Lane A (2020) From Athens to the Blockchain: Oracles for Digital Democracy. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630713

Pocher N, Veneris A (2022b) Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme. IEEE Transactions on Network and Service Management, 19(2), 1776-88

Pocher N, Zichichi M (2022) Towards CBDC-based Machine-to-Machine Payments in Consumer IoT. In: Proceedings of the 37th ACM/SIGAPP Symposium On Applied Computing. Available at: http://hdl.handle.net/11585/843221

Pocher N, Zichichi M, Merizzi F, Shafiq MZ, Ferretti S (2022) Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics. Version 2. Available at: https://arxiv.org/abs/2206.04803

Pocher N, Zichichi M, Ferretti S (2023) The AML/CFT/CPF application of on-chain analytics and machine learning: overview and open issues. AIGEL CEUR WP. Forthcoming.

Prasad R, Rohokale V (2020) Internet of Things (IoT) and Machine to Machine (M2M) Communication. In: Cyber Security: The Lifeline of Information and Communication Technology. Springer, 125–141

Puzis R, Barshap G, Zilberman P, Leiba O (2019) Controllable Privacy Preserving Blockchain: Fiatchain: Distributed Privacy Preserving Cryptocurrency with Law Enforcement Capabilities. LNCS. 11527. Springer.

Ranchordás S (2015) Innovation Experimentalism in the Age of the Sharing Economy. 19 Lewis & Clark Law Rev. 871

Reid F Harrigan M (2013) An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds) Security and Privacy in Social Networks. Springer

Reidenberg J (1998) Lex Informatica: The Formulation of Information Policy Rules Through Technology. 76 Texas Law Review 3, 552, 556

Rennie E, Steele S (2021) Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency. Law, Technology and Humans, 3(1)

Renwick R, Gleasure R (2020) Those Who Control the Code Control the Rules: How Different Perspectives of Privacy Are Being Written into the Code of Blockchain Systems. Journal of Information Technology, 36(1), SAGE Publishing

Reyes C (2016) Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. 61 Villanova Law Review

Reyes CL (2017) Conceptualising Cryptolaw. Nebraska Law Review(2), 384-445

Reynolds P, Irwin ASM (2017) Tracking Digital Footprint: Anonymity within the Bitcoin System. Journal of Money Laundering Control 20 (2), 172-89

Rogaway P (2016) The Moral Character of Cryptographic Work. Available at: https://www.semanticscholar.org/paper/The-Moral-Character-of-Cryptographic-Work-Rogaway/e0cba1366501846d11a6a4b40840a10deb5b2fe8

Ross TW, Yan J (2015) Comparing Public–Private Partnerships and Traditional Public Procurement: Efficiency vs. Flexibility. Journal of Comparative Policy Analysis: Research and Practice 17(5), 448-466

Salmensuu C (2018) The General Data Protection Regulation and Blockchains. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143992

Sardá T, Natale S, Sotirakopoulos N, Monaghan M (2019) Understanding Online Anonymity. Media, Culture and Society 41 (4), 557–64

Savas ES (2000) Privatisation and Public-Private Partnerships. New York: Chatham House

Schweizer A, Knoll P, Urbach N, von der Gracht HA, Hardjono T (2020) To what extent will blockchain drive the machine economy? Perspectives from a prospective study. IEEE TEM, 67(4), 1169–1183

Scott J, Trubek D (2002) Mind the Gap: Law and New Approaches to Governance in the European Union. 8 European Law Journal 1, 4–6

Serena L, Ferretti S, D'Angelo G (2022) Cryptocurrencies activity as a complex network: Analysis of transaction graphs. Peer-to-Peer Networking and Applications, 15, 839-853

Shayegan MJ, Sabor HR, Uddin M, Chen CL (2022) A collective anomaly detection technique to detect crypto wallet frauds on bitcoin network. Symmetry, 14 (2)

Siena J (2022) Distributed Ledger Technology: Cutting through the Paradox. Journal of Securities Operations & Custody. 15 (1): 28–44

Silva Ramalho D, Igreja Matos N (2021) What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. ERA Forum 22:487-506, DOI: 10.1007/s12027-021-00676-4

Sin YF, Moroney R, Strydom M (2015) Principles-Based versus Rules-Based Auditing Standards: The Effect of the Transition from AS2 to AS5. International Journal of Auditing, 19, 282-294

Skopek JM (2015) Reasonable Expectations of Anonymity.Virginia Law Review 101, 691–762

Stephen A, Christopher R, Huseyin D et al (2016) A "Soft" Approach to Analysing Mobile Financial Services Socio- Technical Systems. Proceedings of the 30th International BCS Human Computer Interaction Conference

Sun X, Zhang J, Zhao Q, Liu S, Chen J, Zhuang R, Cheng X (2021) Cubeflow: Money Laundering Detection with Coupled Tensors. Pacific-Asia Conference on Knowledge Discovery and Data Mining

Surden H (2012) Computable Contracts. University of California, Davis, 46-629

Szabo N (2017) Money, Blockchains, and Social Scalability. Available at: http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html

Tapscott D, Euchner J (2019) Blockchain and the Internet of Value: An Interview with Don Tapscott. Research Technology Management 62 (1), 12–19

Tasca P, Tessone C J (2018) Taxonomy of Blockchain Technologies. Principles of Identification and Classification. Available at: https://arxiv.org/pdf/1708.04872.pdf

Taubenheim J (2019) Integrating blockchain technology into IoT: 3 vendor profiles. Available at: https://www.machnation.com/2019/09/11/integrating-blockchain-technology-into-iot-3-vendor-profiles/

Tennant L (2017) Improving the Anonymity of the IOTA Cryptocurrency. 1–20

Tian H, Luo P, Su Y (2020) Group Signature Based Digital Currency System. 1156, CCIS. Springer

Trubek DM, Trubek, LG (2007) New governance & legal regulation: Complementarity, rivalry, and transformation. Columbia Journal of European Law 13(3), 539-564.

Tsuchiya Y, Hiramoto N (2021a) Dark web in the dark: Investigating when transactions take place on cryptomarkets. Forensic Science International: Digital Investigation, 36, Elsevier

Tsuchiya Y, Hiramoto N (2021b) How cryptocurrency is laundered: Case study of Coincheck hacking incident. Forensic Science International: Reports 4 100241, Elsevier

Veneris A, Park A, Long F, Puri P (2021) Central Bank Digital Loonie: Canadian Cash for a New Global Economy. Available at: https://ssrn.com/abstract=3770024

Verbruggen P (2009) Does Co-Regulation Strengthen EU Legitimacy? 15 European Law Journal 425, 426

Viñuela C, Sapena J, Wandosell G (2020) The future of money and the central bank digital currency dilemma. Sustainability (Switzerland), 12(22)

Vitali F, Palmirani M, Parisse V (2019) Akoma ntoso naming convention version 1.0. OASIS standard

Vitali F, Palmirani M, Sperberg R, Parisse V (2018) Akoma ntoso version 1.0. part 2: Specifications. OASIS standard

Viterbo A (2019) The European Union in the Transnational Financial Regulatory Arena: The Case of the Basel Committee on Banking Supervision. Journal of International Economic Law, 22, 205-228, Oxford University Press

Vogel D (2008) Private Global Business Regulation. Annual Review of Political Science, 11, 261-82

Vutsova A, Ignatova O (2014) The role of public-private partnership for effective technology transfer. Applied Technologies and Innovations 10(3), 83-90

Walch A (2017) Blockchain's Treacherous Vocabulary: One More Challenge for Regulators. Journal of Internet Law 21 (2)

Walch A (2018) In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. The Blockchain Revolution: Legal and Policy Challenges. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198

Wang F, De Filippi P (2020) Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain

Weber M, Chen J, Suzumura T, Pareja A, Ma T, Kanezashi H, Kaler T, Leiserson CE, Schardl TB (2018) Scalable Graph Learning for Anti-Money Laundering: A First Look. Available at: https://arxiv.org/abs/1812.00076

Weber M, Domeniconi G, Chen J, Weidele DKI, Bellei C, Robinson T (2019) Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. KDD 2019, Workshop on Anomaly Detection in Finance, ACM

Weber R, Heinrich U (2012) Anonymisation. SpringerBriefs in Cybersecurity. Springer

Werbach K (2020) The Siren Song: Algorithmic Governance by Blockchain. After the Digital Tornado: Networks, Algorithms, Humanity. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578610

Werbach K, Cornell N (2017) Contracts ex Machina. Duke Law Journal 67, 101–170

Westermeier C (2022) From Flows towards Updates: Security Regimes and Changing Technologies for Financial Surveillance. Review of International Studies, 1–22

Wright A, De Filippi P (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

Wu M, McTighe W, Wang K, Seres IA, Bax N, Puebla M, Mendez M (2022) Tutela: An Open-Source Tool for Assessing User-Privacy on Ethereum and Tornado Cash. Available at: https://arxiv.org/pdf/2201.06811.pdf

Wu T (2003) When Code Isn't Law. 89 Virginia Law Review 103, 106.

Wu Y, Tao F, Liu L, Panneerselvam J, Zhu R, Shahzad MN (2020) A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation. IEEE Transactions on Network Science and Engineering, 8-2

Xia F, Liu J, Nie H, Fu Y, Wan L, Kong X (2020) Random Walks: A Review of Algorithms and Applications. IEEE Transactions on Emerging Topics in Computational Intelligence, 4(2), 95-107

Yao Q (2018) A systematic framework to understand central bank digital currency. Science China Information Sciences, 61(3). Available at: http://scis.scichina.com/en/2018/033101.pdf

Yeung K (2017) Hypernudge: Big Data as a mode of regulation by design. Information, Communication & Society, 20(1), 118-136

Yeung K (2019) Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law. Modern Law Review 82 (2), 207–39

Yin HHS, Langenheldt K, Harlev M, Mukkamala RR, Vatrapu R (2019) Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymising the Bitcoin Blockchain. Journal of Management Information Systems, 36-1. Taylor & Francis

Yousaf H, Kappos G, Meiklejohn S (2019) Tracing Transactions Across Cryptocurrency Ledgers. Proceedings of the 28th USENIX Security Symposium. Available at: https://www.usenix.org/system/files/sec19-yousaf_0.pdf

Yuen TH (2020) PAChain: Private, Authenticated & Auditable Consortium Blockchain and Its Implementation. Future Generation Computer Systems, 112. Springer

Yuen TH (2019) PAChain: Private, Authenticated and Auditable Consortium Blockchain. In Mu Y et al (eds) CANS 2019, LNCS 11829, 214-234, Springer

Zetzsche DA, Arner DW, Buckley RP (2020) Decentralized Finance. Journal of Financial Regulation, 6(2)

Zuech K, Wöhnert K H, Skwarek V (2019) Derivation of Categories for Interoperability of Blockchain and Distributed Ledger Systems. Informatik 2019. LNI

Zunzunegui F (2022) How to regulate digital financial platforms: A research agenda. Revista de Derecho del Mercado Financiero, Working paper 3/2022

3. Legislation, Regulation, Standards, Guidelines, Communications

Commission Delegated Regulation (EU) 2018/1108 of 7 May 2018 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regulatory technical standards on the criteria for the appointment of central contact points for electronic money issuers and payment service providers and with rules on their functions

Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries

Communication from the Commission (2019) - Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework. COM/2019/360 final

Communication from the Commission (2020) on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing. 2020/C 164/06

Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, replaced by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

Council of Europe (1990) ETS No. 141. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime. Opened on 8 Nov. 1990, entered into force on 1 Sep. 1993. Available at: https://rm.coe.int/168007bd23

Council of Europe (2005) CETS No. 198. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. Opened on 16 May 2005 and entered into force on 1 May 2008. Available at: https://rm.coe.int/168008371f

Council of the European Union (2022a) Information Note regarding Interinstitutional File: 2020/0265 (Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)). Compromise text endorsed by the Permanent Representative Committee on 5 October 2022. Available at: https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf

Council of the European Union (2022b) Information Note regarding Interinstitutional File: 2021/0241 (Proposal for a Regulation of the European Parliament and of the Council on Information Accompanying Transfers of Funds and Certain Crypto-assets (recast)). Compromise text endorsed by the Permanent Representative Committee on 5 October 2022. Available at: https://data.consilium.europa.eu/doc/document/ST-13215-2022-INIT/en/pdf

Council of the European Union (2022c) Mandate for negotiations with the European Parliament. Institutional File: 2021/0239 (Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing). Text endorsed on 5 December 2022. Available at: https://www.consilium.europa.eu//media/60610/st15517-en22.pdf

Council of the European Union (2022d) Mandate for negotiations with the European Parliament. Institutional File: 2021/0250 (Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering and terrorist financing and repealing Directive (EU) 2015/849). Text endorsed on 5 December 2022. Available at: https://www.consilium.europa.eu//media/60612/st15519-en22.pdf

Council Regulation (EC) No 2157/2001 of 8 October 2001 on the Statute for a European company (SE)

Decreto Nº 57, del 8 de Junio del año 2021, publicado en el Diario Oficial de la Republica de El Salvador en la America Central Nº 110, Tomo 431, de fecha 9 de Junio del año 2021, "Ley Bitcoin". Available at: https://www.diariooficial.gob.sv/diarios/do-2021/06-junio/09-06-2021.pdf

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

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

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU and lastly by Directive (EU) 2019/2177 of the European Parliament and of the Council of 18 December 2019 amending Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Directive 2014/65/EU on markets in financial instruments and Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing

Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

Directive (EU) 2018/1673 of the European Parliament and the Council of 23 October 2018 on Combating Money Laundering by Criminal Law

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

Directive (EU) 2019/1153 of the European Parliament and the Council of 20 June 2019 laying down rules facilitation the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

European Banking Authority (2017) Final report on joint draft regulatory technical standards on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to Article 45(9) of Directive (EU) 2015/849 is appropriate and the functions of the central contact point. Available at: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1890699/dae7b11d-1c7c-4995-ae9d-b48bfb6e1048/Final%20Draft%20RTS%20on%20CCP%20to%20strengthen%20fight%20against%20financial%20crime%20%28JC%202017%2008%29.pdf?retry=1

European Banking Authority (2019) Report with Advice for the European Commission on Crypto-Assets. Available at: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf

European Banking Authority (2021) Final report on draft regulatory technical standards under Article 9a (1) and (3) of Regulation (EU) No 1093/2010 setting up an AML/CFT central database and specifying the materiality of weaknesses, the type of information collected, the practical implementation of the information collection and the analysis and dissemination of the information contained therein. Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2021/1025576/RTS%20on%20AML%20CFT%20central%20data%20base.pdf

European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority (2017) Final report on Draft Joint

Regulatory Technical Standards on the measures credit institutions and financial institutions shall take to mitigate the risk of money laundering and terrorist financing where a third country's law does not permit the application of group-wide policies and procedures. Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2017/JC%20RTS%20on%20the%20implementation%20of%20group%20wide%20AML-CFT%20policies%20in%20third%20countries%20/1035746/Final%20Report%20on%20Joint%20RTS%20on%203rd%20countries.pdf

European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority (2021) Final Report on draft Technical Standards with regard to the content and presentation of disclosures pursuant to Article 8(4), 9(6) and 11(5) of Regulation (EU) 2019/2088. Available at: https://www.esma.europa.eu/sites/default/files/library/jc_2021_50_-_final_report_on_taxonomy-related_product_disclosure_rts.pdf

European Commission (2003) Interinstitutional Agreement on Better Law-Making. OJ C 321/ 01

European Commission (2016) Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making. OJ L 123/01

European Commission (2018) FinTech Action plan: For a more competitive and innovative European financial sector. COM(2018) 109 final

European Commission (2020a) Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology

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

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

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

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

European Commission (2021d) Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM(2021) 423 final

European Commission (2021e) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final

European Commission (2020c) Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing. 2020/C 164/06

European Commission (2019) 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

European Court of Justice (2001) Judgment (Second Chamber) of 2 September 2001. Case C-790/19. Parchetul de pe lângă Tribunalul Braşov v LG and MH. Request for a preliminary ruling from the Curtea de Apel Braşov. Reference for a preliminary ruling – Prevention of the use of the financial system for the purposes of money laundering and terrorist financing – Directive (EU) 2015/849 – Directive 2005/60/EC – Offence of money laundering – Laundering by the perpetrator of the predicate offence ("self-laundering"). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62019CJ0790

FATF (2021b) International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations. Last Updated: October 2021. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FINTRAC (2019) Canada's Legislation: The Proceeds of Crime (Money Laundering) and Terrorist Financing Act. 31 U.S.C. Title 31 - Money and Finance, Subtitle IV - Money, Chapter 53 – Monetary Transactions, Subchapter II - Records and Reports on Monetary Instruments Trans, Sec. 5331 - Reports relating to coins and currency received in nonfinancial trade or business

ISO/TC 307. Available at: https://www.iso.org/committee/6266604/x/catalogue/p/1/u/0/w/0/d/0

ISO (2017) ISO/IEC 30182:2017, Smart city concept model. Guidance for establishing a model for data interoperability

ISO (2013) 16759:2013, concerning Graphic technology – Quantification and communication for calculating the carbon footprint of print media products

ITU-T FG DLT (2019a) Distributed Ledger Technology Terms and Definitions. FG DLT D1.1

ITU-T FG DLT (2019b) Technical Report FG DLT D1.2 Distributed Ledger Technology Overview, Concepts, Ecosystem

ITU-T FG DLT (2019c) Distributed Ledger Technology Regulatory Framework. Technical Report FG DLT D4.1

ITU-T Focus Group on Digital Currency (2019) Taxonomy and definition of terms for digital fiat currency

Law No. 22.004 of 22 April 2022 governing cryptocurrency in the Central African Republic. Text available in Frech at: http://www.droit-afrique.com/uploads/RCA-Loi-2022-04-crypto-monnaie.pdf

Liechtenstein's Gesetz über Token und VT-Dienstleister (2019) vom 3. Oktober 2019 (Token- und VT-Dienstleister-Gesetz; TVTG). English translation available at https://www.regierung.li/media/medienarchiv/950_6_08_01_2020.pdf?t=2

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

Regulation (EU) 2018/1672 Of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005

Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) 1094/ 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds.

Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final

UN General Assembly (1988) Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. Opened on 20 Dec. 1988, entered into force on 11 Nov. 1990. Available at: https://www.unodc.org/pdf/convention_1988_en.pdf

UN General Assembly (1999) Convention for the Suppression of the Financing of Terrorism. Opened on 9 Dec. 1999, entered into force on 10 Apr. 2002. Available at: https://treaties.un.org/doc/db/terrorism/english-18-11.pdf

UN General Assembly (2000) Convention Against Transnational Organised Crime. Res. 55/25 of 15 Nov. 2000, into force on 29 Sep. 2003. Available at: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf. Three Protocols: (1) to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children. Res. 55/25 of 15 November 2000, into force on 25 Dec. 2003. (2) Against the Smuggling of Migrants by Land, Sea and Air. Res. 55/25 of 15 Nov. 2000, into force on 28 Jan. 2004. (3) Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. Res. 55/255 of 31 May 2001, into force on 3 Jul. 2005

UN General Assembly (2003) Res. 58/4 of 31 October 2003. Convention against Corruption. Opened on 9 Dec. 2003, entered into force on 14 Dec. 2003. Available at: https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

US Presidential Actions (2022) Executive Order on Ensuring Responsible Development of Digital Assets. March 9, 2022. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets

4. Institutional Reports and Working Papers

Adrian T (2020) Evolving to Work Better Together: Public-Private Partnerships for Digital Payments. International Monetary Fund. Available at: https://www.imf.org/en/News/Articles/2020/07/22/sp072220-public-privatepartnerships-for-digital-payments

Adrian T, Mancini-Griffoli T (2019) The Rise of Digital Money. IMF FinTech Note No. 19/10. International Monetary Fund. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097

Allen JG, Rauchs M, Blandin A, Bear K (2020) Legal and Regulatory Considerations for Digital Assets. University of Cambridge. Available at: https://www.jbs.cam.ac.uk/faculty-research/centres/alternativefinance/publications/legal-and-regulatory-considerations-for-digital-assets

Allen S, Capkun S, Eyal I et al (2020) Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. IZA Institute. Available at: https://ftp.iza.org/dp13535.pdf

Amsden Z, Arora R, Bano S, Baudet M, Blackshear S, Bothra A, Cabrera G (2019) The Libra Blockchain - White Paper, 1–29. Available at: https://diemdevelopers-components.netlify.app/papers/the-diem-blockchain/2019-06-25.pdf

Arab Monetary Fund (2022) Arab Monetary Fund Releases a Study on "Trends of Issuing CBDCs in the Arab Region". Available at: https://www.amf.org.ae/en/content/arab-monetary-fund-releases-study-trends-issuing-central-bank-digital-currencies-cbdcs-arab

Aramonte S, Huang W, Schrimpf A (2021) DeFi Risks and the Decentralisation Illusion. BIS Quarterly Review. Available at: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf

Article 19 (2015) Right to Online Anonymity - Policy Brief. Available at: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

Article 29 Data Protection Working Party (2014) Opinion 05/2014 on Anonymisation Techniques. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Auer R (2022) Embedded Supervision: How to Build Regulation into Decentralised Finance. CESIFO Working Papers 9771. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4127658#

Also published as Working Paper No. 811 Bank for International Settlements. Available at: https://www.bis.org/publ/work811.pdf

Auer R, Banka H, Boakye-Adjei NY, Faragallah A, Frost J, Natarajan H, Prenio J (2022) Central bank digital currencies: a new tool in the financial inclusion toolkit? Bank for International Settlements. Available at: https://www.bis.org/fsi/publ/insights41.htm

Auer R, Boar C, Cornelli G, Frost J, Holden H, Wehrli A (2021) CBDCs beyond borders: results from a survey of central banks. Bank for International Settlements. Available at: https://www.bis.org/publ/bppdf/bispap116.ht

Auer R, Cornelli G, Frost J (2020) Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies. Bank for International Settlements. Available at: https://www.bis.org/publ/work880.htm

Auer R, Farag M, Lewrick U, Orazem L, Zoss M (2022) Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies. BIS Working Paper No 1013. Bank for International Settlements. Available at: https://www.bis.org/publ/work1013.htm

Auer R, Haene P, Holden H (2021) Multi-CBDC arrangements and the future of cross-border payments. Bank for International Settlements. Available at: https://www.bis.org/publ/bppdf/bispap115.htm

Bank of Canada (2020) Contingency Planning for a Central Bank Digital Currency. Available at: https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/

Barotini C, Holden H (2019) Proceeding with caution. A survey on central bank digital currency. Bank for International Settlements, 101. Available at: https://www.bis.org/publ/bppdf/bispap101.htm

BIS (2020) Central bank digital currencies: foundational principles and core features. Bank for International Settlements. Available at: https://www.bis.org/publ/othp33.htm

BIS (2021) CBDCs: an opportunity for the monetary system. Bank for International Settlements. Available at: https://www.bis.org/publ/arpdf/ar2021e3.pdf

BIS (2022) Project Dunbar: International settlements using multi-CBDCs. Bank for International Settlements. Available at: https://www.bis.org/publ/othp47.pdf

BIS Innovation Hub Hong Kong Centre, HKMA, Bank of Thailand, Digital Currency Institute PBoC, Central Bank UAE (2021) Inthanon-LionRock to mBridge: Building a multi CBDC platform for international payments. Bank for International Settlements. Available at: https://www.bis.org/publ/othp40.htm

BIS Innovation Hub Hong Kong Centre, HKMA (2022) Project Aurum: A Prototype for Two-tier Central Bank Digital Currency (CBDC). Bank for International Settlements. Available at: https://www.bis.org/publ/othp57.pdf

Blandin A, Pieters G, Wu Y, Eisermann T, Dek A, Taylor S, Njoki D (2020) 3rd Global Cryptoasset Benchmarking Study. Cambridge Judge Business School. Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2021/01/2021-ccaf-3rd-global-cryptoasset-benchmarking-study.pdf

Boar C, Holden H, Wadsworth A (2020) Impending arrival - a sequel to the survey on central bank digital currency. Bank for International Settlements. Available at: https://www.bis.org/publ/bppdf/bispap107.htm

Board of Governors of the Federal Reserve System (2022) Money and Payments: The US Dollar in the Age of Digital Transformation. The Federal Reserve. Available at: https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

Bossu W, Itatani M, Margulis C, et al (2020) Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law. International Monetary Fund. Available: https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827

Bullmann D, Klemm J, Pinna A (2019) In Search for Stability in Crypto-Assets: Are Stablecoins the Solution? Occasional Paper Series. European Central Bank. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf

Buterin V (2013) Ethereum whitepaper. Ethereum Foundation. Available at: https://ethereum.org/en/whitepaper/

Carstens A (2021) Digital Currencies and the Future Monetary System. Hoover Institution Policy Seminar, 89(1). Bank for International Settlements. Available at: https://www.bis.org/speeches/sp210127.pdf

Casey M, Crane J, Gensler G, Johnson S, Narula N (2018) The Impact of Blockchain Technology on Finance: A Catalyst for Change. Geneva Reports. International Center for Monetary and Banking Studies (ICMB). Available at: https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change

Chainalysis (2022) The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime. February 2022. Available at: https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Chaum D, Grothoff C, Moser T (2021) How to Issue a Central Bank Digital Currency. Swiss National Bank. Available at: https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03

CipherTrace (2021) Cryptocurrency Crime and Anti-Money Laundering Report, p 6. Available at: https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/

Codruta B, Wehrli A (2021) Ready, steady, go? – Results of the third BIS survey on central bank digital currency. Bank for International Settlements. Available at: https://www.bis.org/publ/bppdf/bispap114.pdf

Cuervo C, Morozova A, Sugimoto N (2019) Regulation of Crypto Assets. FinTech Notes. International Monetary Fund. Available at https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Regulation-of-Crypto-Assets-48810

Dabrowski M, Janikowski L (2018) Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead. Monetary Dialogue Papers. European Parliament. Available at: https://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf

Department of the Treasury FinCEN Guidance (2013) Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Available at: https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering

Department of the Treasury FinCEN (2019) Guidance on the application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies. Available at: https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

Digital Euro Association (2023) Privacy and Central Bank Digital Currencies. Available at: https://7869715.fs1.hubspotusercontent-na1.net/hubfs/7869715/Privacy%20and%20CBDCs%20-%20Digital%20Euro%20Association%20Working%20Group.pdf

Duarte A, Frost J, Gambacorta L, Koo Wilkens P, Song Shin H (2022) Central banks, the monetary system and public payment infrastructures: lessons from Brazil's Pix. Bank for International Settlements. Available at: https://www.bis.org/publ/bisbull52.pdf

Duffie D (2020) Interoperable Payment Systems and the Role of Central Bank Digital Currencies. Finance and Insurance Reloaded, Institut Louis Bachelier Annual Report. Available at: https://www.darrellduffie.com/uploads/policy/DuffiePaymentInteropMay2020.pdf

Duffie D, Economy E (2022) Digital Currencies. The US, China, and the World at a Crossroads. Hoover Institution Press, Stanford University. Available at: https://www.hoover.org/research/digital-currencies-us-china-and-world-crossroads

Ecorys and Centre for European Policy Studies (2017) Study on an EU initiative for a restriction on payments in cash. Available at: https://ec.europa.eu/info/sites/default/files/economy-finance/final_report_study_on_an_eu_initative_ecorys_180206.pdf

European Central Bank (2019) Exploring Anonymity in Central Bank Digital Currencies. In Focus. Available at: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

European Central Bank (2020a) Report on a digital euro. Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

European Central Bank (2020b) Tiered CBDC and the financial system. Available at: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf

European Central Bank (2021a) Eurosystem report on the public consultation on a digital euro. Available at: https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

European Central Bank (2021b) Press Release 14 July 2021. Eurosystem launches digital euro project. Available at: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

European Central Bank (2022a) Progress on the investigation phase of a digital euro. Available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf?8eec0678b57e98372a7ae6b59047604b

European Central Bank (2022b) Progress on the investigation phase of a digital euro – second report. Available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221221_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071

European Central Bank and Bank of Japan (2020) Balancing Confidentiality and Auditability in a Distributed Ledger Environment. Available at: https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf

European Central Bank Crypto-Assets Task Force (2019) Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

European Parliamentary Research Service (2023) Anti-Money Laundering Authority (AMLA). Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733645/EPRS_BRI(2022)733645_EN.pdf

European Securities and Markets Authority (2019) Advice - Initial Coin Offerings and Crypto-Assets. Available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

Financial Action Task Force (2014) Virtual Currencies – Key Definitions and Potential AML/CFT Risks. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Action Task Force (2015) Guidance for a Risk-Based Approach: Virtual Currencies. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

Financial Action Task Force (2019) Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

Financial Action Task Force (2020a) 12-Month Review of the Revised FATF Standards – Virtual Assets and Virtual Asset Service Providers. July 2020. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

Financial Action Task Force (2020b) FATF Report to the G20 Finance Ministers and Central Banks Governors on So-called Stablecoins. June 2020. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf

Financial Action Task Force (2020c) Guidance on Digital ID. March 2020. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

Financial Action Task Force (2020d) Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Financial Action Task Force (2021a) High-Risk Jurisdictions subject to a Call for Action. Available at: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-october-2021.html

Financial Action Task Force (2021c) Jurisdictions under Increased Monitoring. Available at: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html

Financial Action Task Force (2021d) Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. July 2021. Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

Financial Action Task Force (2021e) Virtual Assets and Virtual Asset Service Providers - Updated Guidance for a Risk-Based Approach. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

Financial Action Task Force (2021f) Guidance on Risk-Based Supervision. March 2021. Available at: http://www.fatf-gafi.org/media/fatf/documents/Guidance-Risk-Based-Supervision.pdf

Financial Stability Board (2019) Regulatory Issues of Stablecoins. Available at: https://www.fsb.org/wp-content/uploads/P181019.pdf

Forster M, Gross J, Kamping AK, Katilmis S, Reichel M, Sandner P, Schröder P (2021) The future of payments: programmable payments in the IoT sector. PPI. Available at: https://www.ppi.de/en/payments/next-generation-payments/whitepaper-the-future-of-payments/

G7 Working Group on Stablecoins (2019) Investigating the Impact of Global Stablecoins. Committee on Payments and Market Infrastructures. Bank for International Settlements. Available at: https://www.bis.org/cpmi/publ/d187.pdf

Gang X, Mount Union of Science and Technology (2019) Analysis of the Central Bank's Digital Currency DC/EP Dual Offline Payment Scenarios and Solutions. Available at: https://www.mpaypass.com.cn/news/201912/06094420.html

Garratt RJ, Van Oordt MR (2019) Privacy as a Public Good: A Cash for Electronic Cash. Bank of Canada Staff Working Paper, 24. Available at: https://www.bankofcanada.ca/wp-content/uploads/2019/07/swp2019-24.pdf

Geva B (2018) Banking in the Digital Age – Who is Afraid of Payment Disintermediation? EBI Working Paper Series 23. Available at: https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1329&context=all_papers.

Gorjón S (2021) The Role of Cryptoassets as Legal Tender: The Example of El Salvador. Analytical Articles, Nº 4/2021. Banco de España. Available at: https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/InformesBoletinesRevistas/ArticulosAnaliticos/21/T4/Files/be2104-art35e.pdf

Group of 30 (2020) Digital Currencies and Stablecoins: Risks, opportunities, and challenges ahead. Available at: https://group30.org/images/uploads/publications/G30_Digital_Currencies.pdf

HM Treasury, Financial Conduct Authority, Bank of England (2018) Cryptoassets Taskforce: Final Report. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

Information & Privacy Commissioner of Ontario (2013) Privacy by Design. Available at: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

Information Commissioner's Office (2021) Introduction to Anonymisation. May. Available at: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

Khiaonarong T, Humphrey D (2019) Cash Use Across Countries and the Demand for CBDC. International Monetary Fund. Available at: https://www.imf.org/en/Publications/WP/Issues/2019/03/01/Cash-Use-Across-Countries-and-the-Demand-for-Central-Bank-Digital-Currency-46617

Kriwoluzky A, Kim CH (2019) Public or Private? The Future of Money. European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_IDA(2019)642356

Maimeri F, Mancini M (2019) Le Nuove Frontiere Dei Servizi Bancari e Di Pagamento Fra PSD2, Criptovalute e Rivoluzione Digitale. Banca d'Italia. Available at: https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2019-0087/index.html

Makarov I, Schoar A (2022) Cryptocurrencies and Decentralized Finance. W. Paper No 1061. Bank for International Settlements. Available at: https://www.bis.org/publ/work1061.htm

Monti M (2010) A New Strategy for the Single Market - At the Service of Europe's Economy and Society. Available at: http://ec.europa.eu/bepa/pdf/monti_report_final_10_05_2010_en.pdf

Oliver Wayman Forum (2022) Retail Central Bank Digital Currency: From Vision to Design. A framework to align policy objectives and technology design choices. Available at: https://www.oliverwymanforum.com/content/dam/oliver-wyman/ow-forum/future-of-money/Retail-Central-Bank-Digital-Currency-From-Vision-to-Design.pdf

Paesano F (2019) Working Paper 28 Regulating Cryptocurrencies: Challenges & Considerations. Basel Institute on Governance. Available at: https://baselgovernance.org/sites/default/files/2019-06/190628%20Working%20Paper%20Cryptocurrency%20Regulations.pdf

PPI AG (2020) Internet of Payments. PPI. Available at: https://www.ppi.de/en/payments/next-generation-payments/study-internet-of-payments-iop/

Project Atom (2021) Exploring a Wholesale CBDC for Syndicated Lending. Available at: https://www.rba.gov.au/payments-and-infrastructure/central-bank-digital-currency/pdf/project-atom-report_2021-12.pdf

Sandner P, Gross J, Grale L, Schulden P (2020) The Digital Programmable Euro, Libra and CBDC: Implications for European Banks. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3663142

Schrepel T (2021) Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach. European Commission. Available at: https://op.europa.eu/en/publication-detail/-/publication/224da7da-1c18-11ec-b4fe-01aa75ed71a1/language-en

Soderberg G, Bechara M, Bossu W et al (2022) Behind the Scenes of Central Bank Digital Currency. Emerging Trends, Insights, and Policy Lessons. IMF FinTech Notes 22/4. International

Monetary Fund. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174

Sveriges Riksbank (2021) E-krona pilot Phase 1. Riksbank. Available at: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/ekrona-pilot-phase-1.pdf

Tapscott D (2020) Token Taxonomy: The Need for Open-Source Standards Around Digital Assets. Blockchain Research Institute. Available at: https://www.blockchainresearchinstitute.org/wp-content/uploads/2020/02/Tapscott_Token-Economy_Blockchain-Research-Institute.pdf

Van Saberhagen N (2013) Cryptonote v 2.0 https://cryptonote.org/whitepaper.pdf

Whitehouse-Levine M, Kelleher L (2020) Self-Hosted Wallets and the Future of Free Societies. Blockchain Association. Available at: https://theblockchainassociation.org/wp-content/uploads/2020/11/Self-Hosted-Wallets-and-the-Future-of-Free-Societies.pdf

Working Group on E-CNY People's Bank of China (2021) Progress of Research Development of e-CNY in China. Available at: http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

World Economic Forum (2020a) Crypto, What Is It Good For? An Overview of Cryptocurrency Use Cases. Available at: https://www3.weforum.org/docs/WEF_Cryptocurrency_Uses_Cases_2020.pdf

World Economic Forum (2020b) Global Standards Mapping Initiative: An Overview of blockchain technical standards. White Paper available at: https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf

World Economic Forum (2021a) The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth. White Paper 1/8. In: Digital Currency Governance Consortium White Paper Series. Compendium Report. November 2021. Available at: https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf

World Economic Forum (2021b) Privacy and Confidentiality Options for Central Bank Digital Currency. White Paper 6/8. In: Digital Currency Governance Consortium White Paper Series. Compendium Report. November 2021. Available at: https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf

World Economic Forum (2021c) Defining Interoperability. White Paper 7/8. In: Digital Currency Governance Consortium White Paper Series. Compendium Report. November 2021. Available at: https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf

World Economic Forum (2021d) CBDC Technology Considerations. White Paper 8/8. In: Digital Currency Governance Consortium White Paper Series. Compendium Report. November 2021. Available at: https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf

World Economic Forum (2021e) Glossary. In: Digital Currency Governance Consortium White Paper Series. Compendium Report. November 2021. Available at: https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf

Zetzsche DA, Buckley RP, Arner DW, Barberis JN (2017) Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. European Banking Institute Working Paper Series, 11. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018534

5. Websites, Web Articles and Other Online Sources

Airfoil (2019) De-Anonymising Anonymous Crypto Services. Medium DDI

Antonopoulos A (2021) Keynote Address at the Harvard Law School Blockchain and FinTech Initiative Third Annual Conference: The Rise of Decentralized Finance

Auer R, Böhme R (2020) CBDC architectures, the financial system, and the central bank of the future. Available at: https://voxeu.org/article/cbdc-architectures-financial-system-and-central-bank-future.

BitKom (2020) Decentralized Finance (DeFi)—Anew Fintech Revolution? The Blockchain Trend explained

Bloomberg (2022) Silvergate Purchases Blockchain Payment Network Assets from Diem. January 31, 2022. Available at: https://www.bloomberg.com/press-releases/2022-01-31/silvergate-purchases-blockchain-payment-network-assets-from-diem.

C4 (2022) CryptoCurrency Security Standard (CCSS). Available at: https://cryptoconsortium.github.io/CCSS/

CBDC Tracker (2022) Today's Central Bank Digital Currencies Status. Last accessed: September 19, 2022. Available at: https://cbdctracker.org/timeline

Choo H (2019) Blockchain Application: DEX (Dec. Exchange). EE817/IS893: Blockchain and Cryptocurrency

Clement S (2021) Debunking the false narrative that cryptocurrencies are mainly used for illicit activities. Available at: https://btcpeers.com/debunking-the-false-narrative-that-cryptocurrencies-are-mainly-used-for-illicit-activity/

CoinMarketCap (2022) Homepage. Last accessed: October 18, 2022. Available at: https://coinmarketcap.com

Daniels A (2018) The rise of private permissionless blockchains – part 1. LTO Network, Medium. Available at: https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be

Dex & Cex (2021). Available at: https://ghoststaking.com/dex-cex/

Diem (2021) Diem Announces Partnership with Silvergate and Strategic Shift to the United States. May 12, 2021. Available at: https://www.diem.com/en-us/updates/diem-silvergate-partnership/

Diem (2022) Statement by Diem CEO Stuart Levey on the Sale of the Diem Group's Assets to Silvergate. January 31, 3022. Available at: https://www.diem.com/en-us/updates/stuart-levey-statement-diem-asset-sale/

Ethereum (2022) Non-fungible Token (NFT). Last accessed: October 29, 2022. Available at: https://ethereum.org/en/nft/

Euler T (2018) The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens. Available at: http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

European Central Bank (2022) For a few cryptos more: the Wild West of crypto finance. Speech by Fabio Panetta, Member of the Executive Board of the ECB, at Columbia University. 25 April 2022. Available at: https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220425~6436006db0.en.html

European Commission (2020d) Digital Finance Package. Available at: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

European Commission (2021f) Anti-money laundering and countering the financing of terrorism legislative package. Available at: https://ec.europa.eu/info/publications/210720-anti-money-laundering-counteringfinancing-terrorism_en

European Consumer Centre France (2022) Cash Payments Limitations. Available at: https://www.europe-consommateurs.eu/en/shopping-internet/cash-payment-limitations.html

Fruth, J (2018) Crypto-cleansing: strategies fight digital money laundering and sanctions evasion. Financial Regulatory Forum. Reuters. Available at: https://www.reuters.com/article/bc-finreg-aml-cryptocurrency-idUSKCN1FX29I

Genesereth M (2015) Computational Law: The Cop in the Backseat, CodeX Stanford Center Legal Informatics Available at: http://logic.stanford.edu/complaw/complaw.html

Genesereth M (2021) What is Computational Law? CodeX Stanford Center Legal Informatics, pp 1-5. Available at: https://law.stanford.edu/2021/03/10/what-is-computational-law/

International Token Standardisation Association (2022) Homepage. Last accessed: October 18, 2022. Available at: https://itsa.global

Introduction to ECash (1997) Available at: https://web.archive.org/web/19971009044558/http://digicash.com/publish/ecash_intro/ecash_intro.html

ITU-T (2022a) ITU-T in Brief. Available at: https://www.itu.int/en/ITU-T/about/Pages/default.aspx

ITU-T (2022b) ITU-T Groups. Available at: https://www.itu.int/en/ITU-T/groups/Pages/default.aspx

ITU-T (2022c) List of Focus Groups that have completed their activities. Available at: https://www.itu.int/en/ITU-T/focusgroups/Pages/concluded.aspx

Jagati S (2020) CBDCs With a Twist: The Public-Private Solutions Needed for Adoption. Available at: https://cointelegraph.com/news/cbdcs-with-a-twist-the-public-privatesolutions-needed-for-adoption

Kabré RJ (2022) Regulating cryptocurrencies in the Central African Republic: Has the cart been put before the horse? 21 July 2022. AfricLaw. Available at: https://africlaw.com/2022/07/21/regulating-cryptocurrencies-in-the-central-african-republic-has-the-cart-been-put-before-the-horse/

Lennon H (2021) The False Narrative of Bitcoin's Role in Illicit Activity. Available at: https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/

LTO Network (2019) Permissionless Private Blockchain. Available at: https://blog.ltonetwork.com/permissionless-private-blockchains-lto-network/

Marquardt P, Rosenberg G, Schisa W (2022) Digital assets and sanctions compliance: Tornado Cash and beyond. Available: https://www.iflr.com/article/2at0k2n6ovj2j92nms64g/digital-assets-and-sanctions-compliance-tornado-cash-and-beyond

Massari J, Catalini C (2021) DeFi, Disintermediation, and the Regulatory Path Ahead. The Regulatory Review. Available at: https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead/

Oxford Languages Dictionary (2022) Definition of "Teleological". Available at: https://www.google.com/search?q=teleological

Phan T (2021) Exploring Blockchain Forensics. Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/exploring-blockchain-forensics

Pocher N (2021a) Crypto-wallets and the new EU AML package: where are the battle lines drawn? CiTiP Blog. Available at: https://www.law.kuleuven.be/citip/blog/crypto-wallets-and-the-new-eu-aml-package/

Pocher N (2021b) Self-hosted wallets: the elephant in the crypto room? CiTiP Blog. Available at: https://www.law.kuleuven.be/citip/blog/self-hosted-wallets/

PYMNTS (2020) BIS To Open Four New Innovation Hubs Over Next Two Years: https://www.pymnts.com/news/banking/2020/bis-to-open-four-new-innovation-hubs-over-next-two-years/

Roy A (2021) El Salvador's Bitcoin Law: Full English Text. FREOPP. https://freopp.org/el-salvadors-bitcoin-law-full-proposed-english-text-9a2153ad1d19

Sandner P (2020) Unique Referencing and Identification in the Token Universe: Cross-Chain, Worldwide, and Fork-Resilient. Medium

Sands P, Campbell H, Keatinge T, Weisman B (2017) Limiting the use of cash for big purchases: Assessing the case for uniform cash thresholds. Available at: https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/80_limiting.cash.p

Satoshi (2019) Hash Time Locked Contracts (HTLCs) Explained. Medium Liquality

Sharma TK (2022) Types of Crypto Wallets Explained. Blockchain Council. Last accessed: October 29, 2022. Available at: https://www.blockchain-council.org/blockchain/types-of-crypto-wallets-explained/

Shilina S (2021) What is Mimblewimble, and how does it work? Cointelegraph. Available at: https://cointelegraph.com/news/what-is-mimblewimble-and-how-does-it-work

Skalex (2019) Making Sense of Crypto Token Types. Available at: https://www.skalex.io/crypto-token-types/

Sun Y, Yi YZ (2018a) Privacy in Cryptocurrencies: An Overview. Medium. Available at: https://medium.com/@yi.sun/privacy-in-cryptocurrencies-d4b268157f6c

Sun Y, Yi YZ (2018b) Privacy in Cryptocurrencies: Mixing-Based Approaches. Medium. Available at: https://medium.com/@yi.sun/privacy-in-cryptocurrencies-mixing-based-approaches-ce08d0040c88

The Arthur W. Page Center (2022) Ethical Orientations: Teleology. Available at: https://www.pagecentertraining.psu.edu/public-relations-ethics/core-ethical-principles/lesson-1-title/ethical-orientations-teleology/

The Cryptocurrency Consultant (2019a) What Is the Internet of Values? Medium The Startup

The Cryptocurrency Consultant (2019b) Crypto Forensics: How the Blockchain Convicts Criminals. Medium The Startup

UK Government (2022) Policy paper. Fact sheet: cryptoassets technical. Available at: https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-cryptoassets-technical

Wachsman (2019) Answering One of Blockchain's Biggest Questions: Anonymity or Pseudonymity? Medium

Wiesflecker L (2021) CEX vs. DEX – here are the differences. Coinmonks, Medium. Available at: https://medium.com/coinmonks/cex-vs-dex-here-are-the-differences-143fae4c33d4

Yazdanparast E (2021) CEX vs DEX: A Comprehensive Comparison of Features. Coinmonks, Medium. Available at: https://medium.com/coinmonks/cex-vs-dex-a-comprehensive-comparison-of-features-bb398d416d4f

Zhang T (2020) Deputy Managing Director Tao Zhang's Keynote Address on CBDC. IMF. Available at: https://www.imf.org/en/News/Articles/2020/03/19/sp031920-deputy-managing-director-tao-zhangs-keynote-address-on-central-bank-digital-currency

Zhang Y, Sun Y (2019) Privacy in Cryptocurrencies: Zero-Knowledge and Zk-SNARKs (1/2). Medium.

Zimmerman M (2017) Your DMCA Safe Harbor Questions Answered. Fenwick&West. Available at: https://assets.fenwick.com/legacy/FenwickDocuments/DMCA-QA.pdf