BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Quaderni dell'antiriciclaggio

Analisi e studi

Report on crypto-assets and the risk of money laundering

Michele Manna, Irene Cesarotto, Marco Militello and Andrea Silvestrini

luglio 2025

numero 31

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Quaderni dell'antiriciclaggio

Analisi e studi

Report on crypto-assets and the risk of money laundering

Michele Manna, Irene Cesarotto, Marco Militello and Andrea Silvestrini

n. 31 – luglio 2025

La collana Quaderni dell'antiriciclaggio *ha la finalità di presentare statistiche, studi e documentazione su aspetti rilevanti per i compiti istituzionali dell'Unità d'Informazione Finanziaria per l'Italia.*

La collana si articola in diversi filoni: il filone Statistiche *presenta, con periodicità semestrale, statistiche sulle segnalazioni ricevute e dati sulle attività dell'Unità; il filone* Rassegna normativa *illustra i principali aggiornamenti della normativa e della giurisprudenza in materia AML/CFT; il filone* Analisi e studi *comprende contributi sulle tematiche e sui metodi in materia di contrasto al riciclaggio e al finanziamento del terrorismo. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.*

Unità di Informazione Finanziaria per l'Italia
Per la pubblicazione cartacea: autorizzazione del Tribunale di Roma n. 1942013 del 30 luglio 2013
Per la pubblicazione telematica: autorizzazione del Tribunale di Roma n. 1932013 del 30 luglio 2013

Direttore responsabile
Enzo Serata

Indirizzo
Largo Bastia, 35 – 00181 Roma – Italia

Telefono
+39 0647921

Sito internet
https://uif.bancaditalia.it/

ISSN 2283-3498 (stampa)
ISSN 2283-6977 (online)

Stampato nel mese di luglio 2025

Grafica e stampa a cura della Divisione Editoria e stampa della Banca d'Italia

REPORT ON CRYPTO-ASSETS AND THE RISK OF MONEY LAUNDERING

Michele Manna, Irene Cesarotto, Marco Militello and Andrea Silvestrini[1]

Abstract

The report examines the crypto-asset (CA) sector, analyzing its technological, regulatory, and market dimensions from the perspective of anti-money laundering and countering the financing of terrorism (AML/CFT). The interdisciplinary approach adopted is designed not only to address the complexity of the phenomenon but also to facilitate its understanding by a potentially broad and diversified audience. The CA sector is a highly heterogeneous domain. This trait poses a major challenge for authorities, who must acquire adequate expertise to effectively oversee their development and associated risks. In exploring the market dimension of CAs, the report presents a series of indicators that help to assess the level of evolution of this phenomenon, including the progressive convergence of CA markets with those of traditional financial assets. The report concludes by suggesting several possible courses of action, including: deepening the development of tools for analyzing CA transactions; systematically collecting data to support analyses and research; and fostering more direct exchanges of information between AML/CFT authorities and crypto-asset service providers (CASPs) operating in other EU Member States.

Sommario

Il rapporto esamina il comparto delle cripto-attività (CA), analizzandone le dimensioni tecnologica, normativa e di mercato, nella prospettiva di prevenzione del riciclaggio e del finanziamento del terrorismo (AML/CFT). L'interdisciplinarità dell'approccio adottato risponde non solo alla complessità del fenomeno, ma anche all'obiettivo di facilitarne la comprensione da parte di un pubblico potenzialmente ampio e diversificato. Al suo interno, il comparto delle CA è fortemente eterogeneo: ciò rappresenta una sfida rilevante per le Autorità, chiamate ad acquisire conoscenze adeguate a governarne lo sviluppo e i rischi associati. Nell'esplorare la dimensione del mercato delle CA, si presentano una serie di indicatori che consentono di valutare il livello di evoluzione del fenomeno, incluso il progressivo avvicinamento dei mercati delle CA a quelli di attività finanziarie tradizionali. Il rapporto conclude suggerendo alcune possibili linee di azione, tra le quali l'approfondimento di strumenti di analisi delle transazioni in CA, la raccolta sistematica di dati a sostegno di analisi, la ricerca di scambi informativi più diretti tra le Autorità di AML/CFT e i CASP operanti in altri Stati membri dell'Unione.

JEL Classification: G10, G23, K24, O33

Keywords: crypto-assets, anti-money laundering, financial markets, MICAR

---

[1] Financial Intelligence Unit for Italy – Bank of Italy. The views and opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the belonging Institution. The authors wish to thank all participants of an internal seminar held on 17 April 2025. The authors would also like to thank Mauro Bufano and Gerardo Palazzo for their valuable help in retrieving some financial data and news, as well as Mario Gara for his insightful comments and suggestions on Chapter 4. The paper is the outcome of a collective effort: Michele Manna authored chapters 1 to 5, while Marco Militello, Irene Cesarotto, and Andrea Silvestrini co-authored chapter 2, chapter 3 and chapter 4, respectively.

Contents

Chapter 1: Introduction, setting the framework

1.1 Preliminary remarks

This report has been written to deepen the knowledge of money laundering (ML) risks associated with innovative means of payment, particularly crypto-assets (CAs).[2]

Two straightforward and preliminary questions arise when addressing this topic. First, what are these means of payment, and in what sense are they innovative? Second, why should they be considered particularly vulnerable to ML risk? In this chapter, we aim to provide preliminary answers to both questions, deferring a deeper analysis to later chapters. In doing so, we outline key milestones in this field, chiefly the announcement of Bitcoin in 2008. We also examine how this chronology is closely connected to the sequence of actions of leading standard-setting bodies such as the Financial Action Task Force (FATF) and the European Union.

It has been argued that analyzing innovative means of payment – a broad category that includes CAs, among others – requires a deep understanding of both the technology and the regulatory environment (Biancotti, 2022). We add a third dimension: financial markets. Admittedly, this is easier said than done. Nonetheless, this work aims to assemble various pieces of an intricated puzzle. We acknowledge the challenge of balancing breadth with depth, but we aim to compensate for this by citing specialized literature throughout.

As a further introductory element, our approach is based on an uneven selection of topics across the three dimensions we have just outlined, giving priority to those topics most relevant from a ML perspective. To offer two examples, throughout this report we will devote ample attention to the MICA Regulation (EU) 2023/1114 (hereinafter, also the MICAR), but we will just briefly mention its provisions on the 'white paper', which does not offer major ML elements; remaining on the regulatory field, we will explore the content of the new AML Package and its elements of novelty in relation to CAs. Likewise, while an adequate introduction to how Bitcoin operates is warranted, we will only touch lightly on the consensus mechanism to validate the transactions in the blockchain, even though this topic tends to be prominent in more technically oriented papers.

1.2 Taxonomy and the mixed nature of crypto-assets

To properly assess the money laundering risks associated with CAs, it is first necessary to understand what these instruments are and how they relate to more traditional forms of money and payment. Indeed, the very classification of CAs – whether as money, financial instruments, or something else – remains fluid. We first clarify the monetary attributes of CAs, and then explore how they fit into the broader classification of economic instruments.

Broadly speaking, 'money' can be understood as any suitable medium for undertaking a purchase at a later stage, compared to the point in time when that medium was acquired in the first place.[3] Money exists in multiple forms. For the purposes of this research, a paramount classification is between 'token money' (also referred to as store of value) and 'account-based (claim) money', which differ critically in the type of verification required (CPMI, 2018; Kahn, 2016; Kahn and Roberds,

[2] This is the prevailing definition adopted in this report to refer to tokens which are transferred using distributed ledger technology, with crypto elements, in adherence to ECB (2019) and the Regulation (EU) no. 2023/1114. In a few contexts we switch to alternative definitions – e.g., virtual currencies, virtual assets and crypto-currencies – in accordance with the language adopted by the source being examined.

[3] Thus, in the broadest sense, 'money' can be defined as anything overcoming the limitations of barter, which is based on matching needs from the two counterparties of the exchange, at a given point of time.

2009).[4] In the token form, money has value *per se* either because it is a commodity (e.g., gold) or by government decree (in which case it is referred to as 'fiat currency'). The payee's main responsibility is to verify its integrity and authenticity, to ensure it is not a forgery. Conversely, he/she does not need to be overly concerned about the identity of the payer (or, at least, this is not a primary concern). Banknotes are the classical example of this type of money. In juxtaposition, in forms of 'account-based money' the two sides of the transaction transfer a claim (a credit) via an intermediary. Within this category, a typical example is a deposit with a bank, which can be transferred using a cheque or via a credit/debit card. Here, the payee is prompted to double check the identity of the payer and his accreditation with a qualified intermediary. We will see that these elements of the taxonomy are quite relevant for understanding the debate on the existing EU regulatory body on CAs.

Against this background, Adrian and Mancini-Griffoli (2021) put forward a classification of money which, starting from the above distinction between token and claim, follows further ramifications depending on whether the value of money is fixed or variable (relative to the standard of fiat money) and the type of technology involved in the transaction settlement, noticeably whether this calls for a centralized or decentralized set-up.[5] Based on this framework, Adrian and Mancini-Griffoli identify the following types of money:

- token money: (i) central bank money – cash and, in the future, central bank digital currencies (CBDC) – and (ii) crypto-currencies, of which the by-now household's example is Bitcoin;
- account-based money: (iii) B-money, namely money issued by banks (credit institutions in the European Union lingo) with some form of backing by the government; (iv) E-money, which differs from B-money insofar its redemption is not backstopped by government;[6] (v) I-money (the I stand for investment money).

This taxonomy provides a useful foundation for our research.

Firstly, it allows us to encompass under the expression 'innovative means of payment' the groups (ii) and (iv), which embed a technological advanced component for end-users.[7] By choice, CBDC is not included.[8] This brings us to note that innovation encompasses both changes of incremental nature compared to the more settled landscape in payment systems – E-money does probably better and certainly faster what B-money has already done for decades and centuries – as well as more radical transformations – arguably, the blockchain technology as a substitute of a trusted intermediary is a big leap forward.

Taking note of this demarcation line, and to keep the present study manageable, we have chosen to focus this report on group (ii), namely the crypto-currencies (to borrow the terminology of Adrian and Mancini-Griffoli).

---

[4] Another traditional classification is between 'inside money' and 'outside money'. The former is an asset representing, or backed by, any form of private credit that circulates as a medium of exchange; by design, inside money is in zero net supply within the private sector, since some agent's asset is some other agent's liability. Conversely, the latter is money that is either of a fiat nature (unbacked) or backed by some asset that is not in zero net supply within the private sector of the economy, e.g., a commodity (Lagos, 2006).

[5] As additional dimensions of the technological component, speed of the payment and the overlay being used increasingly matter in defining the interaction between payer and payee (Bech and Hancock, 2020).

[6] E-Money can be further subdivided depending on whether the settlement infrastructure is centralized (e.g., Alipay and M-Pesa) or decentralized (e.g., USD Coin and TrueUSD). It differs from CAs insofar as it is a digital mechanism denominated in, and used for, fiat currency (He et al., 2016); moreover, it usually does not require cryptography.

[7] Hence, under the banner of innovative means of payments we also include fast payments (e.g., Fednow) or payment methods, which combine the use of specific devices and Big-Tech as intermediaries (e.g., Applepay, Googlepay and PayPal).

[8] We felt that adding a general discussion on CBDC, including any potential ML misuse which might arise in the future, would have over-expanded an already ambitious agenda. A similar argument led us to exclude I-money, which anyway can, at best and despite the naming convention, be regarded as money only at the margin (Adrian and Mancini-Griffoli, 2021).

Secondly, the taxonomy we have just introduced should provide at least a first signal on why the pivotal 'know-your-customer' (KYC) rule, conceived for, and effectively implemented in respect to B-Money, cannot be expected to deliver automatically similar positive results with CAs, right because these latter set a distinct category. At the same time, also the parallelism of CAs with banknotes and a commodity such as gold should be pursued only up to a certain point, since relevant differences arise here as well.

To cut a long story short, CAs feature elements of both worlds, the token as well as the claim, and this calls for a bespoke regulatory framework. Let us consider the following example based on Mosna and Soana (2023) to illustrate the mixed nature of a transfer in the digital world. Our ownership of a (paper) book is proved by the sheer fact that we hold it, and no one is interfering with it. If we wish to transfer the book to a friend, we simply hand it over, with no need for the involvement of any third party in any form.[9] Hence, for the sake of this example, a book can be regarded as a form of token money. What if I wish to share a photo with the same friend through my account on a social media? True, that does not require the same degree of active involvement by the media compared to the role played by my bank when I pay using my credit card; however, there is no doubt that a third-party infrastructure is involved to finalize the photo sharing. So, in this metaphor, is this act more similar to transferring token money or account-based money, or is it a bit of both?

Garratt, Lee, Malone and Martin (2020) argue that a digital currency such as Bitcoin is both. Bitcoin belongs to the token camp, since its transfer depends on the correct execution of the entire transaction history, just as, in the case of a banknote, the hand-over is effective only if the banknote was genuinely issued by the central bank and no alterations have occurred at any stage (e.g., no tearing of the support). Equally, it fits the concept of an account-based money, as transferring a Bitcoin requires a proof of identification (it is not relevant at this stage that this is done via the private key and not by releasing our name/family name). Noticeably, the user is required to act in compliance with the procedure set by the platform on which the digital currency runs. *Mutatis mutandis*, this is not conceptually different from what we are required to do when we identify ourselves at a brick-and-mortar bank to withdraw cash.

Taking an even stronger stance, Milne (2024) argues that the distinction between token and account is of limited usefulness in describing the current technological opportunities in digital money. Cryptocurrencies (e.g., Bitcoin) would not qualify as token money;[10] at the same time, they represent at best a special case of account money, since their transfer involves only the payer and the payee.

Regardless of whether both the token and claim concepts apply, or neither applies, there are reasons to consider digital assets as having unique features, that cannot be easily framed within already existing categories. This points to the need for a bespoke response by the authorities.

1.3 A cursory history of crypto payments and official reports

As it is often the case in the history of innovations, the launch of Bitcoin in 2008 did not emerge from the void. A first wave of work on CAs dates to the early 1980s with proposals for untraceable payments. The Cypherpunk's [11] and the Crypto Anarchist Manifestos followed, providing an

[9] We could also ship the book by mail, but this is not always necessary.

[10] Milne qualifies this negative conclusion based on a historical usage of the term token. However, he accepts that 'Bitcoin and other cryptocurrencies are tokens in the new sense that of virtual assets transferred without the need for any financial intermediary' (Milne, 2024, p. 2203).

[11] Wikipedia (https://en.wikipedia.org/wiki/Cypherpunk) describes a cypherpunk as one who advocates the widespread use of strong cryptography and privacy-enhancing technologies as a means towards social and political change.

ideological basis, while new attempts to design decentralized digital currencies were enacted in the last 1990s.[12]

However, the true turning point dates to 2008, owing to two main factors: (i) Bitcoin combines existing technologies with new ingenious additions, which through cryptographic instruments largely prevents the risk of double spending; (ii) a good timing in its launch as a libertarian innovation. The financial crisis of 2007-2008, which began as a U.S. mortgage crisis and escalated into a global economic recession with widespread unemployment and public debt crises, created a fertile ground for such an idea. On October 31, 2008, a still-today unknown individual using the alias of Satoshi Nakamoto[13] published on internet a paper entitled 'Bitcoin: A peer-to-peer Electronic Cash System', while the first Bitcoin transaction occurred on January 12, 2009. The broad objective of the proposal, well attuned to the then prevailing public mood against further expansions of the role of and rule by authorities, is set out as 'an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party' (Nakamoto, 2008, p. 1). We cite this passage also because the ambition for full decentralization, central to Bitcoin's original intent, is increasingly being questioned today, with implications for future legislation as well as AML/CFT efforts.

Despite its eventual popularity, the launch of Bitcoin and its blockchain technology initially received limited attention from official circles. This can be tracked by counting the number of communications of various sorts on the topic issued on an annual basis by a total of ten international institutions and standard setting bodies (Figure 1[14]). To the best of our search, the first such document appeared in 2012,[15] with little additional activity until 2014, when as a first milestone the FATF published a report on key definitions and potential AML/CFT risks associated to virtual currencies. With all likelihood, the rising interest on the topic owed to widespread concerns generated by two major incidents associated which Bitcoin: in 2013, the arrest by the FBI of the founder of Silk's Road[16] and, in 2014, the closure of Mt. Gox, an exchange of CAs. After the FATF communication, followed in 2015 by the publication of a glossary, CAs entered the official debate. However, a wait-and-see attitude by the institutions still prevailed until 2017 (Carlisle, 2017).[17] Finally, everything changed in 2018 and 2019, driven by two key events: first, the near-collapse of CAs valuations[18] and, second, the announcement by Facebook on June 18, 2019, of the planned launch of its stablecoin, Libra. These events arguably triggered a substantial increase in official actions and reports.

---

[12] A massive literature explores the environment in which the launch of Bitcoin took place. Out of many possible choices, we refer the reader to Butler (2019); Taskinsoy (2019) and Yadav et al. (2022). Given the richness of the literature – the original paper by Nakamoto is credited with citations by some 36.000 published other papers – it is impossible to establish any meaningful ranking.

[13] The identity behind this alias, which could be a person or a group of persons or an organization, remains unknown to this day. On the frustration for this search, see e.g. a BBC article dated 3 November 2024 entitled 'Hunt for Bitcoin's elusive creator Satoshi Nakamoto hits another dead-end' (https://www.bbc.com/news/articles/c079zp2vy31o).

[14] The figure is an adaptation and expansion of work by Ferreira and Sandner (2021). Two elements of caution are warranted as regards our exercise: (i) the fact that an institution does not publish a document on a given topic does not rule out some degree of internal debate and study; (ii) the survey has been undertaken based on the authors' best effort, so the exact counting could be subject to errors.

[15] A report by the ECB entitled 'Virtual Currency Schemes'.

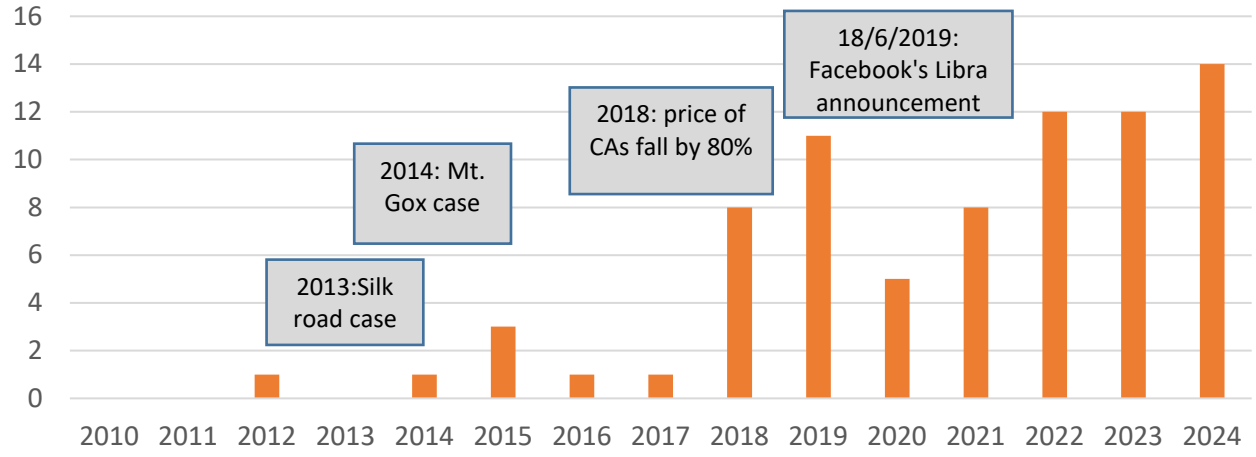
[16] Silk Road was an online market operating on the so-called dark net, in which transactions were conducted with Bitcoin. The website had gained increasing popularity for its listing of illegal product (besides legal ones).

[17] In Italy, already in May 2017, the Legislative Decree no. 90 defined what was then called 'valuta virtuale' (virtual asset) and set rules on entities offering services on such assets.

[18] The market capitalization of CAs fell from €650 billion in January 2018 to €96 billion in January 2019, recording a loss of 85% (Bullmann et al., 2019).

Figure 1

Number of reports by international / supranational institutions and standard setting bodies on crypto-assets (1)



(1) The original concept of this figure is in Ferreira and Sandner (2021). The figure shows the number of documents published per year by BIS, EBA, ECB, ESMA, FATF, FSB, IMF, IOSCO, OECD and the World Bank. The count includes reports, recommendations, guidelines, and similar documents published on the official website of each institution or standard setting body (SSB), where the primary topic is Bitcoin / CAs / DeFi. Documents on central banks digital currencies (CBDCs) are not counted, just as blogs, podcasts, press releases and speeches. A document is counted only if it was published at least three months after the last document on the same topic by the same institution or SSB. Joint documents are counted once; cross-references are not counted. Counting was carried out by the authors on a best-effort basis.

This chronology deserves particular attention, as arguably it has dictated the pace of the EU lawmaking in the field. While the first set of EU norms specifically dealing with virtual assets appeared only in 2018 – the Directive (EU) 2018/843, better known as the 5th Anti-Money Laundering Directive (AMLD5) – it took then only two years for the EU Commission to publish in 2020 a draft text of its MICAR (later the Regulation (EU) 2023/1114 on markets in crypto-assets). This initially delayed but subsequently rapid legislative activity has not been devoid of consequences in view of many commentators, as it will be discussed in Chapter 3.

1.4 Why crypto-assets are reckoned to be especially vulnerable to ML risks

Several factors are regarded as conduits for ML risk in CAs. For sure, one is the potential for anonymity[19] and, in a related way, the fact that transactions in this world are based on a peer-to-peer approach (with no face-to-face contacts, as an add on), without the strict need for intermediaries, neither regulated nor shadow ones. This is coupled by the global reach of digital platforms and the fact that undertaking a transaction in CAs requires only an internet connection and easily accessible software; therefore, standard national borders are very easily by-passed. From the viewpoint of a criminal organization, this pattern is further facilitated by the uneven application of domestic AML/CFT measures.

It is also worth highlighting, though often underrated, the multiplicity of elements that can be encountered when facing CAs. It is not just their sheer number, over 10,000 to the current counting, but also the fact that CAs emerge as a highly fragmented camp, something on which we will provide some statistics later. This means that labels such as stablecoins, native vs. non-native coins, fungible

[19] This aspect is openly acknowledged within the AML Package (see Section 3.3).

vs. non-fungible coins are helpful to set up a preliminary framework, but they just scratch the surface of a highly diversified world. One can easily grasp the difficulty for anyone, including officials of a law-enforcement agency, attempting to master the nitty-gritty of each CA.

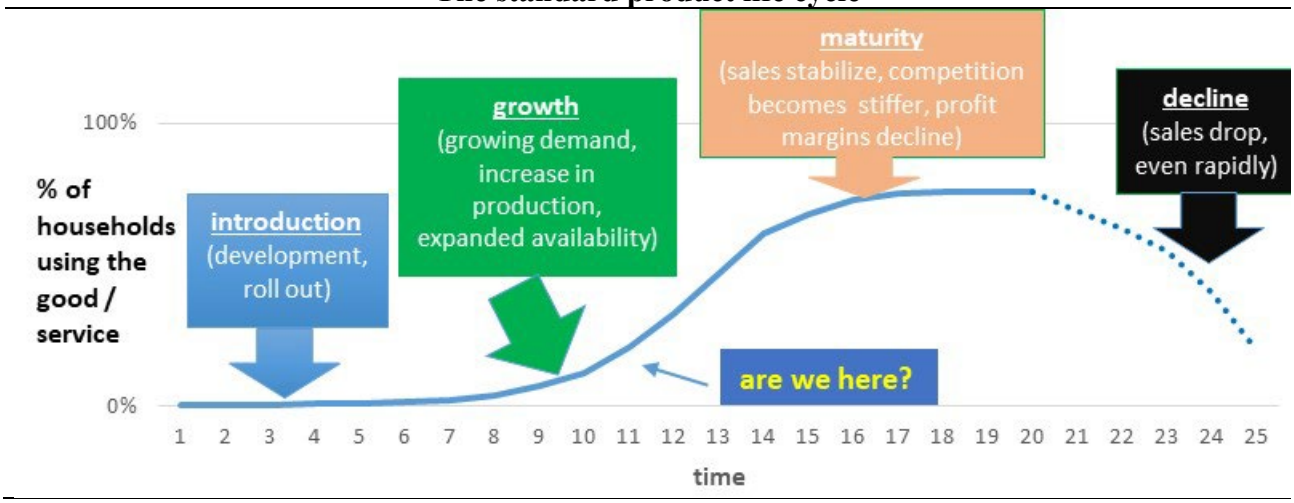
This list of issues would not be complete without acknowledging that there is truth in the observation that criminals are often early adopters of new technologies, outpacing both regulation and law enforcement responses (Carlisle, 2017; Fletcher, Larkin and Corbet, 2021; Schwarz et al. 2021; Gabriel et al., 2024).

1.5 Why a further report on crypto-assets?

There is certainly no shortage of material on CAs; if anything, one is spoiled for choice given the availability of a vast number of dedicated websites, books, as well as academic papers. It is hard to deny that this deluge also reflects the hype currently surrounding the topic. If that holds true, we owe to our readers at least a quick explanation on why we see merits in publishing yet another report on CAs. To clarify our reasoning, we take a step back and refer to studies on the product life cycle; after all, a CA is a 'product', no more no less than a washing-machine or a cell phone. This branch of studies typically identifies four distinct stages: introduction, growth, maturity, and decline (Figure 2; Kopp 2024).

Figure 2

The standard product life cycle



There are clear signs that the introduction phase has given way to the growth phase, characterized by rising demand, increased production (supply), and broader availability. One example is the growing attention from official institutions, as shown in Figure 1, which suggests that the topic has expanded beyond circles of specialized buffs. An even more telling indicator is the increasing diffusion of CAs across the public at large. According to Statista, in 2024 16% of US residents either owned or used CAs, while the average share in twelve euro-area countries was 13% (up from 7% in both cases in 2020; for Italy, the figures are 13% in 2024 and 6% in 2020).[20] These numbers are consistent with a trajectory towards a mass-market adoption. When you hear your neighbor talking up the new hot thing in town, you wish to own it as well. Marketing professionals are responding to

[20] The euro-area countries polled by Statista are (in alphabetical order): Austria, Belgium, Finland, France, Germany, Greece, Ireland, Italy, Lithuania, the Netherlands, Portugal, and Spain. We aggregated national shares using the current population as weights. These twelve countries account for 95% of euro-area current population.

this shift: references to Bitcoin and similar assets are becoming more common on main streets of our cities, along forms of advertisements typical of mass consumption goods.[21]

No matter what your view on CAs is, if the standard product life cycle applies once again, the odds are that the share of holders could surge in just a few years. Hence, if the 'CA product' is no longer confined to *niche* communities and is beginning to enter the mainstream, then a broad, multidisciplinary report along the lines we laid down in the opening Section 1.1 is warranted. What is more, in an environment where plenty of specific bits of information are available – from technical whitepapers to specialized newsletters – there is a clear need for structured, evidence-based, and accessible analysis. A multidisciplinary report grounded in empirical research and policy relevance can help filter signal from noise, especially for professionals and institutions that must make decisions in a fast-evolving landscape.

We cannot be over-ambitious, and a single report cannot cover every technical or legal twist associated with CAs. At the same time, reached the current stage of development, we wish to discuss matters beyond the level of a basic introduction of concepts such as blockchain and proof of work.[22] This is certainly the case when describing the legal framework, considering the progress reached by the EU body of norms relating in one way or another to CAs. It also applies to our empirical findings on the financial convergence of prices of leading CAs with traditional financial assets such as stock indices or gold.

Finally, in approaching the topic, we shall focus on aspects more relevant from an anti-money laundering perspective. After all, as CAs reach mass adoption, the risks of misuse also scale up, particularly in relation to money laundering and financial integrity. The growth of decentralized finance (DeFi), multi-chain exchanges, and privacy coins introduces new typologies of risk. This underscores further the need for a thematic report offering practical tools tailored to financial intermediaries and supervisory authorities.

[21] Many photos can be retrieved by googling 'images Bitcoin advertising hits main street' (or something like that).

[22] However, we reserve the first section of the next chapter to an overview of how Bitcoin works for newbies.

Chapter 2: The technology

2.1 Bitcoin for beginners[23]

Our fictional character Mark has heard a lot about Bitcoin and now feels ready to put 50€ into it, just to make some small purchases and to find the truth behind the rumors.

As nearly ubiquitous today, Mark's first step is to get an application enabling him to operate in this CA. He quickly learns that the term used for this application is 'bitcoin wallet', basically a user's interface to the Bitcoin system.[24] Googling the expression he runs into many software suppliers. Whatever his pick, he will need to make two preliminary choices: (i) on which device installing the software, noticeably whether on his smartphone (this is a 'mobile wallet') or on his pc, in which case he will access it through either a web browser add-in ('web wallet') or a standalone application ('desktop wallet'), and (ii) which degree of operating autonomy he wishes to enjoy, acting as a full-node client or as an aptly-named light-weight one.[25]

Let us suppose he opts for the smartphone (wallets can run on Apple iOS and Android operating systems) as a light-weight client. This will allow him to send and receive Bitcoins, but not to validate others' transactions; however, as a big plus, while a Bitcoin full-node requires at least 7 GB of free disk space,[26] 2 GB of RAM and a broadband internet connection of at least 50 kilobytes per second,[27] a light-weight one is much less demanding in terms of memory capacity since it can run on pretty ordinary devices (the smartphone we hold in our pocket should suffice).

Once the application opens on the screen, Mark will notice a string of numbers and letters and a QR code, which in two different versions provide for his Bitcoin address.[28] The next step for Mark is to receive his first Bitcoin, and there are three main options for doing so. Firstly, he can ask an acquaintance to send him a Bitcoin in exchange for a payment or, along a roughly similar line, he can search online for a seller,[29] or he can attend one of those social gatherings where people exchange bitcoins. Secondly, he can use a Bitcoin ATM, which is very much like a traditional ATM we know

---

[23] Valuable introduction to the working of Bitcoin can be found in many papers and a short list of references could include Badev and Chen (2014), Balaskas and Franqueira (2018), Möser (2022) and Vujičić, Jagodić and Ranđić (2018). However, our best tip is to afford the time to read Antonopoulos (2017), to which this chapter is indebted, while not being frightened by the 405 pages of this book, which is addressed to both the expert (who finds also programming codes) and the beginner (who can skip the more in-depth sections).

[24] In fact, that is not the only option, but we abstract from more technical elements, unless crucial to understanding the working of Bitcoin and the related distributed-ledger technology. Within the crypto world, the term wallet is not meant to refer to a store of digital values (so, a wallet is not the digital equivalent of an ordinary purse in which we store cash) but rather a tool to hold, directly or indirectly via a virtual-asset operator, the private keys required to operate the crypto addresses (see https://utimaco.com/service/knowledge-base/blockchain/what-blockchain-wallet).

[25] Ann, Mark's sister, who opened her first wallet already three years ago and is now well-versed in the world of CAs, could prefer a hardware wallet, basically a specialized hardware which can be operated via USB or via near-field-communication (NFC) on a mobile device.

[26] If the disk space is close to 7 GB, it is possible that not all functionalities operate properly.

[27] See Bitcoin.org, https://bitcoin.org/en/full-node#what-is-a-full-node. Other blockchains may require different (and heavier) requirements; for instance, a minimum of 16 GB of RAM is generally recommended to host a full Ethereum node.

[28] Often, one reads that the Bitcoin address is comparable to the number of our bank account (IBAN or ABA routing number for those living in the USA). That holds reasonably correct to the extent that one needs to know our address to send us Bitcoins, just as one needs to know our IBAN to execute a bank order. However, the parallelism breaks down insofar a bank code is assigned by a bank, and it remains the same over time (unless we close the account and we open another one probably at another bank) while, conversely, in the Bitcoin world we can, in fact we are encouraged to, adopt a different address for each transaction.

[29] Many sites offer such services, and a list could include, among other choices, Bisq, Robosats, AgoraDesk, Localbitcoins.

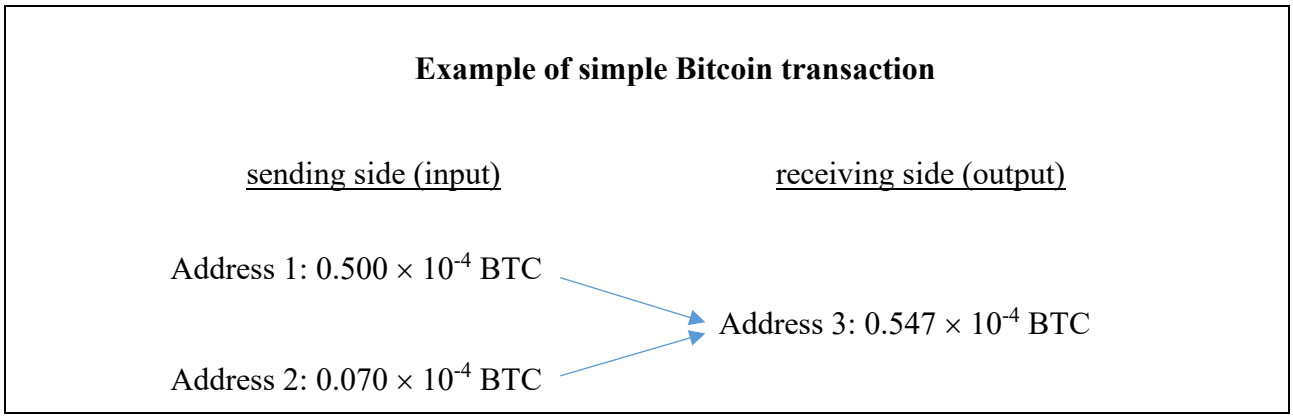
well except that rather than withdrawing banknotes the machine sends bitcoins to your wallet.[30] Thirdly, he can access a currency exchange linked to Bitcoin.

Ann, Mark's sister (we introduced her in fn. 25), is happy to help and agrees to send him 0.547×10^{-4} bitcoins (BTC), which is (approximately) equivalent to 50€.[31] As a crucial step in understanding the way Bitcoin works, this transfer is executed much alike if we were using physical cash. For instance, when we pay to our local shop, say, 17€, we cannot use a 17€ banknote because it does not exist. Instead, we take from our wallet a banknote worth more than this amount, say, a 20€ banknote, or a combination of smaller denominations that exceed the required amount, such as a 10€ banknote and two 5€ banknotes. In turn, we have these banknotes in our wallet because someone else has handed them over to us in earlier transactions, or because we have withdrawn them from an ATM.

For the sake of the example, we imagine that Ann puts together 0.500×10^{-4} and 0.070×10^{-4} BTC, which exceeds the 0.547×10^{-4} BTC she has promised to send to Mark, plus an implicit change of 0.023×10^{-4} BTC; this optional difference is there to remunerate the node (the so-called miner) which will employ its resources (electricity, ITC hardware and software) to validate the transaction.[32] To stress it more, Ann can spend the amount of 0.500×10^{-4} BTC she got from a previous transaction in full or not use it at all, but spending part of it is not an option. This is the same as with physical banknotes: we cannot tear one in two to create smaller denominations; we can only choose whether to spend the banknote or not.

In concept, the transaction we have described above will look something like this:

Example of simple Bitcoin transaction



In the following, we will adopt this notation:

[1a] $\{address^{n1}; 0.500\times10^{-4}\ BTC\}+\{address^{n2}; 0.070\times10^{-4}\ BTC\} \rightarrow \{address^{n3}; 0.547\times10^{-4}\ BTC\}$

Moreover, to simplify further, we shall write 'A' instead of 'address', so that [1a] becomes:

[1b] $\{A^{n1}; 0.500\times10^{-4}\ BTC\}+\{A^{n2}; 0.070\times10^{-4}\ BTC\} \rightarrow \{A^{n3}; 0.547\times10^{-4}\ BTC\}$

[30] See, e.g., https://coinatmradar.com/ to find a bitcoin ATM near you.

[31] Based on a price of 95,099.65$ per Bitcoin (https://coinmarketcap.com/) and an exchange rate of 1.04 $/€ (both quotes as of 23 December 2024).

[32] There is no obligation to set the transaction so that a change is implicit in the difference between input(s) and output(s). However, the larger the change, the higher the incentive for a miner to include the transaction into a block to be validated.

Once Ann has transmitted the transaction via her application, duly signed using her private key,[33] this will appear on Mark's mobile Bitcoin wallet. In a short amount of time, also the full-node clients – we mentioned them above as an alternative to the light-weight client option – will be made aware of this transmission.[34] As a second crucial step in the Bitcoin proceedings, this transaction will initially be under the status of 'unconfirmed', until someone else has verified that $\{A^{n1}\}$ and $\{A^{n2}\}$ have not already spent the respective amounts of 0.500×10^{-4} and 0.070×10^{-4} BTC.

As a rule, full-node clients constantly update a list of unconfirmed transactions (the memory pool, or mempool, or transaction pool) from which they will select a number of them, usually between 1,000 and 2,500, that end up in a 'candidate block'.[35] A key feature of a block is its serial number (the genesis starting block holds number 1), which is set as the number of the latest confirmed block plus one. If that number is, for instance, 876,019, the new candidate block's number will be 876,020.[36] Then, reached this stage, full nodes compete in what is effectively a mathematical game, repeating more and more extractions until they draw a suitable result with pre-defined characteristics.[37]

The full node that first achieves this is rewarded by the change, if any, implicit in the transactions of the block,[38] plus a small amount of newly generated bitcoins.[39]

On average, it takes around ten minutes to draw the winning number, and then the candidate block is confirmed. Information on this success will quickly be propagated through the network and a new lottery will start again, this time on candidate block 876,021. Once six blocks have been confirmed, up to number 876,026, the transactions included in block 876,020 are reckoned as being irrevocable since too huge a computational power would be required to recalculate the six blocks.

The underlying algorithm is periodically adjusted to make solving the mathematical problem increasingly difficult over time, thereby slowing the growth of the outstanding stocks of bitcoins. In doing so, what is often overlooked is the strong positive correlation between the difficulty of mining

---

[33] So long as a third party does not manage to get our private key, by hook or crook, there is no way to guess it through random generation number approaches. The size of bitcoin's private key space is approximately 10^{77}, a number which is approximately of the same order of magnitude as the estimated number of atoms in the visible universe, 10^{80}.

[34] Antonopolous (2017) reports that this happens in a second for most of the nodes. They may be informed directly, via Ann's application, or via other nodes, which in turn have been informed by other nodes by Ann's application through the peer-to-peer protocol.

[35] A node will add an unconfirmed transaction to its memory pool after it has completed some preliminary checks on the formal correctness of the transaction itself.

[36] The number of outstanding 876,019 blocks is verified as of 23 December 2024, 10:27:36 CET (https://bitinfocharts.com/bitcoin/).

[37] In a nutshell, this is the decentralized consensus mechanism applied in the Bitcoin blockchain, known as Proof of Work (PoW). This is an increasingly resource intensive procedure and alternative consensus mechanisms have been adopted in other blockchains. The most well-known among these alternatives is the Proof of Stake (PoS), adopted in the Ethereum blockchain. While in PoW all full-nodes are eligible to solve the mathematical riddle – which requires making this riddle very complex in order to obtain a fair winner – in the PoS a sort of pre-selection applies, as some full-nodes are selected randomly, where the chance to be extracted is a function of the coins put at stake (hence, the name) and thus what they hold. As fewer nodes are now eligible to compete, the riddle can be eased accordingly and the entire PoS mechanism turns out to be faster and much less energy consuming than PoW. On the other hand, it is more exposed to a potential risk of collusion by big holders of coins, a risk which is however reckoned to be less and less of a threat over time.

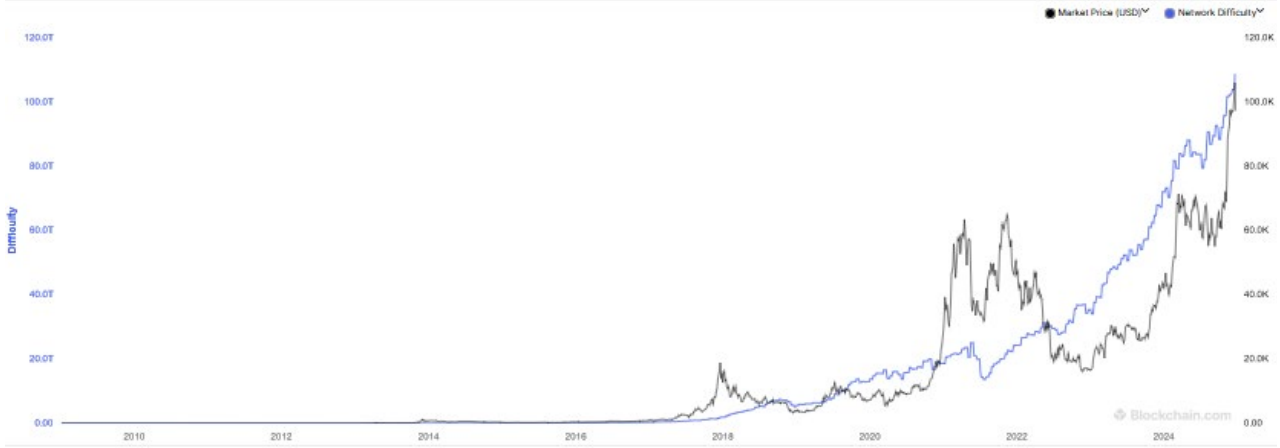
[38] Since full-node clients are free to select the unconfirmed transaction to insert in a candidate block, they have the incentive to prioritize those with largest change so that if eventually they win the mathematical game, they will earn the biggest prize. In turn, a sender knows that, with an adequate change, chances are that her/his transaction will soon be added to a candidate block and thus it will reach the confirmation status. That said, the sender is not obliged to leave a change, and a full-node client may choose to pick up also transactions with no change implicit in it.

[39] The first transaction of each block, so-called coinbase transaction, is designed for the purpose to generate the reward by a fixed number of bitcoins to the miner, namely the full node client who is first in solving the mathematical game.

and the value of Bitcoin in US dollar terms (Figure 3).[40] While correlation does not imply causality, an educated guess suggests that if the price of Bitcoin were to plunge for any reason, the incentive for full-node clients to validate a transaction would diminish, maybe up to the point of making uneconomical the effort which is nowadays pretty high in terms of computational power.[41] In turn, this slowdown in the generation of additional bitcoins could support the price of Bitcoin itself through a standard matching of demand and supply.

Figure 3

Network difficult of mining a block and market price of a bitcoin in USD



Source: https://www.blockchain.com/explorer/charts/difficulty.

We stressed above some common ground between physical cash and CAs. At the same time, there is an important twist. In the physical world, it will be some Mr X handing to some Mr Y the 10€ banknote and the two 5€ banknotes.[42] In the Bitcoin context, there is no rule forcing just a single Mr X on the input side and a single Mr Y on the output one. It follows that besides the structure laid down in [1], bitcoin transactions can be of the type 'one-to-many' or 'many-to-many' as in [2] and [3] below, respectively:

[2] $\{A^{n1}; X1\ BTC\} \rightarrow \{A^{n2}; X2\ BTC\}+\{A^{n3}; X3\ BTC\}$

[3] $\{A^{n4}; X4\ BTC\}+\{A^{n5}; X5\ BTC\} \rightarrow \{A^{n6}; X6\ BTC\}+\{A^{n7}; X7\ BTC\}$

Whatever the number of addresses on either side, it always applies that the total amount on the input side must be at least as large as that on the output side, i.e., $X1 + X2 \geq X3$ and $X4 + X5 \geq X6 + X7$. It is worth stressing that one or more of the addresses on the receiving side can belong to the sender, that may have just generated them for various purposes, including an elementary form of obfuscation.

[40] The commonly used term 'miner' to refer to full-node clients competing to validate candidate blocks seems to stem from this increasing difficulty, much like in a physical mine, in which marginal returns tend to diminish over time.

[41] This effort is reckoned to be way too big for an amateur, and nowadays even professional miners tend to pool their computational resources to enhance their chances of winning the mathematical game (clearly, this implies splicing the reward across the pool's members).

[42] Another difference is worth underlining. With physical cash, banknotes circulate in a limited set of round denominations defined by the central bank. This is not the case with Bitcoin, as Ann can use amounts received from previous transactions in which she was the recipient and has not yet spent (hence, one can speak of unspent transaction output, UTXO, where this amount can be an integer number of Bitcoins just as a number followed by up to 8 decimals).

Out of this cursory description of the functioning of the Bitcoin world, our main take-away for further steps in terms of AML are:

(i) the history of all transactions is visible in its entirety to full-node clients, as a requirement to undertake the validation step and prevent the double spending;
(ii) new public addresses can always be generated, and an address can exchange only unspent bitcoins received from a previous transaction;
(iii) blocks are chained, hence the term blockchain, since any block carries in its header reference to the previous block, up to the genesis block (the first block ever minted).

2.2 Tracking the transactions, the baseline scenario

The blockchain in Bitcoin is public and each fully-fledged node stores the entire sequence of blocks, from number 1 (the 'genesis') to the latest confirmed one, and thus each transaction. This means that managing any such node – which can easily be done by any individual or organization with professional IT equipment – is sufficient to read all transactions that refer to any address of choice. Moreover, since transactions are grouped into blocks and each block includes a reference to the previous one, this reading informs also on the chronology of transactions. As a further add-on, with the highest degree of confidence this wealth of information can be regarded as pristine, since there is no way to tamper it.[43,44]

With one important caveat: an address is a string of up to 34 digits and characters such as:[45]

14qViLJfdGaP4EeHnDyJbEGQysnCpwk3gd

This is very much like having access to a book written in an unknown language. One can follow the sequence of typographical symbols, without any clue of their underlying meaning. By itself, the crypto address reveals nothing about the identity of the person/organization behind it. Due to the mix of these elements of transparency and secrecy, Bitcoin is widely understood as a pseudo-anonymous coin (more frequently the contracted form 'pseudonymous' is used) rather than a fully anonymous one.

In fact, there are various ways to know more. The address may have undertaken a transaction with an exchange,[46] which *ought* to require the identification of the address' holder; then, a law enforcement agency could simply query the firm running the exchange (so long as this is located within a reachable jurisdiction). Or the address may have been the counterparty in a transaction with an ATM Bitcoin, which again may require some form of identification. A third option, no matter if it sounds naïve, arises when the holder of the Bitcoin address has spent coins on a retail purchase, such as a pizza, and has provided to the seller his/her physical address for delivery. Finally, more

[43] This level of security is ensured in Bitcoin through the Secure Hash Algorithm 256-bit (SHA-256), which returns a fixed-size string from input data of arbitrary length; other CAs adopt similar goal-minded algorithms. Two key features of the algorithm make it suitable for security purposes: firstly, it is asymmetric since it is easy to convert input data into the ash, but it is nearly impossible to reverse the process; secondly, even small alterations in the input data yield very different end results. So, you cannot work by analogy. Consider applying the SHA-256 on the book Les Misérables, by Victor Hugo, and again on the same book where just one sentence has been replaced. Although this accounts for a tiny fraction of the total of 1462 pages of the book, the two output strings will be quite different.

[44] More caution should be adopted with respect to most recent blocks (up to last six ones). Basically, this means that one can trust the reliability of every transaction on the blockchain older than an hour or so.

[45] See https://bitcoinwiki.org/wiki/bitcoin-address.

[46] In the crypto world, this is an entity (or sometimes a person) offering exchange services to users, who wish to buy or sell CAs, accepting payments in other CAs or also in fiat currencies; a similar function is performed by 'trading platforms', which connect users that aim to buy and sell CAs, while not undertaking directly the negotiation (a good overview of such functions is in Houben and Snyers, 2018). Basically, the distinction between exchanges and platforms mirrors the one between dealers and brokers in more standard financial markets.

information can be derived through the Internet connection, from the IP of the device executing the Bitcoin wallet; however, a user who takes care of his privacy might use proxies or VPNs[47] to disguise the real origin of the connection. One could add to this list of options the fact that bitcoin wallets are of heterogeneous quality, and some can be cracked, obtaining direct information on their customers.

As a simple line of privacy safeguard, any entity operating in Bitcoins can, in fact it is, encouraged to change addresses at every step. Consider the following transaction:

[4] $\{A^{n1}; X1\ BTC\} \rightarrow \{A^{n2}; X2\ BTC\}+\{A^{n3}; X3\ BTC\}+\{A^{n4}; X4\ BTC\}$

where A^{n4} can be an address relating to the same holder as A^{n1}, while A^{n2} and A^{n3} relate to different holders. That is, besides making payments to A^{n2} and A^{n3}, this holder is effectively transferring coins between his addresses A^{n1} and A^{n4}. For intuitive reasons, the denominations of spend and change outputs are used respectively. This highlights one further point: even if the payer has unspent Bitcoins matching the sum of X2 and X3, he may still prefer to use a larger amount than X2+X3, rightly to generate a change output.

That being noted, should the holder adopt regularly the precaution of inserting a change output (i.e., generating a new address and using it), tracing transactions becomes more laborious (not impossible), since each address would now occur only two times, in one transaction on the receiving side (on the right-hand side after the '→') and in a second and final transaction on the spending side (on the left-hand side before the '→'). Quite clearly, we do not know for sure whether any address between A^{n2}, A^{n3} and A^{n4} is a change output and if, there is any, which is which.[48]

Some information can be harnessed, nonetheless. Consider a simple variant of [4] such as:

[5] $\{A^{n1}; X1\ BTC\}+\{A^{n5}; X5\ BTC\} \rightarrow \{A^{n2}; X2\ BTC\}+\{A^{n3}; X3\ BTC\}+\{A^{n4}; X4\ BTC\}$

This is called a co-spend clustering since more than one address appears on the spending side (Harlev et al., 2018). Then, it is reasonable to assume that A^{n1} and A^{n5} relate to the same holder, although this conjecture does not necessarily hold true if the spending cluster is organized by a mixer, on which we will say more in the sequel.

We can extract further information by comparing the amounts, the X's. If, say, X1 > X2 + X3 and X5 > X4, then [5] could have been organized as well as

[6a] $\{A^{n1}; X1\ BTC\} \rightarrow \{A^{n2}; X2\ BTC\}+\{A^{n3}; X3\ BTC\}$

[6b] $\{A^{n5}; X5\ BTC\} \rightarrow \{A^{n4}; X4\ BTC\}$

In this case, an educated guess wants A^{n4} to be a change address; [6a] and [6b] are glued together into [5] to mask A^{n4} among the output addresses A^{n2} and A^{n3}. More broadly, as put it by Möser and Narayanan (2022), there should be no unnecessary elements. Should that happen, chances are that a change is involved and thus there is a trace worth pursuing.

At this very intuitive level, another example is provided by partially overlapping transactions of this type:

---

[47] A Virtual Private Network (VPN) establishes a connection between a computer and a remote server owned by the VPN provider. This masks the IP address of the computer itself and allows to sidestep website blocks and firewalls. See https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn.

[48] Nothing prevents the holder of A^{n1} to enact a transaction with more than one change address on the receiving side. It is equally possible that all receiving addresses are change ones.

[7a] $\{A^{n1}; X1\ BTC\}+\{A^{n4}; X5\ BTC\} \rightarrow \{A^{n2}; X2\ BTC\}+\{A^{n3}; X3\ BTC\}$

[7b] $\{A^{n1}; X1\ BTC\}+\{A^{n5}; X5\ BTC\} \rightarrow \{A^{n6}; X2\ BTC\}+\{A^{n7}; X3\ BTC\}$

Since A^{n1} appears both in [7a] and [7b], then the educated guess is that A^{n1}, A^{n4} and A^{n5} belong to the same holder.

These examples are intended only to convey a very preliminary idea of how addresses can be linked. In fact, a burgeoning and quickly expanding literature is focusing on employing more and more sophisticated techniques – variously based on cluster types of analysis, machine learning algorithms, graphs, and so on and so forth – to cluster addresses. Note, incidentally, that we are dealing with probabilistic results – there is a reason for the common use of the term 'address clustering heuristics', even if they are often highly sophisticated – which can yield false negative and false positive results.

Mastering this literature is a daunting task. A search over Google scholar for 'papers on de-anonymization in bitcoin' returned 2,450 results, of which 613 are dated in only the last two years. This large number can be seen as a double-edged sword. On the one hand, it speaks volumes about the effort scholars worldwide have invested in devising ingenious methods to trace Bitcoin addresses, which in turn confirms that there is scope to obtain meaningful results. On the other hand, if many new contributions become available – at the hectic rate of a new paper every 7 hours in January 2023 through December 2024, holidays included – one could surmise that no smoking gun is really in sight. While these papers could add to our knowledge of the process, they still do not provide for 'The answer' a crime-fighting authority would need. To be clear, this literature does achieve reasonably satisfactory results (Harlev et al., 2018, and Möser and Narayanan, 2022, are two good examples), but one cannot hope for quick and certain workarounds.

The sheer large number of papers we have reported offers thought for another reflection. Hard to deny that a thorough study of this literature would require the availability within a law enforcement agency of skilled analysts, in a number likely beyond real-life budgets. Probably the same applies to criminal organizations, which may also have their own analysts, but just not enough of them to counter the solutions that scientists in academia keep putting forward. To cut a long story short, the odds are that a chunk of this literature does not overstep the boundaries of the academia and neither law-enforcement agencies nor crime organizations can make a systematic use of it. Then, the innovations being used are those embedded in user-friendly software, of which Chainalysis is an example (see below Section 2.5).

2.3 Beyond Bitcoins: other leading crypto-assets and their blockchains[49]

Ether (ETH) is a good starting point to expand a little our understanding of the CA world beyond Bitcoin. It deserves a focus, being the second largest CA in terms of capitalization (see Table 2); in addition, it allows us to shed light on the difference between a coin and a blockchain. In effect, ETH is the native CA of the Ethereum blockchain-based platform.[50] This is a network of computers, through which one can run applications, the so-called smart contracts, for finance, gaming and as a base for decentralized autonomous organizations (DAOs).

[49] Information provided in this section is derived from the websites of Investopedia (https://www.investopedia.com/), Bernard Marr & Co. (https://bernardmarr.com/), Caleb & Brown (https://calebandbrown.com/blog/), as well as the 'analytics' sections on individual CAs of CoinMarketCap, e.g., https://coinmarketcap.com/currencies/ethereum/#Analytics for Ether (ETH) and Ethereum.

[50] To avoid terminological confusion, crypto-market providers refer to the coin being quoted using the acronym rather than its full name (say, ETH more than Ether or even Ethereum).

Since this structure implies costs, starting with electricity and the purchase of hardware, ETH is the 'currency' through which users pay for their access to the Ethereum network. In this sense, ETH is native to this blockchain, which however hosts also other 'tokens' such as, among others, USDT, USDC and BNB.

Tellingly, while the term Bitcoin refers to both the CA and its blockchain, in Ether/Ethereum two terms are used. In the former case, the blockchain can effectively be regarded as a close support to its own token, meant as an alternative to transfers of fiat currencies (so, one would argue, there is not much need to split terms). In the latter case, the blockchain is not ancillary to its native token, since it offers multiple functions – running several types of applications – while it is more the coin being instrumental to its working, in the sense explained above.

XRP, another well-known platform-type CA, is the native CA of the Ripple network, which is a system for payment settlement and currency exchanges for banks and payment system providers. Rather than bitcoin (here understood as the blockchain), a closer comparison to Ripple could be the Swift payment system, used by banks on a cross-border basis. Ripple helps highlighting another important point, being a type of distributed ledger technology (DLT) that does not employ blockchains. Often, the two terms are used interchangeably because Bitcoin, the most famous CA, is based on DLT running on a blockchain, but as the example of Ripple shows this is not necessarily the case.[51]

We mentioned smart contracts above. These are programmable, self-executing agreement designed to create, manage, or enforce the conditions of digital assets, also known as tokens.[52] In turn, tokens serve as digital representations of various asset types, such as artwork, cryptocurrency, and carbon credits on the blockchain. In Ethereum (today's leading blockchain), the standards shared by the developer's community enable the definition of common methods easing interoperability between different tokens and programs. However, while these methods are broadly uniform, the rights, goods, and services to which tokens provide access are the most diverse and essentially reflect those present in the traditional world.

A baseline taxonomy of tokens divides them into three categories:

- utility tokens, which provide access to the purchase of goods and services made available by the issuer, such as a voucher for the gym or the use of an IT application;
- securities tokens, representative of financial assets;
- stablecoins, which maintain a stable value and are therefore suitable for use as substitutes for more traditional payment instruments.

Along a different dimension, with respect to this taxonomy of fungible tokens, one finds the non-fungible ones, which are unique and typically represent collectible items (common in the gaming world), digital artworks, or the ownership/title of unique and real objects.

In the CA world, stablecoins play quite a relevant role and Tether (USDT is the acronym) is the most famous example of this category. The 'stable' emphasizes that the value of coin is pegged to some real-world assets, as it is not the case for BTC. Specifically, USDT is pegged 1:1 to the USD, allegedly being backed by an adequate pool of reserves.[53] This is why USDT, like other stablecoins

[51] It is true, however, that a blockchain is a way to implement a DLT.

[52] Smart contracts can be used to create also more complex applications than tokens: true decentralized platforms, at the heart of the so-called decentralized finance revolution, today allow for the exchange of virtual assets and the request for loans without the need for a traditional exchange. In these business models, the liquidity necessary for the provision of services is made available by blockchain users, upon payment of fees that are recognized by the algorithms written in the smart contracts that manage exchanges between users.

[53] To shed some light on the range of services an entity can provide in the crypto world, based on our research Tether is issued by Tether International Ltd. and Tether Ltd., two companies both fully owned by Tether Holdings Ltd., a British

(e.g., USDC), are also defined as 'centralized', in the sense that they are created by 'centralized' issuers, which in principle ought to be identifiable and should guarantee the custody of the assets to which they are pegged. It is also worth noting that USDT is not native to a blockchain, rather it is built on top of other blockchains such as Ethereum and Tron; this pattern is shared by other stablecoins.

In a variant class of stablecoins, the stability of the price can be achieved by adapting the supply of the coin to match the fluctuations in demand. The change in supply is then worked out through algorithms – hence, the denomination of 'algorithmic stablecoins' – and enacted also through smart contracts.

We complete this quick overview by mentioning Shiba Inu (SHIB). This is an Ethereum-based meme coin, that is a CA associated with a theme, in this case Shiba Inu, a Japanese breed of hunting dog. Often, meme coins are launched as a parody addressed to circles of meme-buffs, but they can reach out much wider audiences over time.

2.4 Privacy coins

The user highly concerned about his/her privacy can turn to, guess what, privacy coins, of which some of the most popular examples are Monero, ZCash and Dash.

Privacy coins feature in a native way advanced obfuscation tools such as:[54]

- Ring Confidentiality Transactions (RingCT): these are in fact two obfuscation approaches combining the 'ring' element of signature – in each transaction only one ring member is the truly spent input and the others are decoys (as of 2023, the mandatory ring size in Monero is 16, implying 15 decoys) so that an observer cannot link a signature to a specific payee (Houben and Snyers, 2018) – to the confidentiality element – as amounts are visible only to users involved in the transaction;[55]
- Stealth addresses: these are randomly generated, one-time addresses created for each transaction, which severe the link between the payer and the payee on the blockchain (Houben and Snyers, 2018; Möser, 2022);[56]
- Dandelion++: through this tool transactions are dispatched to trusted peers and only in turn to the wider network, raising the stake for someone monitoring specific, possibly weak, nodes.[57]

Nevertheless, Möser et al. (2018) proved that the real input could be deduced in nearly two-thirds of transaction inputs with one or more chaff coins (mixins)[58], the real one being often the 'newest' input.[59] More recent work by Hammad and Victor (2024) has shown that using sophisticated heuristics (which go under the names of '10 Block Decoy Bug', 'Differ-by-one', etc.) there is room to unveil a number of elements within Monero with high precision. It is also true that, following the cat and mouse metaphor, the Monero community has reacted and bugs have been fixed, closing most

---

Virgin Islands-registered entity, which is reputed as the ultimate owner of iFinex, which in turn owns and operates the crypto exchange BitFinex.

[54] A simple overview of privacy coins is in the dedicated section of the website of Skrill, a company offering cross-border payment services both in fiat currencies and CAs, accessible at https://www.skrill.com/en/crypto/the-skrill-crypto-academy/advanced/what-is-a-privacy-coin/.

[55] Key images are generated to allow for the consensus mechanism to work and to prevent double spending (Möser, 2022).

[56] This eliminates by design the possibility of re-using the address, which remains an option in Bitcoin.

[57] See https://www.trmlabs.com/post/the-rise-of-monero-traceability-challenges-and-research-review.

[58] In radar technology, a chaff involves the dispersal of thin strips of aluminum, metallized glass fiber, or plastic to blind or disrupt radar systems. More broadly, a chaff designates 'fake, dummy actions automatically generated on behalf of the user bearing no relation to the utility users expect to obtain from a service' (Balsa, 2019, p. 46).

[59] We use the past tense since this heuristic, based on occurrences of zero mixins, is regarded as largely ineffective today.

of these gaps according to a site such as TRM (see fn. 57 for full reference), which accordingly reckons Monero as still one of the most secure and private CAs.

What we have described so far offers just a glimpse of a much wider world, as we have hinted at some features of a few coins and mechanisms such as the so-called chain-hopping.[60] However, this should convey the main message: when it comes to clustering addresses on blockchains and possibly de-anonymizing them, it is more accurate to think in terms of varying degrees of anonymity rather than a strict binary distinction between pseudonymous and anonymous CAs. It is also true that we have touched base on just a few such coins – although Bitcoins, Ethereum and Monero stand out prominently in any ranking – while the crypto world boasts coins in very large numbers. This, together with the dynamism and relentless progress in privacy protocols, makes it highly unlikely that a law enforcement strategy could count on maintaining a permanent technological advantage.

2.5 Lines of attack and defense of privacy in non-privacy coins

The tech world offers a short-cut to this deluge of research, in the forms of tools to identify clusters of address in blockchains. Chainalysis, to mention one, is a US firm offering compliance and investigation software to analyze the blockchain public ledger.[61] The firm would count among its customers the US FBI, DEA and IRS Criminal Investigation, as well as the UK's National Crime Agency only to mention law enforcement agencies, as suggested by queries in Internet.

The market for blockchain analysis software is rapidly expanding. Just to mention two specialized sites, Slashdot examines 73 different suites, including Chainalysis, while GitHub lists 97 products, including blockchain explorers, blockchain databases and analyzers and a range of other tools.[62] The magnitude of these figures suggests that this is a market with a broad-based demand, probably from private individuals/companies whose aim is to seek protections from hacks, scams, and theft; reasonably, law enforcing agencies and Financial Intelligence Units (FIUs) alone could hardly sustain the commercial life of so many products. A subset of such products caters for intelligent analysis on AML/KYT requirements: examples include ChainAegis, MistTrack, Ancilia.[63] In general, these tools meet quite a diversified set of purposes, from inquiries on the wallet related to an address (https://www.walletexplorer.com/), on the amount of Bitcoin held on given addresses (https://bitref.com/), to the identification of sanctioned addresses (https://www.maltego.com/).

While a complete cross-examination of these tools is beyond the scope of the current analysis, it makes sense to gather an intuition of why there is scope and market for all such technical developments. Indeed, if Bitcoin and Ethereum insiders were to use the blockchain in its maiden way, with the only precaution of generating new addresses, the process of unveiling clusters of addresses would be relatively simple. Even tracing them back out of pseudo-anonymity is not beyond reach and already a decade ago Koshy, Koshy and McDaniel (2014) demonstrated how Bitcoin address-to-IP mappings can be derived with high confidence based on probability thresholds.

The fact is that, over time, more and more ingenious ways have been developed to obscure the transaction trail. As in the recourse to chaff in radar technology (see fn. 58), in a blockchain set-up, chaff transactions involve the launching of parallel transactions along the substantive one. Figure 4 (based on Figure 3.1 in Möser, 2022) provides a stylized example of chaff transactions: the rhomboid

---

[60] This is the process of conversion of one CA into another, exploiting software applications that enable transactions between various blockchains (so-called cross-chain bridges). Or possibly, the CA holding is transferred from one to another blockchain.

[61] See https://www.quora.com/How-does-Chainalysis-work.

[62] https://slashdot.org/software/blockchain-analysis/ and https://github.com/aaarghhh/awesome_osint_blockchain_analysis?tab=readme-ov-file#ada-blockchain-databases-and-analyzers respectively.

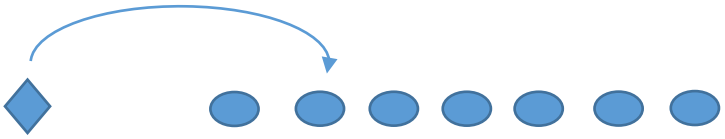
[63] Two scholarly papers discussing such tools are Balaskas and Franqueira (2018) and Wronka (2022).

on the left-hand side is the input address, while the circles on the right-hand side are possible output addresses of previous transactions, which multiply with chaff (fake) solutions in the second version.

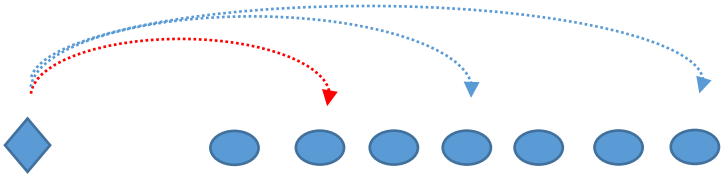
Figure 4

Stylized example of transactions with and without mixins

1) basic transaction (without mixins)



2) obscured transaction (with mixins)



In the interplay we are describing, each action is followed by a counter-reaction. For example, the use of chaff transactions helps but it is not yet a decisive precaution; Möser (2022) argues that many mixins (the fake output addresses) can be ruled out by deduction via different heuristics and in any case the real input is usually the 'newest' one.

Another approach to obscure transactions is through a 'mixer service', which receives coins from several payers and, after having pooled them, it dispatches them in a single transaction to another number of payees (notified by the payers). Mixers, aka tumblers, can be of the centralized or decentralized type. The former method centers on a single entity, which receives the various inputs and then executes the 'mixed' transaction (i.e., many-to-many as in [3] above). Clearly enough, this hub-and-spoke design sets almost unavoidably a privacy risk, since the hub stores the information from all inputs which it could disclose at some later stage (either by will or bowing to pressure by authorities or due to a breach). Conversely, the decentralized tumbler, as the name suggests, does not rely on a single center collecting all the information, since the process is dispersed via several addresses; for instance, anonymity can be further enhanced using CoinJoin-type protocols.[64] Hence, decentralized mixers are more secure than centralized ones, which, however, offer greater ease of use and faster transaction speeds.[65]

While the (shared send) mixer is a relatively old obfuscation tool (against the Bitcoin's time scale), this is still reckoned quite an effective instrument for increasing privacy (Larionov and Yanovich, 2023). Quite effective does not mean that it cannot be overcome via very smart de-

[64] We follow here the article "Bitcoin Mixers: what it is", https://medium.com/@AMLCrypto/bitcoin-mixers-what-it-is-62d718d1e611.

[65] Tumblers can be ranked according to other characteristics, and some may be more secure than others, even within the two main categories of centralization and decentralization. For example, the redistribution of pooled coins amongst the payees may embed delays and randomness in amounts to various degrees.

anonymizing tools, although there is always a degree of uncertainty. According to a highly rated wallet operator:

> *Tumblers are especially problematic to authorities due to the ability of the application to help launder money for terrorist organizations. As such, tumblers could help organizations launder money more easily because the transactions' source and recipient are often concealed.*
>
> *Although crypto tumblers offer a boost in anonymity, they do not guarantee complete anonymity. Factors such as transaction volume and external scrutiny can impact their effectiveness. It's possible for sophisticated tracking methods to identify patterns or links to the original transactions*. (PlasBit website[66])

While apparently pointing to opposite directions, both statements can be regarded as correct, without incoherence. Tumblers are hard to beat, but this is not a world in which the last word has been said.

To sum up, the balance between tools for obscuration and algorithms to unveil clusters of addresses is a dynamic one and the odds are that any assessment we draw today is going to change tomorrow, when newer and smarter crypto developments will become available. It is very much part and parcel of this balance a simple logical argument which defies the ambition of any commercially available software *à la* Chainalysis to harness a full victory. As a matter of fact, just as a law enforcement agency does, so a crime organization too could access, directly or indirectly, any such software, double checking whether it unveils a cluster of its blockchain addresses. If it does, the organization could sensibly (from its viewpoint) seek to add further layers of protection, switching to coins which better shelter its privacy, making a chain hopping move (see fn. 60), and so on and so forth. This purchase too entails a risk of identification plus naïve mistakes are made routinely (e.g., users do not rely on new addresses, bitcoins are spent for retail purchases revealing a physical address for delivery, in mixins the true output is the most recent unspent coin, etc.), so that neither side is ever sure to be 100% on the winning side.

We emphasized the reference to 'commercially available software'. That is to stress that a Financial Intelligence Unit or a law enforcement agency could develop a proprietary software, not accessible to outsiders and highly effective in identifying clusters of addresses in a blockchain, with the possible additional element of de-anonymizing them. That is not night dreaming, bearing in mind that many technological innovations have been conceived within States' defense sector for military purposes (also funding the Academia to undertake the related research), hence strictly proprietary technologies, as famously was the case for internet and GPS satellites for navigation.[67] The snag is that the degree of sophistication requires the availability of highly-skilled staff in a number which only a few law enforcement agencies could gather. Moreover, sooner or later the information will turn to public domain, possibly due to a leak, and the informational advantage will be lost.

---

[66] See https://plasbit.com/anonymous/what-is-a-crypto-tumbler.

[67] The website of NATO devotes an entire section to 'Military inventions that we use every day', https://www.nato.int/cps/fr/natohq/declassified_215371.htm?msg_pos=1.

Chapter III: The legal landscape

3.1 Comparing the definitions

To understand the extant European framework on CAs and AML/CFT, as laid down in the MICA Regulation[68] and the AML Package,[69] it could be appropriate to take a step back and start with the definitions adopted in recent years to refer in aggregate terms to Bitcoin and its brethren.[70] Indeed, even more than already usual in the legal world, in this context words do carry a meaning.[71]

Let us observe first that naming conventions in this field tend to follow a two-word rule and examples include digital currencies, virtual currency, crypto-assets, etc. The first term signals that we are dealing with something that exists only electronically, something which is not tangible (so, it is not cash-like). The second term is meant to convey the function performed. In what follows we compare the definitions put forward by FATF in 2014 and 2019[72] together with those laid down in the 5th AML Directive and in the MiCa Regulation, plus what put forward by the ECB in a report on CAs issued in 2019 (see Table 1).[73]

Advancing in the analysis, one could note that a stark dividing line in terms of wording content pits FATF (2014), FATF (2019) and AMLD5 (2018) on the one side and ECB (2019) and MICAR (2023) on the other side: while the former camp uses the word 'virtual', the latter camp opts for 'crypto'. The AML Package adopts the definitions set out in MICAR. However, as an important element of novelty, the AML Regulation introduces, in its Article 2 on definitions, the concept of 'anonymity-enhancing coins', being understood as those CAs that have built-in features designed to make crypto-asset transfer information anonymous, either systematically or optionally. We will discuss further how this concept could weigh in from an AML perspective.

This is by no means small change, as it implies that while the earlier definition aimed to support the principle of technological neutrality, the two most recent efforts have forsaken this approach in

---

68 Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets.

69 It includes: (i) Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLR); (ii) Directive (EU) 2024/1640 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD6); (iii) Regulation (EU) 2024/1620 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLAR); (iv) Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (Funds Transfer Regulation 2, FTR2).

70 This section draws on Soana (2024), chapter 3, part one.

71 Conversely, an institution adopting various naming conventions probably signals its intention to keep all options open. To mention two examples, on its website the Bank of England puts forward an educational text whose title is 'What are cryptoassets (cryptocurrencies)?' (https://www.bankofengland.co.uk/explainers/what-are-cryptocurrencies) while in two speeches delivered on 15 May 2018 and 16 October 2019 Governor Brainard, member of the US Federal Reserve Board, uses 'cryptocurrencies', 'digital currencies', 'digital money' (https://www.federalreserve.gov/newsevents/speech/brainard20180515a.htm and https://www.federalreserve.gov/newsevents/speech/brainard20191016a.htm).

72 Respectively, the documents entitled 'Virtual Currencies Key Definitions and Potential AML/CFT Risks', June 2014, and 'Guidance for a risk-based approach. Virtual assets and virtual asset services providers', June 2019. Since for the purposes of this Section chronology matters, one should note that already in October 2018 the FATF issued the new definition of 'virtual asset'. Hence, in Table 1, we will refer to this year, even if the glossary is today available in the 2019 report. As a further general remark, strictly speaking, the FATF is not a lawmaker, but its guidance has arguably quite a bearing on the choices adopted by the EU and other legislators.

73 Throughout this chapter we will write 'MICAR (2023)', that being the year when the Regulation was issued. However, it should be borne in mind that the draft text was circulated already in 2020, close to the ECB Report of the previous year. As a remark on the latter, that appeared in the Occasional Paper Series. While that carries the usual disclaimer, the fact that the author of the paper identifies itself as 'The ECB Crypto-Assets Task Force' suggests that the paper was meant to convey a quasi-official view of the ECB on what is a CA.

favor of an explicit reference to DLT and its core cryptographic features.[74] It is not without content the observation that since CAs are by design technology-specific, earlier efforts attempting to be technology-neutral could be regarded almost as an oxymoron (Mathis, 2023). To put it otherwise, a piece of law that pretends to be technology neutral is ill suited from the start to regulate Bitcoin, which is technology specific. More likely, one could put forward the interpretation that, from the very beginning, the claim to be neutral was in name only, a matter of paying lip service.

FATF (2014) describes 'virtual currency' in terms of the three standard functions of money: medium of exchange, unit of account and store of value. Namely, 'virtual currency' is a form of money, thence the reference to 'currency' in the first place. This approach is softened in FATF (2019) – following on the definition issued in 2018 – which adopts the word 'asset' but then it puts nevertheless at the forefront the fact that the virtual asset 'can be digitally traded or transferred, and can be used for payment or investment purposes'. That is, it adheres to the concept of medium of exchange. As to AMLD5 (2018), this can be regarded as a mix of the two solutions offered by FATF. It does revert to 'currenc(ies)' and 'means of exchange' as in FATF (2014), but as in FATF (2019) it does not go on to elaborate on the functions of money. All in all, these three sources share more elements than those dividing them and can effectively regarded as being under the same tent.

Conversely, such features of moneyness are not mentioned at all in the ECB (2019) and MICAR (2023) definitions.[75] It is also of note in this respect that the latter regulation joins the wording of 'digital representation of a value', ubiquitous across all definitions, with the additional clause 'or of a right'.

For the objectives of the later analysis, it is worth highlighting a specific element of ECB (2019), which states that a CA is not 'a financial claim on, or a liability of, any natural or legal person'.

[74] The reference included in the MICAR, noticeably its recital 9, to technology neutrality is regarded by many scholars as lip service, given other elements of the Regulation itself (Lehmann, 2024; Maume, 2023; Soana, 2024).

[75] It is regarded as relatively uncontroversial that, in this second stage, authorities were concerned about distancing their fiat currencies from Bitcoin/other CAs and Libra, the would-be coin by Facebook which was later ditched. Hence, the choice to drop the word 'currency/ies' in the definition and any reference to the function of money.

Table 1

Definitions put forward by FATF, ECB and EU lawmaker						
	FATF (2014)	**FATF (2019) - (based on definition issued in 2018)**	**AMLD5 (2018)**	**ECB (2019)**	**MICAR (2023)**	**AMLR (2024)**
definition	virtual currency	virtual asset	virtual currencies	crypto-asset	crypto-asset	crypto-asset
nature	digital representation of value	digital representation of value	digital representation of value	asset recorded in digital form	digital representation of a value or of a right	digital representation of a value or of a right
function	[it] can be digitally trade and function as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value,	[it] can be digitally traded, or transferred, and can be used for payment or investment purposes	[it is] accepted by natural or legal persons as a means of exchange and [it] can be transferred, stored and traded electronically		able to be transferred and stored electronically	able to be transferred and stored electronically
status	[it] does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction.	[they] do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations	[it] is not necessarily attached to a legally established currency and does not possess a legal status of currency or money	[it] is not and does not represent either a financial claim on, or a financial liability of, any natural or legal person, and which does not embody a proprietary right against an entity		
(lack of) issuer	not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency		not issued or guaranteed by a central bank or a public authority,			
other				the emergence of crypto-assets has been enabled by DLT	using DLT or similar technology;	using DLT or similar technology; introduces the concept of 'anonymity-enhancing coins'

3.2 The MICA Regulation (MICAR)

Published scholarly works are not short of plaudits on the MICAR. One reads that this Regulation is 'an unprecedented regulatory effort' (Ferreira and Sandner, 2021, p. 3) as it sets 'to reshape the legal framework of the crypto industry' (Lehmann, 2024, p. 699). Indeed, the MICAR stands out as 'the first comprehensive framework for DLT-based units (tokens or crypto-assets) in the world' (Maume, 2023, p. 243), an effort which puts the EU 'in a unique position, also on a geopolitical level, as it now constitutes the sole multi-state geographic area endowed with a homogeneous and uniform discipline (as directly applicable in the Member States) on markets in crypto-assets' (Annunziata, 2023, p. 1).

Then, the buts follow. On the milder side, one reads:

> *while MiCA is an ambitious legislative project, there is room for improvement* (Zetzsche, Annunziata, Arner and Buckley, 2020, p. 1)
>
> *MICAR is not future-proof. It will have to be adapted frequently to keep up with new technological developments* (Lehmann, 2024, p. 710).

More sternly, it is argued that:

> *the approach adopted by MiCAR does not excel in clarity, potentially leaving open to different national interpretation certain concepts* (Vianelli and Pantaleo, 2024, p. 10)
>
> *the overarching critique that can be moved is, hence, that the legislator has lacked the political will and creativity to overcome its previous approach and devise innovative solutions. The intermediary-centred strategy has simply been extended from traditional finance to crypto-assets* (Soana, 2024, p. 171).

Up to the beholder to judge whether the glass is half full or half empty.

To make sense of the seemingly opposite remarks we have quoted, one ought to bear in mind the following sequence of events: (a) 18 June 2019, the then-Facebook (Meta since 2021) announced a new crypto-currency called Libra, whose goals were broadly defined in terms of accessibility, stability and security;[76] (b) first half of 2020 was the possible time window when Libra would have been launched; (c) 24 September 2020, the EU Commission put forward the proposal for the new Regulation highlighting that 'the absence of applicable rules to services related to such assets leaves consumers and investors exposed to substantial risks'.[77] In addition, while the title of the MICAR refers to CAs in general, actually its *raison d'être* lies more specifically with the stablecoins, a category to which the legal text devotes two of its three definitions,[78] while the residual third one encompasses all other types of CAs. This approach can be regarded as the smoking gun, bearing in mind that Libra was intended to be a form of stablecoin. Based on these elements (and more could be added), it is widely believed that the MICAR represented the regulatory reaction by European authorities to the proposal of a US tech giant, which could potentially have become a massive game-changer for national currencies and the global monetary landscape.[79]

---

[76] See https://www.cnbc.com/2019/06/17/facebook-announces-libra-digital-currency-calibra-digital-wallet.html.

[77] See https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1.

[78] Although this is not the terminology used in the Regulation, except for a reference in Recital 41.

[79] In the hindsight 'It is a bit of an irony that while Libra and its potential successor Diem have been put on hold indefinitely, the MiCAR project came to fruition' (Maume, 2023, p. 248). To further appreciate the speed in terms of MICAR drafting, the launch of Bitcoin took nearly a decade to trigger a regulatory reaction by the authorities, with the 5th Anti-Money Laundering Directive of 2018. But Libra was perceived as a totally different ballgame, not because of any specific complexity or novelty in its technology but in the light of the number (to be counted in billions) of human beings holding world-wide a Facebook account. Hence, the potential audience of Libra was huge.

Given the time pressure to deliver, it is understandable that, besides other reasons, the EU lawmakers opted for the shorter and safer incremental approach, along which the MICAR was drafted taking close inspiration from other bits of EU financial services legislation, noticeably the MiFID II.

Nor the criticism of lack of courage in devising a newer legal approach to match a truly new challenge such as the CAs is entirely warranted. To mention the most relevant element of novelty actually enacted, the MICAR has forfeited the principle of technological neutrality, which had been a hallmark of earlier FATF documents as well as the AMLD5, to adopt a definition of CAs wired into a specific technology, the DLT (see fn. 74). Finally, the European legislator was not blind of many of the shortcomings we have mentioned, as it can be deducted through a close reading of the MICAR recitals.

Fair to add that alternative approaches do not necessarily meet full success either. In comparing the US and EU legal frameworks on CAs, Annunziata (2025) observes that the US system may be considered more flexible, being based heavily on primary judicial decisions. However, this implies a case-by-case regulation, which could involve the application to CAs of criteria developed in the past, sometimes the distant past, within a totally different financial environment. From this perspective, merits should be given to the more analytical EU approach, which the author describes as detailed and depictive legislation.[80]

Opting for the shorter and safer road has come to a cost though and a lively legal debate has developed since the first proposal of the new Regulation became public. Here, we will not attempt to examine the MICAR in all its aspects, something which would take dozens of pages and for which many good contributions are already available.[81] Rather, adopting a more focused AML perspective, we will try to identify those areas of the CA world which remain unregulated or imperfectly regulated, offering leeway for illicit activities.

Before turning to *medias res*, a preliminary remark is warranted. The Regulation deals with the CA market (thence covering the offering, negotiation, and exchange of assets in this market, together with the related provision of services), with a view to safeguarding its customers, *à la* MIFID. In this vein, the MICAR does not regulate CAs as such, nor say it dwells (at least directly) on smart contracts (see Section 2.3). That being stressed, the definitions laid down in the MICAR are imported one-to-one into the legal texts of the AML Package and as such have a strong bearing on the conduct of AML, while not being customized to that purpose. Hence, the MICAR is not per se a piece of AML legislation, but it stands as a hallmark of this legislation.

That said, the Regulation focuses on tokens issued by a legal entity and, as such, does not address the many instances in the crypto space in which the offering is decentralized, and cannot be attributed to any specific entity. The rationale for this choice is widely linked to the overarching approach adopted across the extant EU financial legislation – of which as just noted the MICAR is effectively a branch – which is built around the concepts of issuer and service provider; to the extent these entities

[80] A market source such as CoinMarketCap defines the EU regulatory approach to CAs as cautious, short of the friendlier one adopted by Singapore and Switzerland, but still better than the label of 'confusing' this source adopts to summarize the US set-up (https://coinmarketcap.com/academy/article/4dc9c34c-b600-4cd1-8ba4-5bcdbd3f1b6d).

[81] A selective reading list could include Annunziata (2023), Coelho and Poças (2024), Ferreira and Sandner (2021), Fliche, Uri and Vileyn (2023), Lehmann (2024), Maume (2023), Vianelli and Pantaleo (2024), Soana (2024), van der Linden and Shirazi (2023), Zetzsche, Annunziata, Arner and Buckley (2020) and Zetzsche, Buckley, Arner and van Ek (2023). Based on such list of sources, to which one needs to add Soana (2024) – a source which deals with a broader set of topics, beyond the Regulation – one could get heed of the list of thorny issues raised by the legal text. As a further remark, throughout this section we will not specify further such references, which across the board apply to virtually every subsequent paragraph, to avoid overloading the text. This editorial rule admits two exceptions: when we quote a passage, and when we report a view which, while not at odds with the thinking of other authors, we could find it mentioned just by one or a few of the aforementioned scholars.

can hardly be identified at all in segments of the crypto world, the lawmaker has taken a hands-off approach.

To mention the most prominent example of the limitations of this approach: a Regulation that, from its title, addresses CAs is generally understood not to apply to Bitcoin, certainly not to its issuance, even though Bitcoin holds a central place in the broader crypto environment. This speaks volumes about the need for a more mature legislative approach to the world of CAs.

In the scope of the MICAR, issues on its coverage ought to be addressed through at least two mechanisms. Firstly, the definition of CAs provided by the legislator is broad and should be read jointly with Recital 22, which extends the coverage of the Regulation, as far as the post-issuance phase is concerned, to crypto-asset service providers (CASPs) offering services in relation to CAs without an identifiable issuer. Second, it includes a closing rule which could be interpreted as filling potential regulatory gaps, but open for interpretation.[82]

There is no doubt that Non-Fungible Tokens (NFTs) are outside the scope of the Regulation. If something is unique and non-fungible,[83] it should be ill-suited to be the object of ordinary trading in a market; hence, the regulator's choice. It remains the fact that, with a relatively simple software, anyone can create an NFT collection and then issue it via a decentralized platform, possibly for illicit purposes.

As partly anticipated, there are segments of the crypto world which are within the purview of the Regulation but are weakened by classification uncertainties:

> *Although the Regulation positively defines ARTs and EMTs, as well as utility tokens, the Regulation then makes use of an open notion, identifying, from time to time, its scope of application not limited to those three categories, but extending it to an undefined universe of tokens 'different' from the first two: see, [..] emblematically, Title II of the Regulation, and, in this context, already Art. 4 that opens it, which applies to 'crypto-assets other than asset-referenced tokens or electronic money tokens'. [..] Now, this definitional approach itself is notoriously fraught with pitfalls.* (Annunziata, 2023, pages 24 and 25)

The mission of MICAR is to cover what is not already regulated by extant EU financial legislation. Vice versa, a CA that qualifies as a financial instrument will be regulated by the MIFID II and, as such, it stands out of the purview of MICAR. In principle, this should make little difference, since MICAR is broadly drafted along other EU financial legislation. However, this is true only in first approximation: for example, when issuing a financial instrument, the requirements on the prospectus as imposed by the eponymous Regulation are much heavier than those imposed by MICAR (which does not require the approval of the 'white paper' by the competent authority). A similar point can be raised with respect to the insider list (Lehmann, 2024). This opens a gap from CA to CA, depending on its nature of being a financial instrument or not.

This point has gained a sort of official status insofar it is part also of the Opinion delivered by the ECB in 2021 on MICAR:

> *With regard to the definition of 'crypto-asset' introduced by the proposed regulation, the ECB notes that the proposed regulation contains a wide, catch-all definition. However, in order to avoid diverging interpretations at national level on what may or may not constitute*

---

[82] MICAR, Art. 59(3): '[..] other undertakings that are not legal persons shall only provide crypto-asset services if their legal form ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if they are subject to equivalent prudential supervision appropriate to their legal form'. Some ambiguity remains regarding the extent of this extension, since as pointed out by Annunziata (2023, p. 29), the reading of the closing rule depends crucially on the interpretation of 'other undertakings', raising the question of whether a set of programming code could fall under this term.

[83] An NFT is effectively a data file, recorded on a blockchain, providing reference to a given asset, such as artworks, photos, a music piece, etc.

a crypto-asset under the proposed regulation, to help support the provision of crypto-asset services on a cross-border basis and to establish a truly harmonised set of rules for crypto assets, the scope of application of the proposed regulation should be further clarified. In particular, more clarity is needed with respect to the distinction between crypto-assets that may be characterised as financial instruments (falling under the scope of the MiFID II) and those which would fall under the scope of the proposed regulation. (ECB, 2021, section 1.4)

Furthermore, bearing in mind the design of a financial legislation within which there is contiguity between MIFID II and MICAR, problems start with MIFID II itself, since there is no commonly adopted application of the definition of 'financial instrument' across the different national transpositions. Heterogeneity can also be found on the judiciary/implementation side. For example, the Italian Corte di Cassazione offers rulings which accept Bitcoin as a financial product,[84] not stretching however to adopting the MIFID wording of 'instrument' (Annunziata, 2023), while the German Financial Supervisory Authority BaFin characterized decentralized CAs as units of account and thus, according to German law, as financial instruments (Barsan, 2017). Against this background, ESMA (2024b) issued a guideline on the conditions and criteria for the qualification of CAs as financial instruments, as mandated by MICAR, Art. 2(5).[85]

So far, we have spoken of a Regulation, not a Directive, hence a European legal construction that does not require transposition into national laws. This could be an important step forward to regulate at least on a European scale a phenomenon which by its very nature does not acknowledge national borders (probably, a global regulation would be even better). At the same time, this approach yields a relevant inconsistency, since it will coexist with the prevailing instrument adopted in other bits of EU financial law, namely the Directive. Hence, those CAs falling under the radar of MICAR will be regulated directly by the European law, those falling under the MIFID (because they are 'financial instrument') will be subject to national laws.

There is a negative side effect of the various elements of uncertainty which have been outlined:

If the scope of financial regulation is uncertain, supervisory authorities may be disincentivized to act, and this results in under-enforcement of existing financial regulation (Zetzsche, Buckley, Arner and van Ek, 2023, p. 81).

This couples with the warnings by ESMA (2024b, pages 12 and 27) to undertake 'a case-by-case analysis to determine whether a crypto-asset qualifies as a financial instrument' and 'the circumstances must be considered on a case-by-case basis in order to legally qualify crypto-assets'. Arguably, this analysis can be laborious given the strong heterogeneity across coins, an element on which we will provide statistical evidence in Chapter 4 (specifically, Figure 7 and related text).[86]

3.3 The AML Package

As mentioned above (see fn. 69), the AML Package is composed of four legal texts, of which Regulation 2023/1113 (TFR), Regulation 2024/1624 (AMLR) and Directive 2024/1640 (AMLD6) deserve specific attention for the purposes of this report.

The principle of traceability of CAs is at the center of an effective AML/CFT policy (e.g., TFR, Recital 16). To this end, it is set out in detail the information which are required to accompany the

[84] Sentences of Italian Corte di Cassazione of 10 November 2021, no. 44337, and 22 November 2022, no. 44378.

[85] Point 72 of the said Guideline acknowledges the difficulty of setting fixed rules against a rapidly evolving background and calls for 'a periodic reassessment of such hybrid tokens [i.e. tokens which due to their features could be regarded both as financial instruments and as complying with the definition of CA set out in the MICAR] to determine whether their classification needs to be updated'.

[86] Workstreams of legal aspects of CAs continue to develop at the time of writing and what presented in this and next section includes information available at what was the effective day of 'freezing' of this report, that is April 2025.

transfer of CAs by the CASP of the originator (TFR, Art. 14). In turn, the CASP of the beneficiary shall implement effective procedures to detect whether the requested information is included (TFR, Art. 16). As a rule, these norms apply to transfer worth at least 1,000€.

Definitions on the transfer of CAs, distributed ledger address and CA account (TFR, Art. 3) represent all important tools to enable the implementation of these rules.

Three elements of the 'information being transferred with CAs' requirement ought to be underlined. Firstly, reference is made to CASPs, in juxtapositions to transfers of CAs not involving an intermediary. This is because the TFR (Recital 22) explicitly states that person-to-person CA transfers fall outside of its purview. Secondly, crypto-ATMs are reckoned to be particularly exposed to ML/FT risks owing to the anonymity they can provide (TFR, Recitals 25). Accordingly, the legislator has extended the application of the TFR to transfers of CAs executed by means of crypto-ATMs (Art. 2). Thirdly, while the recourse to so-called self-hosted wallets – a wallet hosted and controlled by the user, rather than being hosted by a third-party service like a CASP[87] – is not directly subject to AML requirements, the involvement of the associated self-hosted address is subject to several requirements (e.g., TFR, Art. 14(5) and Art. 16(2)).

It would not make justice to the obligation imposed on CASPs to adopt an active stance when the required information is missing or incomplete, besides the duty to collect it, should this point be presented just as fourth item of the above list. Among others, the payment service provider of the payee (i) has to implement effective risk-based procedures (TFR, Art. 8); (ii) in case of incomplete or missing information, shall reject the transfer; or (iii) request the required information before or after crediting the payee's payment account or making the funds available to the payee; (iv) shall restrict or terminate its business with the corresponding provider of the payer in case of repeated infringements of the due information (TFR, Art. 8); (v) shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the Financial Intelligence Unit (TFR, Art. 9).

Moving from TFR to AMLR, we observe that it provides a comprehensive AML framework for CASPs, including them in the scope of 'financial institutions'. CASPs are required to implement all AML measures laid down in the Regulation, including costumer due diligence. It is not without meaning on the centrality of this concept, the frequency with which the expression is used within the AMLR.[88] The principle is laid down with no ambiguity as follows:

> *[..] Accurate identification and verification of data of prospective and existing customers are essential for understanding the risks of money laundering and terrorist financing associated with clients, whether they are natural or legal persons.* (AMLR, Recital 51)

It is worth noting that CASPs are subject to a specific regime: in fact, by way of derogation from the general rule (Art. 19. Par. 1 lett. b), CASPs shall apply customer due diligence measures when carrying out an occasional transaction that amounts to a value of at least EUR 1,000 and apply at least the identification and the verification of the customer's identity when carrying out an occasional transaction where the value is below EUR 1,000.

As an important element of novelty, the AML Package flags the concerns for the anonymity characterizing the crypto world. Recital 160 of the AMLR acknowledges this weak point, but also offers a possible solution:

---

[87] Self-hosted wallets (SHWs) can be of two forms: software SHWs are applications installed on users' computers or mobile devices; hardware SHWs are physical devices which do not need to be continuously connected to the internet and as a result they tend to be less exposed to online threats (https://www.21analytics.ch/what-is-a-self-hosted-wallet/). For an introduction on wallets, see Section 2.1.

[88] A search on the text of the AMLR of the string 'customer due diligence' returned 110 entries.

The anonymity of crypto-assets exposes them to risks of misuse for criminal purposes. Anonymous crypto-asset accounts, as well as other anonymising instruments, do not allow the traceability of crypto-asset transfers, and make it difficult to identify linked transactions that might raise suspicion or to apply an adequate level of customer due diligence. In order to ensure effective application of AML/CFT requirements to crypto-assets, it is necessary to prohibit the provision and the custody of anonymous crypto-asset accounts or accounts allowing for the anonymisation or the increased obfuscation of transactions by crypto-asset service providers, including through anonymity-enhancing coins. That prohibition does not apply to providers of hardware and software or providers of self-hosted wallets insofar as they do not possess access to or control over those crypto-asset wallets. (emphasis added)

Furthermore, the AMLR devotes its Chapter VIII to 'measures to mitigate risks from anonymous instruments'. Regarding the CAs, Art. 79 sets out a prohibition on credit institutions, financial institutions and CASPs to keep, among others, anonymous CA accounts, and more broadly, 'any account otherwise allowing for the anonymization of the customer account holder or the anonymization or increased obfuscation of transactions, including through anonymity-enhancing coins'.

The question arises of where to draw the line between identifiable and anonymous accounts and tools, a point that will probably need to be addressed in lower-level regulations. A narrow reading to Art. 79 of AMLR would interpret the ban as strictly applying to intermediaries, which could nevertheless be entitled to receive, store, and send coins tainted by obfuscation in earlier transactions (transactions not involving the intermediaries themselves) along the blockchain. A broader and possibly more effective interpretation could be upheld as well. Namely, that the principle laid down in this Article should be applied more sensibly by preventing intermediaries from receiving, storing, and sending coins that have been tainted at any stage along the blockchain. In the final Chapter V of this report, we will argue in favor of the latter interpretation – which admittedly would need to be carefully crafted, both in legal and technical terms – as an important step forward enabling authorities to regain ground in the currently unregulated realm of person-to-person transfers of CAs.[89]

Coherently with the extant EU financial legislation, the AML Package assumes the single passport framework.[90] More specifically, where CASPs carry out activities in a Member State's territory under the freedom to provide services (whether through agents or distributors, or through other types of infrastructure), Member States shall ensure that such activities are subject to supervision by their national competent authorities.[91]

---

[89] The limits on the use of physical cash (banknotes) that are applicable also in person-to-person transfers are a good reminder that difficulty in regulating these transfers in general does not translate necessarily into lack of any scope for regulation.

[90] The single passport is based on the principle of mutual recognition and harmonised prudential measures, and essentially means that a European financial institution that has been authorised by its domestic authority has the right to establish a branch or provide services in any other European Economic Area (EEA) Member State without the need to seek further authorisation or another licence (European Parliament, 2017).

[91] By way of derogation from this rule, supervision of agents, distributors, or other types of infrastructure, shall be carried out by the supervisor of the Member State where the head office of the obliged entity is located where: (a) the criteria set out in the RTS referred to in Article 41(2) are not met; and (b) the supervisor of the 'host' State notifies the supervisor of the 'home' State that, considering the limited infrastructure of the entity in its territory, supervision is to be carried out by this last. In addition, according to art. 41 of Directive 2024/1640, Member States may require CASPs operating establishments in their territory other than a subsidiary or a branch, or operating in their territory through agents or distributors, or through other types of infrastructure, under the freedom to provide services, to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the obliged entity, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.

Chapter IV: The market dimension and structure

4.1 Some stylized facts on the crypto market capitalization and concentration

In previous chapters we have mostly confined ourselves to a few well-known names in the crypto world such as Bitcoin, Ethereum and Monero. Now, it is time to tackle in a more systematic way a highly diversified market that at present counts overall more than 10,000 CAs.[92]

We start with some aggregate statistics. Figure 5 shows the turnover and capitalization (data in USD billion) of all CAs in 2013 through 2024. This is a good moment for a general disclaimer regarding this and subsequent statistics: no trend observed in historical data should be construed as a reliable indicator of future developments. The fact that CAs' capitalization increased 4.4 times between end-2020 and end-2024 should not be interpreted as an indication that the market will continue rising at a similar breakneck speed in coming years, or that it will rise at all. Such a disclaimer applies to most financial instruments, and a fortiori to a set of instruments that represent an absolute novelty by any standard.

That being underlined, despite starting from very low levels before 2018, CAs showed remarkable growth over the selected time window, though with significant volatility (notably during the so-called 'crypto winter' in 2022).

Figure 5

Market capitalization and turnover of crypto-assets

(*value at year end and yearly volumes; USD bn*)

Source: Coincodex (https://coincodex.com/trading-volume/ and https://coincodex.com/market-cap/)

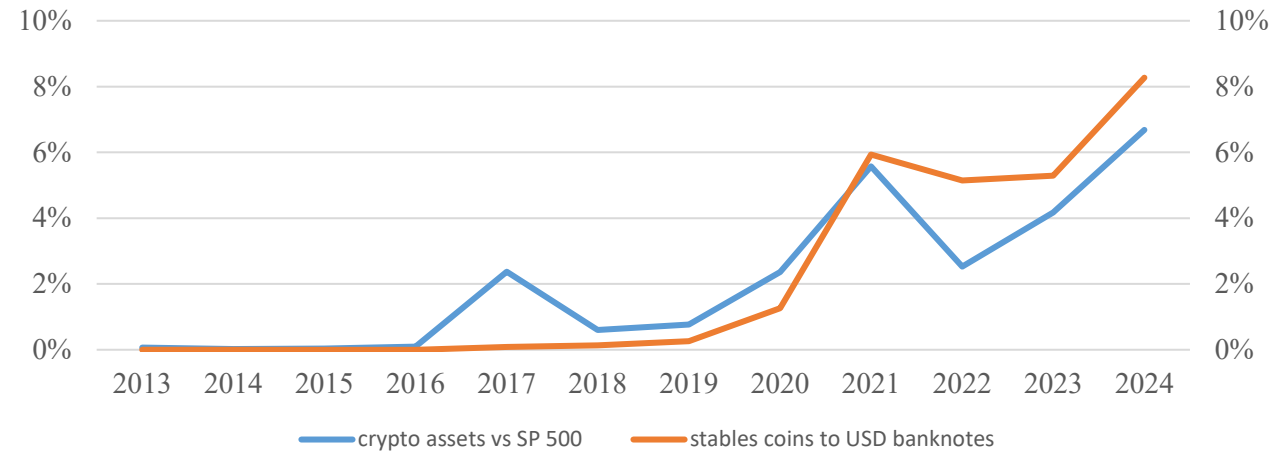
Although the market capitalization of CAs remains small at present compared to that of traditional financial markets, its significant growth means it can no longer be considered negligible. To put this into perspective, Figure 6 presents two comparative metrics based on year-end data: the blue line is the ratio of the total capitalization of CAs to that of the S&P500, a broad index of the US stock market; the red line shows the capitalization of the four most important stablecoins (USDT,

[92] CoinMarketCap (https://coinmarketcap.com/) lists 10,555 active coins as of January 8, 2025. Other sources report even larger numbers, up to the order of 25.000, without however listing them.

USDC, USDe and DAI[93]) – which are all pegged to the USD and function as digital equivalents of USD banknotes – relative to the total value of USD banknotes in circulation. As of the most recent data, both metrics stand at approximately 7-8%, highlighting the increasing relevance of CAs in the broader financial landscape.

Figure 6

Market capitalization of crypto-assets in % of ordinary financial assets
(*year-end data*)



Source. Authors' calculations on data from Coincodex, Bloomberg and US Federal Reserve.

Having examined overall market trends, we now turn to the composition of the crypto market, focusing on the largest assets by capitalization. Table 2 provides a snapshot of the top 30 CAs by market capitalization (data as of May 2, 2025), highlighting their respective turnover and classification. Even on an initial review, a few stylized facts stand out. Market capitalization is highly concentrated in a small number of coins. BTC alone has a capitalization of over $1.900 billion, corresponding to a market share of 67% among the top-30 CAs, and to 63% when measured against the estimated capitalization of all outstanding CAs.[94] When the seven largest CAs are combined, their share of total market capitalization rises to 88%. Caution is warranted when interpreting market turnover, for which we could gather long enough time series only for the seven largest coins. Nonetheless, a comparison over a narrower but more complete snapshot of data suggests that these coins are highly representative of the market also in terms of turnover,[95] in which the crucial role played by USDT emerges very clearly.[96] These findings are broadly consistent with the available literature (see, e.g., ESMA, 2024a).

[93] Throughout this chapter we shall broadly follow the convention of referring to coins using the acronyms provided by data providers, rather than their full names. This helps disentangling potential ambiguities between the names of blockchains and their associated CAs. Thus, we shall use BTC for bitcoin, ETH for ether, SOL for Solana, etc.

[94] Based on the comparison between the two ratios, one gathers that the capitalization of non-top-30 CAs accounts for close to 5% of the market.

[95] We obtained turnover data for all top-30 coins over the last 24 hours as of 16:00 CET on 2 May 2025, source CoinMarketCap. During that interval the turnover in the top-7 CAs accounted for 94% of the overall trading in the top-30 CAs.

[96] The different sources for the 2024 market turnover data (see note at the bottom of Table 2) could make the figure reported for USDC not fully comparable on methodological grounds to those of other CAs (https://visaonchainanalytics.com/transactions#adjusted-transaction-methodology).

Table 2

30 largest crypto-assets by market capitalization (1)

(USD billion)

Rank	Full name	Acronym	Stable coin	Market capitalization 2/5/2025	Turnover latest 2/5/2025	Turnover 2024
1	Bitcoin	BTC		1923.8	29.62	14,164
2	Ether	ETH		221.7	13.80	7,237
3	Tether	USDT	✓	148.9	60.74	20,570
4	XRP	XRP		129.8	2.19	1,144
5	BNB	BNB		84.3	1.47	520
6	Solana	SOL		77.9	3.22	1,493
7	USDC	USDC	✓	61.4	9.81	1,675
8	Dogecoin	DOGE		27.1	1.11	
9	Cardano	ADA		25.1	0.69	
10	TRON	TRX		23.3	0.45	
11	Sui	SUI		11.6	1.67	
12	Chainlink	LINK		9.6	0.33	
13	Avalanche	AVAX		8.9	0.34	
14	Stellar	XLM		8.6	0.15	
15	UNUS SED LEO	LEO		8.2	0.002	
16	Shiba Inu	SHIB		7.9	0.16	
17	Toncoin	TON		7.9	0.13	
18	Hedera	HBAR		7.9	0.17	
19	Bitcoin Cash	BCH		7.4	0.27	
20	Hyperliquid	HYPE		6.9	0.14	
21	Litecoin	LTC		6.7	0.48	
22	Polkadot	DOT		6.6	0.14	
23	Dai	DAI	✓	5.4	0.20	
24	Monero	XMR		5.3	0.12	
25	Bitget Token	BGB		5.2	0.06	
26	Ethena USDe	USDe	✓	4.7	0.10	
27	Pi	PI		4.2	0.06	
28	Pepe	PEPE		3.6	0.59	
29	Aptos	APT		3.4	0.09	
30	Uniswap	UNI		3.3	0.14	

Memorandum items. Market capitalization top-30 CAs: $2,857 bn; Market capitalization of all CAs: $3,020 bn. Total market turnover top-30 CAs as of 2/5/2025: 128.44 bn; total market turnover top-7 CAs as of 2/5/2025: 120.85 bn.

Source: CoinMarketCap for market capitalization and market turnover, latest; Statista for market turnover, 2024, except Visa for data on USDC.

The broad classifications we have used so far only scratches the surface of the crypto market's complexity. Indeed, the choice of labelling what qualifies as a stablecoin and what does not is just a preliminary step towards a more complete classification of coins and a more detailed categorization is essential to understand the diverse functions and potential substitutability of different assets.

CoinMarketCap, a well-known data source in the field, identifies 128 sectors in which active coins can be classified. Each coin is associated to one or more sectors, just as each sector can include one or more coins. We used this source to gain further insights into the structure of the market, tracking how closely related different coins position themselves in terms of categorization and potential substitutability.

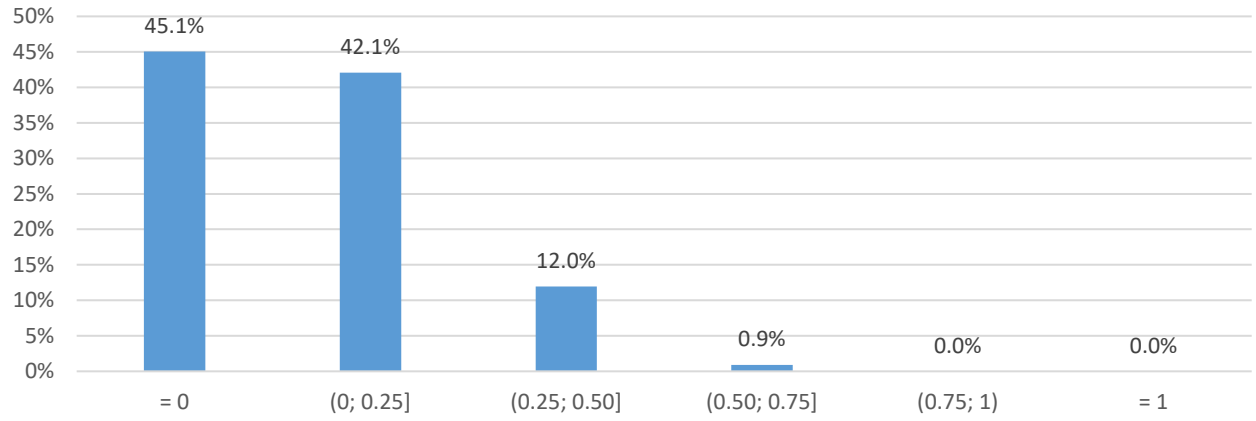
Our classification exercise is organized in two steps. Firstly, we identified the categories of each top-30 coin according to CoinMarketCap.[97] Secondly, we counted the pairwise degree of similarity in categorization as follows. Suppose that coin X belongs to categories A, B, C, D, and E while coin Y to categories B, C, F and G. Then, the degree of similarity is measured as the ratio of 2 (the number of categories, in this case B and C, to which both X and Y belong) to 6 (the total number of distinct categories for X and Y combined, i.e. A, B, C, D, E, and F). More formally, we have:

$$[8] \qquad S_{X.Y} = \frac{X \cap Y}{X \cup Y}$$

We worked out the measure of similarity in [8] for each of the 435 pairs that can be formed between the top-30 coins. The results are shown in Figure 7, as relative frequencies. Our findings show that for 45.1% of coins there is no overlap at all in terms of categories (that is, the result of [8] is zero). For 42.1% of pairs the overlap is strictly positive but does not exceed 0.25. An additional 12.0% of pairs have S values between 0.25 and 0.5. This leaves less than 1% of pairs with a matching score S higher than 0.5, with none achieving a full match (i.e., S = 1). This statistic suggests that each coin has its own distinctive elements. Even when two coins happen to resemble each other, they do it only to a limited extent. This pattern prevails amongst the top-30 coins and, as an educated guess, it can become even stronger should one expand the sample including more esoteric coins.[98]

Figure 7

Degree of overlapping in classification of top-30 crypto-assets by market capitalization (1)



(1) Authors' calculations based on equation [8] across top-30 coins. Categories are based on CoinMarketCap.

Regulatory and law enforcement agencies should take note of the high degree of differentiation among CAs. Without substantial resources, gaining in-depth knowledge of each coin is impractical. This raises serious doubts about the feasibility of placing the burden on authorities to determine what falls within the purview of the MICAR. A more effective approach could involve shifting the burden of proof to issuers, requiring them to demonstrate why specific assets should be exempt.

This complexity in categorization is also due to its focus on the technical elements of CAs. A more compact taxonomy could instead be derived along the standard concepts of supply and demand, an approach that, in the work of Vasselin (2024), leads to the identification of four sub-sectors: (i) platform crypto-currencies; (ii) means of payment crypto-currencies; (iii) tokens; (iv) stablecoins. To further dissect the market structure, we examine this classification approach in Box 1.

[97] Data as of 2 May 2025; https://coinmarketcap.com/cryptocurrency-category/.

[98] We identified top-30 coins in only 45 out of the 128 sectors listed by CoinMarketCap. This implies that two-thirds of sectors are populated by low-capitalization coins.

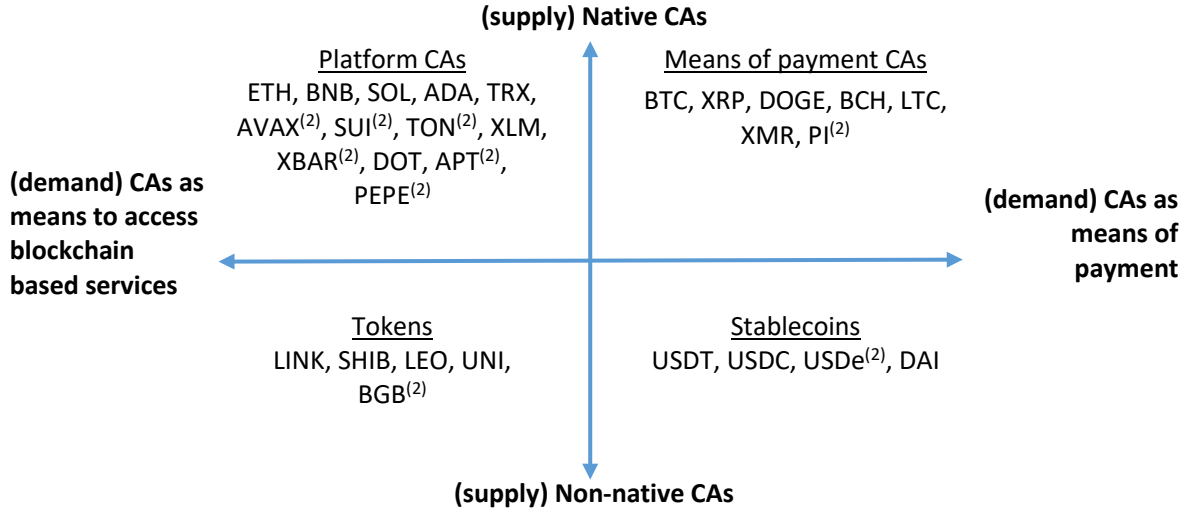
Box 1

A supply and demand-based classification of crypto assets

Vasselin (2024) presents a classification of CAs based on the standard economic concepts of supply and demand. On the supply side, Vasselin distinguishes between native and non-native CAs. Native CAs originate from and are an integral part of a specific blockchain, while non-native CAs do not originate from the blockchain they operate on and are not issued through block rewards. Turning to the demand side, Vasselin identifies CAs based on their primary function: either as a means of payment or as a means of accessing blockchain services. The concept of 'means of payment' has been extensively debated in the academic literature. A practical approach, in the view of the authors of this report, is to classify assets that provide direct services on their blockchain separately while grouping all others as means of payment, though some of them may serve additional functions. By combining these supply and demand dimensions, Vasselin identifies four key segments within the crypto market (see figure below):

i. Platform crypto-currencies – Native CAs that support smart contracts and decentralized applications (e.g., ETH, SOL);
ii. Means of payment crypto-currencies – Native CAs primarily used for transactions (e.g., BTC, XRP);
iii. Tokens – Non-native CAs designed to provide access to blockchain-based services (e.g., LINK, UNI);
iv. Stablecoins – Non-native CAs pegged to a stable asset, typically a fiat currency (e.g., USDT, USDC).

Classification of crypto-assets along the supply and demand dimensions (1)



(1) Based on figure 1 of Vasselin (2024). (2) Classification by the authors.

This classification is valuable not only because it frames CAs in more familiar and accessible economic terms, but also in light of the different micro-structure patterns prevailing in the four quadrants. Moving clockwise from top-right, the means of payment sub-sector is largely dominated by BTC, which alone accounts for 90% of the market capitalization in this segment. This structure has remained stable over time and does not appear to be under immediate competitive threat. In the stablecoins market, USDT leads with a share of 70% of the segment's capitalization, followed by USDC at 23%. While in principle the design of a new stablecoin is not utterly complex, this well-established duopoly has so far prevented tokens issued by major companies from making significant inroads, PayPal's (PYUSD) stablecoin being a notable example. Quite a different structure applies in the bottom-left quadrant of tokens. Not only is there no dominant player (LINK, which tops the list, stands at 27%), but this is a fluid segment. As pointed out by Vasselin, competitors may rise and then disappear within a few years, something which can be explained in terms of low entry barriers. Finally, the top-left quadrant of platform CAs again presents its own distinctive figures: (i) it is by far the most populated quadrant; (ii) its inner market shares are distributed in a granular way, even though ETH clearly holds the top spot with a share of 53% of the sector; and (iii) the structure of this sector has evolved dramatically since the launch of ETH in 2015.

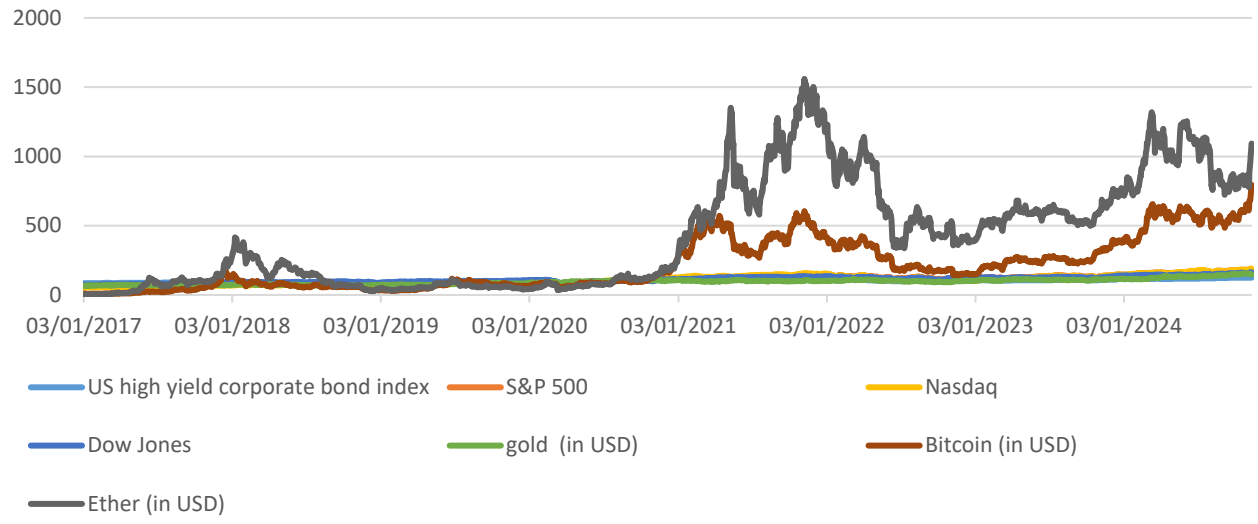
4.2 Market patterns

In this Section, we examine the price developments of key CAs in relation to traditional financial assets. For an overview, Figure 8 shows the historical price developments of Bitcoin and Ether compared to traditional financial assets. Particularly since early 2021, the two CAs appear to belong to a different league, in terms of both price levels and volatility. The main message conveyed by the figure is that the dynamics of these two CAs are so pronounced (in addition to being different from each other) that they make the price movements of traditional assets, used here as benchmarks, appear relatively flat. This holds true even though prices of traditional assets were not stagnant at all, having risen from two to three times (depending on the individual asset) between 2017 and 2024.

Figure 8

Price index of Bitcoin, Ethereum and selected financial assets (1)

(base 100 = average of daily data in 2020)

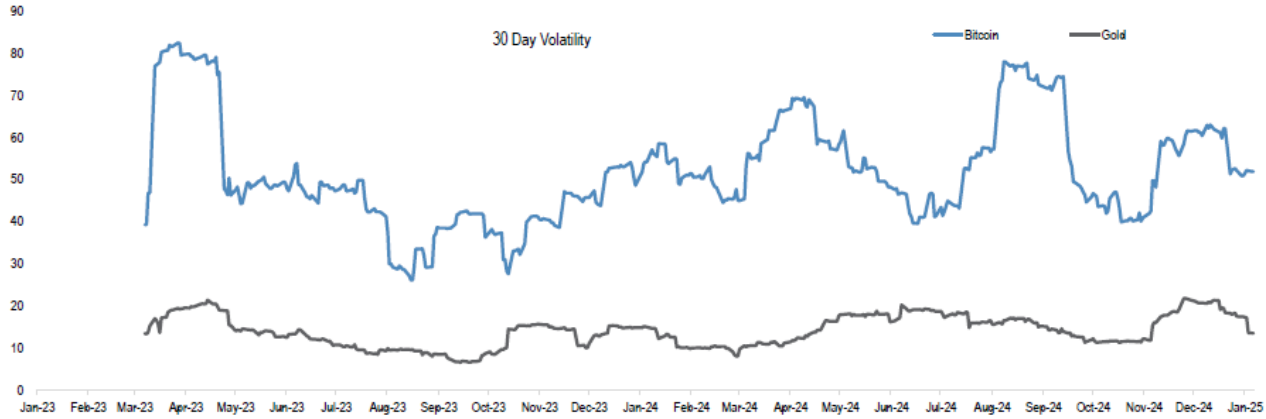


(1) Authors' calculations on Bloomberg and Cryptocoin data.

Additionally, the volatility of Bitcoin remains structurally higher than gold, and even the 'volatility-squared' (the volatility of volatility) is much larger (Figure 9).

Figure 9

30-day volatility in prices of Bitcoin and gold (1)



(1) Reprint from J.P. Morgan (2025). The original source of data is Bloomberg.

While these headlines pattern seem to emphasize a distance, in financial terms, between the two CAs and among them as a class and the five more traditional financial assets, more exploration of the data yields different insights. To this aim, we assembled a dataset covering prices of 10 CAs – BTC (Bitcoin); ETH (Ether); USDT (Tether); XRP; BNB; SOL (Solana); DOGE (Dogecoin); USDC; ADA (Cardano); TRX (Tron) – alongside five traditional, volatile assets – an index of high-yield corporate US bonds; the S&P 500; Nasdaq; Dow Jones; gold. Data are daily, covering the years 2022, 2023, and 2024. A more extensive dataset was compiled for BTC and ETH, among the CAs. As a first step, we worked out pairwise correlations across the CAs listed above, except for the two stablecoins (USDT and USDC; see more below); results are reported in Table 3.

Table 3

Correlations between prices of selected crypto-assets

(based on daily data. 2022-24)

	BTC	ETH	XRP	BNB	SOL	DOGE	ADA	TRX
BTC	--							
ETH	0.72	--						
XRP	0.65	0.53	--					
BNB	0.91	0.85	0.50	--				
SOL	0.96	0.90	0.55	0.93	--			
DOGE	0.81	0.70	0.82	0.75	0.79	--		
ADA	0.39	0.60	0.58	0.39	0.50	0.61	--	
TRX	0.89	0.63	0.73	0.74	0.79	0.75	0.22	--

Source: authors' calculation on CoinMarketCap data.

In total, we identified 12 bilateral correlations of 0.75 or higher, 13 correlations between 0.5 and 0.75, and only three correlations below 0.5, with a minimum of 0.22. The average across all 28 bilateral correlations is 0.68.[99] To avail a term of comparison, the average bilateral correlation among the five traditional financial assets shown in Figure 8 is 0.90. This suggests a notable degree of co-movement among CAs, though still lower than that observed for traditional assets, leaving room for further convergence on this metric.

Further technical evidence on the process of financial convergence is put forward in Box 2, in which we show that BTC and ETH are integrated of order one, just as most ordinary financial assets; we also illustrate that they are cointegrated. The issue of financial convergence is then examined using an appropriate econometric testing framework.

[99] These results could be biased upwards, since the time series being examined all follow a stochastic trend across the three years of the sample (Box 2). Hence, we replicated the analysis over rolling 60-day windows (a time span narrow enough to dampen the role of the three-year trend). The average of this second set of pairwise correlations is 0.58, close enough to the previously reported value of 0.68 to preserve the key message we highlighted. It is also close to 0.62, the average of bilateral correlations among the five traditional assets shown in Figure 8, also calculated over rolling 60-day windows.

Box 2

Order of integration, cointegration properties and financial convergence of leading crypto-assets

Further insights into how closely CA price dynamics resemble those of standard financial assets can be obtained by examining their order of integration.

To delve into the order of integration, it is important to recall first that a crucial concept in time-series analysis is stationarity.[a] Specifically, a variable y_t follows a (covariance) stationary process whenever its statistical properties – mean, variance, and autocovariance (or autocorrelation) structure – do not change over time. This makes the process more predictable and easier to model. A simple example of a stationary process is provided by the autoregressive model of order 1, denoted as AR(1):

$$[1] \quad y_t = \gamma + \varphi\, y_{t-1} + u_t$$

where u_t is a white noise innovation term with mean 0 and finite variance σ_u^2. Crucially, for a (covariance) stationary time series the absolute value of the autoregressive parameter φ must be strictly smaller than one (it lies within the unit circle, in the econometrics jargon). A time series for which this condition holds true is said to be integrated of order 0, for which the notation $\mathrm{I}(0)$ applies.

Many economic (e.g., GDP) and financial (e.g., stock prices) time series exhibit trends over time. These trends often make the series non-stationary in levels but (covariance) stationary in first differences, i.e., integrated of order 1, or $\mathrm{I}(1)$. In such cases, the data-generating process can be written as:

$$[2] \quad y_t = \gamma + y_{t-1} + u_t$$

where a preliminary transformation – such as first differencing – is required to achieve (covariance) stationarity. When this transformation needs to be repeated twice to make a series stationary, the original y_t series is integrated of order two, or I(2), and so on. Thus, in general terms, the order of integration refers to the number of differences required to achieve (covariance) stationarity. A range of statistical tests, known as unit root tests, are used to determine the level of integration of a time series.

That said by way of introduction, we carried out standard unit root tests to assess the integration order of the following nine variables: VIX [b], the US high-yield corporate bond index, the price of gold in USD, Nasdaq, Dow Jones, S&P 500, the USD/EUR exchange rate, and two CAs, BTC and ETH (both priced in USD). The dataset consists of daily observations from 2017 to 2024.

We applied the Augmented Dickey-Fuller (ADF) test to determine the order of integration, using a constant but no trend and incorporating lags selected via the Bayesian Information Criterion (BIC). A p-value below the conventional threshold of 0.05 leads to the rejection of the null hypothesis of a unit root. In tests on levels, the null hypothesis corresponds to I(1), while in tests on first differences, the null corresponds to I(2), with the alternative being I(1).

All variables are unambiguously I(1), with the exception of the VIX index that turns out to be I(0) – a result largely expected, being VIX an index of market volatility that, as such, should exhibit no trend over sufficiently long time horizons – and the USD/EUR exchange rate, a borderline case between I(0) and I(1).

In a subsequent step, we computed the first differences for all the time series (except VIX) and calculated the ADF test statistic on the transformed data. This time, the null hypothesis of non-stationarity was rejected for all series at the 99% confidence level, confirming that the original series are I(1) rather than I(2). To complement the ADF test, we also performed the standard Dickey-Fuller (DF) test and the Phillips-Perron unit root test. The results of both tests aligned with the ADF test, confirming that all examined financial variables (barring the VIX and the USD-EUR exchange rate), including CAs, exhibit persistent stochastic trends.

Tests on order of integration

(p-values of the Augmented Dickey Fuller test; daily data 2017-2024)

	levels	first differences		levels	first differences
VIX	< 0.0001 ***		S&P 500	1.000	0.0001 ***
US high yield corporate bond index	0.999	< 0.0001 ***	USD/EUR exchange rate	0.057	0.0001 ***
Gold (1)	0.999	0.0001 ***	BTC (1)	0.998	0.0001 ***
NASDAQ	1.000	< 0.0001 ***	ETH (1)	0.816	< 0.0001 ***
DOW JONES	0.999	0.0001 ***			

(1) price in US dollar. ***: significance at 1% level

After verifying that the price series of BTC and ETH are I(1), like standard financial assets, we assessed whether they are cointegrated, that is, whether they share a long-term equilibrium relationship.

As a first step, we estimated an unrestricted vector autoregressive (VAR) model using the log prices of ETH and BTC. We then performed a lag-length selection test using the BIC to determine the optimal number of lags based on information criteria. Next, we applied the Johansen (1988) methodology to test for cointegration, examining whether the non-stationary ETH and BTC time series share a common long-term equilibrium relationship. This procedure tests the rank of the long-run cointegration matrix derived from the vector error correction model (VECM) representation of the VAR model. It allows us to determine how many independent cointegrating relationships exist among the system variables. The rank test can be conducted using either the trace test or max-eigenvalue cointegration test (Enders, 2014). The results of both tests are displayed in the table below.

Cointegration rank between BTC and ETH
(maximum eigenvalue and trace test results)

Hp. No. of CEs	Eigenvalue	Trace Statistics	0.05 Critical Value	Prob.** Critical Value
None	0.013384	15.21557	15.49471	0.0550
At most 1	0.000358	0.393643	3.841465	0.5304
Hp. No. of CEs	**Eigenvalue**	**Max-Eigen Statistics**	**0.05 Critical Value**	**Prob.** Critical Value**
None *	0.013384	14.82192	14.26460	0.0408
At most 1	0.000358	0.393643	3.841465	0.5304

Max-eigenvalue test indicates 1 cointegrating equation(s) at the 0.05 level
* denotes rejection of the hypothesis at the 0.05 level; **MacKinnon, Haug and Michelis (1999) p-values.

The max-eigenvalue test indicates the presence of one cointegrating equation (CE) at the 5% level over the examined sample, while the trace statistics is borderline at the same significance level. This suggests that the log prices of ETH and BTC tend to move together in the long run and, while short-term deviations may occur over time, they revert to a stable relationship.

In summary, the prices of the two CAs exhibit time-series features that, at least in terms of order of integration, align fully with those of mainstream (yet volatile) financial variables.[(c)] Additionally, our analysis highlights a cointegrating relationship between the log prices of ETH and BTC, indicating that their long-term dynamics are closely tied.

While the presence of a cointegrating relationship between BTC and ETH suggests a degree of co-movement, it does not necessarily imply convergence in their price dynamics with traditional financial assets. To further explore whether CAs follow similar long-term trajectories as conventional financial instruments, we applied the Phillips and Sul (2007) convergence testing framework.

Phillips and Sul (2007; henceforth PS) demonstrated that a set of time-varying multiple common factors driving the price dynamics of several financial assets can be described within a time-varying single-factor modelling framework. Based on this result, they proposed testing for convergence by decomposing time series into a common growth component and heterogeneous idiosyncratic components. The key idea underlying this approach is to determine whether individual series eventually follow a similar trajectory relative to the common trend. This is done through a log-t regression test, which in broad terms examines whether the cross-sectional variance of relative transition paths vanishes over time.

Unlike traditional convergence models (β- and σ-convergence), the PS methodology allows for divergent time paths as well as individual heterogeneity. Thus, this approach is well-suited for testing convergence of financial asset prices, as financial markets are typically characterized by cross-sectional heterogeneity and time-varying volatility. Additionally, the PS approach is highly flexible. Differently from conventional unit root and cointegration tests, it does not impose any assumption regarding stationarity or non-stationarity, as it is robust to the stationarity properties of the variables under study. Lastly, this methodology enables the endogenous

determination of convergence clubs – groups of units that converge at different speeds or toward different steady states.

We applied this methodology to the same daily dataset of financial variables previously described (covering the period 2017-2024), which includes the US corporate bond index, the price of gold in USD, the Nasdaq, Dow Jones, S&P 500, BTC and ETH. The VIX and the USD/EUR exchange rate were excluded, given the unit root test results discussed earlier. Before implementing the PS convergence approach, we extracted the trend component of each time series using the Hodrick and Prescott (1997) filter.

In the first step, the full-sample results rejected the null hypothesis of overall panel convergence at the 5% significance level, suggesting that the examined financial assets do not converge as a single group. Consequently, in the second step, we applied the clustering algorithm proposed by PS to identify convergence clubs. Specifically, the results presented in the following table indicate the presence of two distinct convergence clubs:

- club 1: Dow Jones, Nasdaq, Bitcoin and Ethereum
- club 2: US corporate bond index and gold.

The first club consists of assets that are typically more sensitive to investor sentiment, liquidity conditions, and macroeconomic factors. Notably, Bitcoin and Ethereum, as major CAs, have increasingly shown correlations with equity markets, particularly during periods of market exuberance or risk aversion. The inclusion of both stocks and CAs in the same club suggests that crypto markets are becoming more integrated with traditional equity markets.

In contrast, the second club consists of financial assets traditionally associated with lower risk and 'safe-haven' properties. Gold, a store of value in times of market stress, has long been known to exhibit a different risk-return profile compared to equities and crypto assets. Similarly, corporate bonds tend to move differently from equities and cryptos, reacting more to credit risk and unexpected monetary policy shocks rather than pure market sentiment.

Convergence Tests for Cryptocurrencies and Standard Financial Assets

Full sample: Gold. US corporate bond index. Nasdaq. Dow Jones. S&P 500. Bitcoin. Ethereum (*)		Club 1: Bitcoin. Dow Jones. Nasdaq. Ethereum		Club 2: Gold. US corporate bond index	
beta	-0.200	beta	0.0878	beta	2.6147
std.err.	0.054	std.err.	0.0727	std.err.	0.6794
tvalue	-3.738	tvalue	1.2076	tvalue	3.8486
pvalue	0.000 **	pvalue	0.8864	pvalue	0.9999
		cstar	0	cstar	0

* S&P 500 is the only element of the full sample not included in either of the two sub-samples (the 'clubs'), on the ground of divergence. ** denotes rejection of the null hypothesis of convergence at the 0.05 level.

This confirms the growing financialization of CAs, particularly Bitcoin and Ethereum, which now exhibit price behavior more aligned with traditional risky assets rather than alternative stores of value. These results highlight that crypto markets are not isolated from broader financial cycles and, specifically, may be increasingly influenced by macroeconomic shocks affecting equity markets.

(a) The topic is discussed in several manuals on econometrics. A standard valuable reference is Davidson and MacKinnon (1993).
(b) The VIX is an index that measures the expected volatility of the stock market based on the implied volatility of a portfolio of S&P 500 options.
(c) More in depth analyses will help to shed additional light on these patterns, bearing in mind the point raised by Gianfreda, Maranzano, Parisio and Pelagatti (2023), who argue that unit root and cointegration tests are biased towards stationarity on noisy times series.

Overall, these findings on price developments offer quite different conclusions from those we have gathered in the analysis of the classification of CAs (Figure 7), and on the headline results on price developments (Figure 8 and Figure 9). There, we concluded that each CA is nearly unique in terms of its characteristics and categorization; here, we find that they broadly move in tune, without

deviating too much from traditional assets. Against this background, one could surmise that the perspective of the financial trader is prevailing over that of the crypto guy. While the latter focuses on the distinct features of each coin, blockchain and so on and so forth, the former organizes his trading treating major CAs as close substitutes. He buys and sells them based on general price developments and market liquidity considerations.

We interpret these findings as preliminary evidence of the ongoing financialization of the crypto market.[100] In other words, the main CAs are progressively resembling traditional financial assets, specifically equities, at least from the perspective of financial markets. The process is likely not yet complete, and some degree of market segmentation still appears in the evidence we have gathered, particularly when considering the classification described in Box 1. Further research is needed to shed light on the extent to which leading CAs are suitable for inclusion in standard financial portfolios, or at least whether they are approaching the stage in which they can be used for that purpose.

The US market, which is witnessing a wave of significant crypto activity by banks, is an obvious place to look for insights into the foundations of these developments (Box 3).

Box 3

Selected news on US banks increasingly investing on crypto-assets (a)

Based on available information, major players in the US financial market largely ignored Bitcoin in its infancy years. The gradual shift in this attitude prompted, in 2017-18, the Chicago Board Options Exchange (CBOE) and the Chicago Mercantile Exchange (CME) to launch Bitcoin Futures contracts(b), while major banks such as Goldman Sachs and Morgan Stanley started setting up their crypto trading desks. It took other two to three years before this approach gained more traction, including adoption by JP Morgan and Citigroup, and Bitcoin started being regarded by traders as an acceptable form of investment.

The growth of the segment has required adaptations in the stance taken by US regulatory agencies, until the landmark decision by the US Securities and Exchange Commission (SEC), reportedly under pressure from a 2023 D.C. Circuit Court of Appeals ruling, to authorize the first spot crypto ETF in early 2024. This has offered a way to gain direct spot exposure to the CAs on which the ETFs invest without holding the coins directly (something which most US banks and financial intermediaries are not allowed to do). Spot bitcoin ETFs are currently available also in Canada, Germany, Brazil, Australia, Switzerland, Hong Kong, among other countries.

Besides futures contracts and shares in ETFs, a third option for US financial intermediaries is to invest in crypto coins indirectly by purchasing stocks of companies heavily exposed to the coins themselves. MicroStrategy, originally an IT firm, which has reportedly purchased Bitcoins worth in total 44 billion US dollars, is a good example of this wave.

Overall, 2024 is widely regarded as the year when CAs have become a more mainstream asset class. The building up of such momentum is reckoned to be the result of changes in (i) regulation, with efforts being promoted across a number of jurisdictions although 'there remains a lack of consensus on how to approach cryptocurrency regulation globally'; (ii) technology, bearing in mind that 'Ethereum's successful transition to Proof of Stake (PoS) in 2022 has demonstrated that it is possible to reduce the environmental impact while improving scalability and transaction speed'; and, (iii) distribution, via the launch of exchange-traded products (the two quotes are from Talha, 2025).

(a) Based on: 'Why Large Banks are Increasingly Using Bitcoin (BTC)', 31 October 2024, and 'What Are Bitcoin Futures and How to Trade', 12 November 2024, both available at https://www.moomoo.com/; 'Cryptocurrency ETFs: An Overview', updated on 28 May 2024. www.investopedia.com/; 'The Growing Gap For Investors Outside The U.S. To Access Crypto ETFs', 17 October 2024, https://www.forbes.com/; 'MicroStrategy Acquires 2.530 BTC and achieves BTC Yield of 0.32% YTD 2025; Now Holds 450.000 BTC', 13 January 2025. https://www.microstrategy.com/.

[100] We adopt this term following Palley (2007), 'Financialization is a process whereby financial markets, financial institutions, and financial elites gain greater influence over economic policy and economic outcomes'.

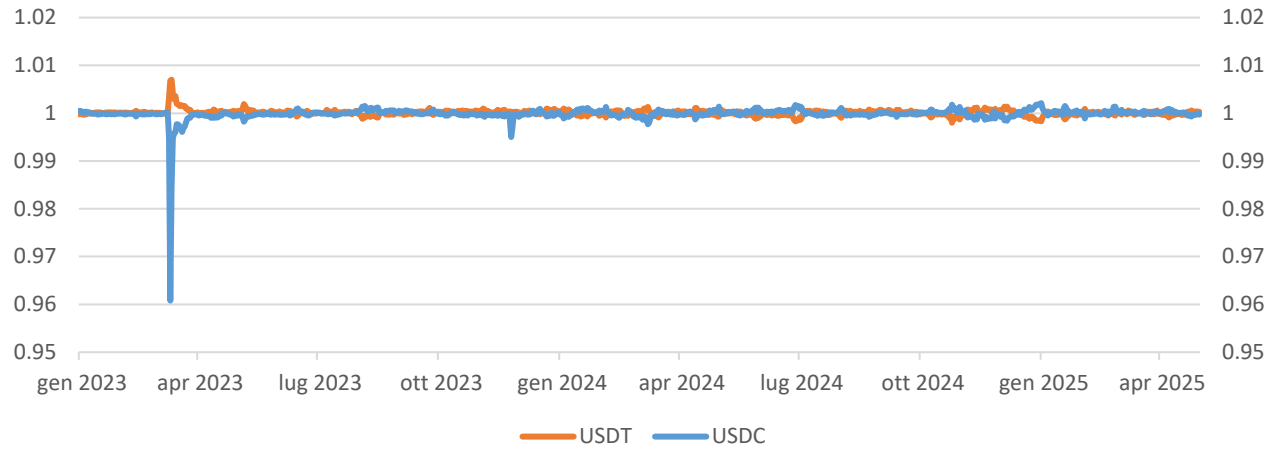
So far, our empirical analysis has mainly focused on BTC (Bitcoin) and ETH (Ether), the two leading coins by overall capitalization, each being the top coin within its crypto sub-sector, platforms and means of payment, respectively (see Box 1). It is important though to shed light also on the stablecoin subsector, where the bulk of the crypto market transactions takes place. We do so by verifying whether the two stablecoins included in the top-30 list (see Table 2), USDC and USDT, have maintained their promised peg to the USD (Figure 10). If USDT and USDC were to fail to do so, this could lead to a loss of confidence and broader instability in crypto markets, not least because USDT and USDC serve as key trading pairs on many exchanges. A divergence from the intended peg could disrupt liquidity, impact pricing across markets, and even lead to contagion effects, where instability in one asset spreads to others.

As a matter of fact, except for a few short-lived fluctuations, the prices of these two coins have fluctuated thus far narrowly against the parity.[101] In Chapter 2, we noted that the way CAs are spent resembles the transfer of physical cash from person to person. The sustained parity with the USD suggests that these two stablecoins can be regarded as a digital equivalent of USD banknotes, albeit with one important difference: transferring a large sum of physical banknotes in dollars implies a serious logistical effort and takes time, at least in the number of days. Conversely, the transfer of an equivalent amount of USDT or USDC can be immediate, straightforward, and subject to limited fees.

Figure 10

Price of USDT and USDC (1)

(in USD; daily data)



Source: Investing.com.

4.3 Crypto exchanges

Exchanges are an essential pillar of the crypto world, as they enable the conversion of fiat currencies into CAs and vice versa, the so-called on- and off-ramp stages, while also facilitating exchanges between CAs (see Section 2.1). In this Section, we focus on these stages, for which more data are available; it is worth bearing in mind however that around two thirds of transactions would occur between CAs (ESMA, 2024a). Table 4 below lists the current top 30 exchanges, according to CoinMarketCap. Additional information includes the jurisdiction of each exchange and whether it supports the US Dollar, the euro, and the British Pound.

[101] Here, a warning similar to the one we put forward at the beginning of this chapter applies. The fact that, in our sample, USDC and USDT displayed their promised peg to the USD does not imply necessarily that they will continue to do so under strain in the future.

Table 4

Leading crypto exchanges

(data as of 6 May 2025

Rank	Name	Market share	Jurisdiction	Support to:		
				USD	EUR	GBP
1	Binance	27.77%	Hong Kong		✓	✓
2	Bitget	5.69%	Seychelles	✓	✓	✓
3	Bybit	5.41%	British Virgin Islands	✓	✓	✓
4	OKX	5.12%	Seychelles	✓	✓	✓
5	MEXC	4.95%	Singapore	✓	✓	✓
6	HTX (Huobi)	4.68%	Singapore	✓	✓	✓
7	Coinbase Exchange	4.37%	United States	✓	✓	✓
8	Gate.io	3.75%	Panama	✓	✓	✓
9	WEEX	3.59%	Singapore			
10	Crypto.com	3.17%	Cayman Islands	✓	✓	
11	Kraken	2.41%	United States	✓	✓	✓
12	KuCoin	2.20%	Seychelles	✓	✓	✓
13	Bitunix	1.59%	Saint Vincent and the Grenadines	✓	✓	✓
14	Lbank	1.53%	PR China	✓	✓	✓
15	Bitrue	1.47%	Singapore	✓	✓	✓
16	PancakeSwap V3 (BNB)	1.15%	DEX, no single centralized jurd. (a)			
17	Uniswap V3 (Ethereum)	1.12%	United States (b)			
18	BiTMart	0.99%	Cayman Islands	✓	✓	✓
19	Upbit	0.93%	Singapore			
20	WhiteBIT	0.90%	Lithuania	✓	✓	✓
21	CoinW	0.87%	Australia	✓	✓	✓
22	AscendEX	0.84%	Singapore	✓		
23	Orca	0,76%	DEX, no single centralized jurd. (a)	✓	✓	✓
24	Poloniex	0.73%	United States	✓		✓
25	Bithumb	0.71%	South Korea			
26	DigiFinex	0.64%	Singapore	✓	✓	✓
27	Aerodrome	0.63%	DEX, no single centralized jurd. (a)	✓	✓	✓
28	BTSE	0.57%	British Virgin Islands	✓	✓	✓
29	Bitforex	0.57%	Hong Kong			
30	Uniswap V3 (Arbitrium)	0.56%	United States (b)			

Sources: CoinMarketCap (https://coinmarketcap.com/) for market share and fiat currencies supported; Cryptorank (https://cryptorank.io/exchanges) for jurisdiction (unless otherwise specified); (a) based on queries in Google; (b) Uniswap Labs, the company behind the Uniswap exchanges, is based in NY City, USA.

As a first stylized fact, the market is heavily concentrated. According to our source (Coinmarketcap), out of a total of 253 exchanges (as of 6 May 2025), the top-10 ones control a market share of 69% and the top-30 ones a share of 90%. Binance is by far the leading player, with a market share of nearly 28%, followed by three other exchanges that command each between 5% and 6%. A similar finding of concentration in market shares was already highlighted by ESMA (2024a).

Turning to the jurisdictions of the exchanges, 7 out of the top-30 ones are under that of Singapore, 5 under the United States' one, followed by 3 exchanges from Seychelles, and 2 each from Hong Kong, British Virgin Islands and Cayman Islands. One exchange operates under the jurisdiction of

an EU country (Lithuania). For three exchanges, our source, Cryptorank, specifies 'not settled', probably to be understood that these are decentralized exchanges (DEX).

The fiat currency most widely supported is the US dollar, managed by 22 out of the top-30 exchanges, followed by the euro and the British pound, each supported by 21 exchanges. However, the business is by no means confined to these three currencies, and we could identify other 64 fiat currencies supported by at least one of such exchanges. It is of note that the Yuan Renmimbi, the currency of the People's Republic of China, is not among them, as Chinese authorities appear to channel business through the Hong Kong dollar, supported by 9 exchanges.

The distribution of exchanges based on supported fiat currencies reveals significant overlaps. Bearing in mind the figures of 22 and 21 that we have just mentioned for the US dollar and the euro, respectively, 20 exchanges support both two leading currencies (Figure 11, overleaf). One exchange supports only the US dollar as its single fiat currency, while no exchange, at least among the top 30, supports only the euro.

The picture seems to be changing fast, though. We gauge that comparing the results we have just cited with those we obtained in a first data collection run in January 2025: then, the US dollar emerged more markedly as the top fiat currency, compared to the euro. In turn, that finding echoed what previously reported by ESMA (2024a, p. 7), which noted 'a clear dominance of the US dollar and the South Korean won [which it still sets a cluster of its own, based on our evidence], which together account for around 80% of fiat volume', while 'The euro plays only a minor role, with a relatively stable share of around 10%'.

What has not changed between our January and May data collections is the finding that the 20 (out of top 30) exchanges supporting both the US dollar and the euro tend also to support a range of other major fiat currencies. Within this subset, we could count 9 out of the 10 exchanges supporting the UAE Dirham (AED), 15 out of 17 for the Australian Dollar (AUD), 15 out of 16 for the Canadian Dollar (CAD), 11 out of 12 for the Swiss Franc (CHF), 19 out of 21 for the British Pound (GBP), 11 out of 12 for the Hong Kong Dollar (HKD), and 6 out of 7 for the Russian Ruble (RUB; Figure 11). Namely, we are witnessing a digital world in which, for instance, one can convert Rubles into a CA, and then after a variable number of iterations throughout the crypto-world, maybe to hide traces, one exits converting back CAs into the US Dollar, or from the Pound to a mix of HK dollar and Swiss Francs, and so on and so forth. Easy to guess the scope for licit but also illicit activities.

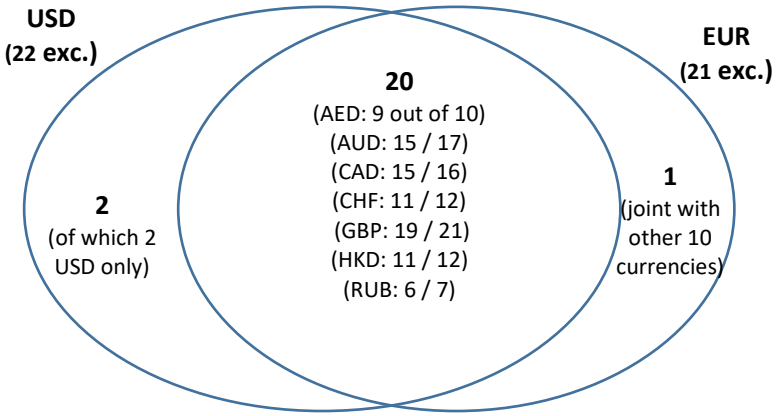
This type of analysis allows us to explore the topology of the crypto market in terms of fiat currency connectivity. A separate but equally important dimension concerns the volume of fiat currencies used in transactions with CAs. It should be noted from the outset that compiling accurate and comprehensive statistics on this specific dimension is highly challenging. Nonetheless, various indicators point in the same direction.

For example, a market source such as Coinhills (https://www.coinhills.com/market/currency/) reports that, over the 24 hours ending on May 7, 2025, 87.6% of Bitcoin conversions involved the US dollar. This figure appears to be broadly representative of a stable pattern: a July 25, 2024, article on Investopedia (link) cited a similar share of 83.7% (https://www.investopedia.com/tech/top-fiat-currencies-used-trade-bitcoin/). Likewise, based on the qualitative information we could gather, the US dollar is reckoned to be also the dominant fiat currency in fiat-to-Ether trading.

Taken together with the fact that the bulk of trading across the CA market involves stablecoins (see Table 2 above), most of which are pegged to the dollar, the picture becomes quite clear.

Figure 11

Distribution of exchanges in terms of supported fiat currencies (1)



(1) Authors' elaboration on CoinMarketCap (https://coinmarketcap.com/) data, as of 6 May 2025.

Chapter V: Concluding remarks and possible AML actions on Crypto Assets

Famously, follow the money and you have a chance to gather valuable information on crime. In the world of CAs, enacting the first part of this sentence is relatively easy. Every fully fledged node of the blockchain – a status which can be acquired by any individual or organization with decent IT equipment – has access to all transactions that have ever been executed.[102] However, as a relevant downside, what one reads is that a certain cryptographic address – a string of up to 34 digits and characters – has been involved in a transaction with another similar address, with generally no hint of the physical person or entity behind the address. When obfuscation tools are employed, it is not even clear what is the output address corresponding to a target input one. Quipping on this situation, Möser, Böhme and Breuker (2013, p. 1) noted that 'AML in Bitcoin has to deal with imperfect knowledge of identities but may exploit perfect knowledge of all transactions'.

This unique element calls for new strategies. The extant EU legal set-up and the available address clustering techniques, while offering important breakthroughs, do not fill entirely the said gap in information of identities, nor major improvements can reasonably be expected by acting just on one or the other front.

Approaching the CAs thus requires a certain degree of flexibility, as one must account for multiple dimensions. It also demands the willingness to invest time in a winding journey, which mixes new things to things that are not new, but which may reappear in unfamiliar forms that are not immediately recognizable.

To try to give an order to many fragments of information, we organize this concluding chapter as follows. First, we list the main facts we have identified, to turn then to illustrating some key trends. Third, we address what we, among others, regard as false myths. Finally, we put forward some possible lines of AML action.

The facts

Firstly, CAs set a stand-alone category, which cannot be encapsulated neatly under either the traditional categories of token-money or account-based money. Accordingly, they call for bespoke action.

Holding unique features does not mean that every trait is novel, or that fundamental questions can be regarded as obsolete. One needs to accept, however, the realities of new worlds. For the scopes of a report on CAs and AML, a notable instance in which 'standard approaches' meet such realities is in terms of the customer due diligence measures, which are part of a broader AML framework of obligations (AMLR, Art. 19) and represent a hallmark of the EU banking legislation.

From a legal standpoint, it makes no difference whether a CASP – exchanges are the most glaring example within this category – is (1) originally established within the Union or (2) is headquartered in an overseas country and operates in the EU having obtained the required license ('overseas exchange with EU license'). Either way, the CASP must comply with the obligations when conducting business in Europe. In principle, the IP of the client's device and the version of the exchange's Internet website designed for the user's supposed jurisdiction should help to assess

[102] Additionally, one also knows the sequence in which transactions have been validated (which approximately coincides with the chronology of their execution) since transactions are grouped in blocks and each block is indexed to the previous one. Moreover, with the highest degree of confidence, this wealth of information can be regarded as pristine since there is no way to tamper it. More caution should be adopted with respect to most recent (up to six) blocks. Basically, this means that one can trust the reliability of every transaction on the blockchain older than an hour or so.

whether this is the case. However, the borderless nature of the cyber world – a customer could hit the foreign website, rather than the European-tagged one – and the ease to mask the own location and origin (a good VPN being a simple tool to do so) can arguably blur the picture. Nor is there gain in ignoring that an overseas exchange, especially one purposely based in a country with mild AML obligations, would give serious consideration to meeting the demands of those segments of customers keener on strong privacy protection.[103]

Secondly, CAs are far from defining a homogeneous block. Even when sub-categories are identified for purposes of legal construction or analysis, a substantial degree of heterogeneity remains.

The heterogeneity of CAs is evident in the statistics shown in Figure 7, which highlight the limited degree of bilateral overlap in the classification of top-30 CAs by market capitalization. More indirect but not less insightful evidence is offered by the EU legislator. In the MICAR, after having introduced two categories of stablecoins, the regulator ends up describing all other CAs in negative terms ('crypto-assets other than asset-referenced tokens and e- money tokens …'; MICAR, Recital 18).

When this heterogeneity is coupled with the sheer number of CAs, estimated at around 10,000, it becomes clear that acquiring a comprehensive understanding of each coin (not to mention the underlying blockchains and other tools) is an immense task. Probably, a more realistic and satisfactory goal might be achieving a solid knowledge of most common coins (perhaps the top 100). Even such limited level of knowledge would require law-enforcement agencies, supervisory authorities, and financial intelligence units to be adequately staffed.

Thirdly, obfuscation tools and privacy coins facilitate the efforts of those very keen on their anonymity when operating in CAs. Many types of software are nowadays available on the shelf to support the identification of clusters of crypto addresses within blockchains: in Section 2.5, we cited two sources counting 73 and 97 such types of clustering tools, respectively. Possibly, the number is larger than that. However, one cannot rely solely on these clustering tools. While the entire sequence of transactions can be read through a fully-fledged node, obfuscation tools – such as decentralized tumblers, ring signatures, chain hopping, etc. – exist precisely to hinder the information one can extract from the blockchain.

The fact itself that new contributions add all the time to the literature on clustering techniques is a double-edged sword. On the one hand, it reflects opportunities to improve current methodologies. On the other hand, if there is demand for papers filling entire libraries, probably there is an underlying difficulty to reach any general, robust, solution.

Fortunately, the idea that no blockchain or CA is entirely immune to investigation is not mere wishful thinking; as shown in Section 2.4, convincing results have been achieved even for highly regarded privacy coins such as Monero. Still, gaps identified by researchers are often quickly fixed by the IT community working on blockchains, typically to the benefit of privacy seeking users.

Fourthly, while Europe expresses a significant share of global demand for CAs, it appears, at least at the time of writing, to have comparatively less influence over the entities active in this sector.

On the demand side, data such as those we reported in Section 1.5 suggest that the volume of demand in Europe is on par with that of the United States. However, the imbalance is evident on the supply/management side: only one of the top-30 exchanges listed in Table 4 is headquartered in the European Union and available evidence points to a limited role of the euro compared to the US dollar in trading between fiat currencies and CAs; the same message is offered by ESMA (2024a), a report

[103] Tellingly about the preferences upheld by global audiences, some exchanges aggressively market their offer for privacy. A noticeable example is the choice of an exchange to brand itself as 'Nonkyc.io Exchange'(https://nonkyc.io/).

on market structures and EU relevance on CAs (specifically its Chart 7). Additionally, there are broader concerns regarding the nationality of firms offering cloud and related ITC services.

No single statistics can offer a complete measure but, overall, the picture emerges of limited soft power which, as things stand now, European authorities can exert on entities whose allegiance is due first to non-European powers.

Fifthly, the extant EU legal framework (and probably not only the EU one) is structured around the entry points into the crypto ecosystem, imposing obligations on intermediaries, while leaving peer-to-peer traffic and DeFi applications largely unregulated.

This emphasis on intermediaries, and by association on the on- and off-ramp phases, might reflect the view that CA holdings are an intermediate step between one fiat currency and another. In fact, however, the growing adoption of CAs suggests they increasingly serve as ends in themselves. Today, CAs can be used for purchases in standard retail shops,[104] as well as in the real estate market[105] and in luxury goods.

In a way, this squares the circle, bringing us back to the first point in this sequence. A legal framework on CAs rooted in the traditional banking and financial regulation naturally tends to center on established (and supervised) intermediaries. However, this is not the required bespoke approach to address blockchain-based transactions, which often occur without any intermediary, leaving room to direct peer-to-peer contacts, as it happens with physical banknotes.

The tendencies

The rate of penetration of CAs amongst households is gradually increasing, having reached – according to survey by Statista – a share of 16% in the United States and 12% in the euro area. These are figures which are large enough to signal that the growth phase of this specific product is under way, as one can no longer speak of roll out and niche use. As we wrote in Section 1.5, if the standard product life cycle applies once again, the odds are that such rate could surge in a few years.

As a side effect, elaborating on the theory of innovation cycle developed by Schumpeter, one can expect a tendency towards concentration among main market players, if not a monopoly altogether (possibly, at the level of the sub-sectors identified in Box 1). So, an educated guess would predict in the coming years even bigger shares held by leading CAs – based on data of our Table 2, at present Bitcoin (BTC) and Ether (ETH) are obvious candidates in terms of capitalization and Tether (USDT) in terms of turnover – and exchanges.

In parallel, we are witnessing a convergence of CA markets towards markets of more traditional financial assets, in terms of patterns (but not yet of volatility). This is happening not by chance, in the light of the increasing role being played by well-established intermediaries, reportedly mainly from North America. What was initially conceived as a crypto anarchist ideology of a financial system independent of traditional intermediaries is turning more and more gentrified.

The myths

Decentralization is (was?) meant to be the hallmark of the crypto world. That being acknowledged, it is debatable the extent to which this claim still meets reality nowadays. The

[104] See for example the website https://www.bitpay.com/directory for a list of more than 250 major retailers accepting Bitcoins, including Starbucks and Microsoft.

[105] A company such as XEROF (https://www.xerof.com/about-us) acts as a gateway for clients interested in real estates, through major realtors such as Engel & Völkers and REMAX, and it accepts equally international fiat currencies and leading CAs.

concentration in market shares we have just mentioned but also the rising cost of mining (see Figure 3) all point to the opposite direction. The crypto world is clearly aware of the issue and is seeking to strike a balance between centralization and decentralization.[106]

Our frequent (too frequent perhaps) use of Internet, especially through wireless connections, could convey a sense of immateriality. In fact, Internet is very physical: cables travel across oceans and connect the continents,[107] servers in big data centers are the repositories of our 'digital' memory and life.

A certain degree of centralization and the physical dimension of the Internet give scope to law enforcement agencies and anti-money laundering agencies: there is something to be searched, which is not lost 'in the thin air'. The extent to which this can succeed across so many jurisdictions involved is a different question.

The possible lines of action

Firstly, there is significant scope for synergies in monitoring the market for IT tools designed to analyze and explore blockchains and related instruments, such as smart contracts. For a single law-enforcement agency or a FIU, it could be difficult to keep up with developments in this rapidly evolving market, and even more difficult to train enough analysts in their use, not to mention the associated costs. Hence, it would make sense to share expertise and experiences, under the coordination of a single intelligence unit operating at the international (European Union) level. Smooth cooperation among experts in the field would help to better separate the wheat from the chaff, increasing efficiency in the IT selection process as well as saving valuable budget resources during procurement.

Secondly, several times throughout this report we have argued in favor of a bespoke approach to regulation, considering the unique characteristics of CAs. As a concrete example of this line of thinking, the distribution of roles between home and host authorities, a core element of the EU banking and financial legislation, could gain from a more flexible interpretation in the context of CAs (see fn. 90). Noticeably, ways should be sought to ease contacts between (host) FIUs and CASPs licensed from other EU countries, especially if originally headquartered outside the EU, while preserving the overall home-host architecture. Such added flexibility would better match the fluidity that arguably defines the links, within the borderless cyber world, between the intermediary and the customer basis as broken down by country.

Thirdly, further legislative work should give content to the call laid down in Recital 160 of the AMLR on the prohibition of a range of anonymous activities in CAs. Simply put, while the right to privacy is a cornerstone of democratic societies, it must not be conceived as a right to secrecy.

Fourthly, additional empirical research is warranted. Based on available evidence, it is reasonable to expect some strengthening of the trend of what we have described as the financialization of the CA market. This development could be leveraged to impose effective restrictions on financial intermediaries engaging with anonymous coins or blockchains designed to maximize user secrecy. Over time, such measures could lead to the emergence of market segments characterized by both higher liquidity and lower levels of obfuscation. There is plenty of evidence showing that financial market participants, regardless of their type, place a high premium on liquidity. As a result, they may well opt for the most liquid financial instruments, even when these provide only partial hedging for their desired investment strategy (i.e., a less liquid instrument can be a suboptimal choice despite

[106] See the blog 'Decentralization in Crypto: A Myth or Reality?' in the CoinMarketCap website (https://coinmarketcap.com/academy/article/4dc9c34c-b600-4cd1-8ba4-5bcdbd3f1b6d).

[107] See the New York Times' article 'People think that data is in the cloud, but it's not. It's in the ocean' for a good, non-technical introduction (https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html).

offering a better hedge). In practical terms, this could mean that even criminal organizations might be willing to forgo some layer of security, if that is the 'price' to gain access to the most actively traded CAs.

Finally, efforts should be made to develop the publication of regular statistics on CAs coherent with the standards of the profession, the staple for any sound research. This is acutely felt across the board and even more so in respect to the peer-to-peer traffic, including that on stablecoins, which increasingly exhibit the potential to serve as substitutes for fiat currencies.

To conclude, this report has provided an overview of the world of CAs across multiple dimensions, based on information available as of the end of April 2025. We are aware that this world is moving fast: many signals point in this direction, calling for sustained attention, also through renewed and updated analyses. Concerning the CA market microstructure, we have already observed significant changes between the initial data collection for this research and the more recent data ultimately used. Likewise, the fast pace of transformation of financial markets is self-evident. Certain segments of CA markets are converging, at least in some respects, to patterns prevailing in more traditional financial instruments. In particular, the systematic collection of data will be crucial for advancing future analyses, especially concerning market liquidity.

This ongoing phase of transformation calls for appropriate governance. As put forward by an authoritative source, the construction of a comprehensive EU digital finance regulatory framework has only just begun (Annunziata, 2023). One way or the other, the European legislator will need to address the areas left outside the scope of MICAR and of the AML Package (P2P and DeFi paradigms, NFTs). Similarly, regulatory solutions should be developed to mitigate the different impact of whether a CA falls on either side of the cliff separating the MICAR and MIFID 2 – with payment sector regulation providing for a further dimension – to reduce the supervisory burden for authorities and fragmentation in the applicable law.

The speed of change in the crypto world – which possibly will abate once the sector matures – is such that the rationale behind the original 2020 decision to centre MICAR on stablecoins has been amply overtaken by subsequent developments. From a European perspective, the level of use attained by 2025 by stablecoins pegged to the US Dollar is a cause for concern (creating a basis for the 'dollarization' of the economy), albeit for quite different reasons from those surrounding the earlier Libra project. This speaks volumes about how protracted a five-year interval can be in the cyber world.

Additional challenges will likely emerge over time. To prevent a losing cat-and-mouse race, a more comprehensive regulatory framework should be explored. Several proposals have already been laid down, including the so-called default rule, which would consider by default CAs as transferable securities unless an exemption is granted. This would make the regulatory field more homogeneous and reverse the onus of arguing that a given CA is outside the scope of EU financial regulation. Notably, this idea has gained traction in institutional settings, for instance in a report prepared at the request of the Committee on Economic and Monetary Affairs of the European Parliament (Zetzsche, Buckley, Arner and van Ek, 2023). Further work should continue along these lines.

References

(URLs cited in the report were verified as of 30 April 2025 latest. unless otherwise specified)

Adrian T. and T. Mancini-Griffoli (2021). The Rise of Digital Money. *Annual Review of Financial Economics.* Vol. 13: 57-77.

Annunziata F. (2023). An Overview of the Markets in Crypto-Assets Regulation (MiCAR). *European Banking Institute (EBI), Working Paper*, no. 158.

Annunziata F. (2025). Tassonomia delle cripto-attività e disciplina del mercato dei capitali: un confronto tra Stati Uniti e Unione europea (paper in Italian, 'Taxonomy of crypto assets and discipline of capital markets: a comparison between the United States and the European Union'). In: Banca d'Italia, Legal Research Papers, no. 103.

Antonopoulos A.M. (2017). *Mastering Bitcoin*. O'Reilly Media. Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

Badev A. and M. Chen (2014). Bitcoin: Technical Background and Data Analysis. U.S. Federal Reserve Board. Washington. D.C., Finance and Economics Discussion Series, no. 2014-104.

Balaskas A. and V.N.L. Franqueira (2018). Analytical Tools for Blockchain: Review. Taxonomy and Open Challenges. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*.

Balsa E. (2019). Chaff-based profile obfuscation. PhD Dissertation. Arenberg Doctoral School. Faculty of Engineering Science.

Barsan I.M. (2017). Legal Challenges of Initial Coin Offerings (ICO). *Revue trimestrielle de droit financier (RTDF)*. Vol. 3, pp. 54-65.

Bech M. and J. Hancock (2020). Innovations in payments. *BIS Quarterly Review*. March issue, 21-36.

Biancotti C. (2022). What's next for crypto? *Bank of Italy, Occasional Papers*, no. 711.

Bullmann D., L. Cardone, A. Delcroix, D. Fornaro, C. Kaufmann, G. Kiewiet, U. Kochanska, E. Kondracka, S. Kördel, J. Körner, K. Löber, M. Mayers, A. Pinna, S. Palligkinis, A. Tracz, and A. Vouldis (Bullmann et al.) (2019). Crypto-Assets: Implications for financial stability. monetary policy. and payments and market infrastructures. *ECB, Occasional Paper*, no. 223.

Butler S. (2019). Criminal use of cryptocurrencies: a great new threat or is cash still king? *Journal of Cyber Policy*. Vol. 4(3): 326-345.

Carlisle D. (2017). Virtual Currencies and Financial Crime - Challenges and Opportunities. *Royal United Services Institute for Defence and Security Studies (RUSI),* Occasional paper, March.

Coelho D.P. and M. Q. Poças (2024). The construction of the legal definition of crypto-assets under MiCAR. including legal subcategories: a very brief updated summary based on the guidelines of the European Supervisory Authorities. Available at SSRN: https://ssrn.com/abstract=4887419 or http://dx.doi.org/10.2139/ssrn.4887419.

Committee on Payments and Market Infrastructures. CPMI (2018). Central bank digital currencies. BIS.

Davidson R. and J.G. MacKinnon (1993). *Estimation and inference in econometrics*. US. New York. Oxford University Press.

ECB (2019). Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. ECB, Occasional Paper Series, no. 223.

Enders, W. (2014). *Applied Econometric Time Series*. Wiley Series in Probability and Statistics. 4th Edition.

ESMA (2024a). *Crypto assets: Market structures and EU relevance*.

ESMA (2024b). *Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments.*

European Parliament (2017). Understanding equivalence and the single passport in financial services. Third-country access to the single market. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599267/EPRS_BRI(2017)599267_EN.pdf.

FATF (2014). *Virtual currencies. Key Definitions and Potential AML/CFT Risks*.

FATF (2019). *Guidance for a risk-based approach. Virtual assets and virtual asset service providers*.

Ferreira A. and P. Sandner (2021). EU search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review*. Vol. 43.

Fletcher E., C. Larkin and S. Corbet (2021). Cryptocurrency Regulation: Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*. Vol. 57.

Fliche O., J. Uri and M. Vileyn (2023). Decentralised or disintermediated finance: what regulatory response? *Banque de France. Discussion Paper*.

Gabriel U., S. Areo, H. Oyadoke, B.F. Okhumende and J. Adeniyi (Gabriel et al.) (2024). The Impact of Bitcoin Cybercrime on the Financial System: Analyzing the Role of Crypto Mining and Criminological Behavioral Threats. *Iconic Research and Engineering Journals*. Vol. 8(3): 382-386.

Garrat R, M. Lee, B. Malone and A. Martin (2020). *Token or Account Based? A Digital Currency Can Be Both.* Available at https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/.

Gianfreda A., P. Maranzano, L. Parisio and M. Pelagatti (2023). Testing for integration and cointegration when time series are observed with noise. *Economic Modelling*. Vol. 125.

Hammad N. and F. Victor (2024). *Monero Traceability Heuristics: Wallet Application Bugs and the Mordinal-P2Pool Perspective*. Cornell University. Available at https://arxiv.org/abs/2408.05332.

Harlev M.A., H.S. Yin. K.C. Langenheldt. R.R. Mukkamala and R. Vatrapu (Harlev et al.) (2018). Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

He D., K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura. T. Saadi Sedik, N. Stetsenko and C. Verdugo-Yepes (He et al.) (2016). Virtual Currencies and Beyond: Initial Considerations. *IMF Staff Discussion Note*, SDN/16/03.

Hodrick R. J. and E.C. Prescott (1997). Postwar U.S. Business Cycles: An Empirical Investigation. *Journal of Money. Credit and Banking*. Vol. 29(1): 1-16.

Houben R. and A. Snyers (2018). *Cryptocurrencies and blockchain. Legal context and implications for financial crime. money laundering and tax evasion*. Document prepared at the request of EU Parliament. Available at https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1.

Johansen S. (1988). Statistical analysis of cointegration vectors. *Journal of Economic Dynamics and Control*. Vol. 12(2-3): 231-254.

JP Morgan (2025). Cryptocurrency Markets. December Data Suggest Ecosystem Maintained Momentum After Previous Record Month. *North America Equity Research*, 10 January.

Kahn C.M. (2016). *How are payment accounts special?* Speech prepared for the Payments Innovation Symposium, Federal Reserve Bank of Chicago, October, 12-13.

Kahn C.M. and W. Roberds (2009). Why pay? An introduction to payments economics. *Journal of Financial Intermediation*. Vol. 18(3): 1–23.

Kopp C.M. (2024). Product Life Cycle Explained: Stage and Examples. Available at https://www.investopedia.com/terms/p/product-life-cycle.asp.

Koshy P., D. Koshy and P. McDaniel (2014). An analysis of anonymity in bitcoin using P2P network traffic. Safavi-Naini. R. and Christin N. (Eds). *Financial Cryptography and Data Security - 18th International Conference*. FC 2014.

Lagos R. (2006). Inside and Outside Money. *Federal Reserve Bank of Minneapolis. Research Department Staff Report,* no. 374.

Larionov N. and Y. Yanovich (2023). Bitcoin Shared Send Transactions Untangling in Numbers. *IEEE Access*. Vol. 11: 71063-71072.

Lehmann M. (2024). MiCaR – Gold Standard or Regulatory Poison for the Crypto Industry? *Common Market Law Review*. Vol. 61: 699-726.

MacKinnon J.G., A.A. Haug and L. Michelis (1999). Numerical Distribution Functions of Likelihood Ratio Tests for Cointegration. *Journal of Applied Econometrics.* Vol. 14(5): 563-577.

Mathis B. (2023). Should Crypto-Asset Regulation Be Technology-Neutral? *Blockchain and Private International Law*, p. 66-80.

Maume P. (2023). The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification. or First Step of Many. or Both? *European Company and Financial Law Review*. Vol. 20(2): 243-275.

Milne A. (2024). Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money. *Journal of Money. Credit and Banking*. Vol. 56(8): 2199-2222.

Möser M. (2022). *Cryptocurrency Privacy in Practice*. Dissertation presented to the faculty of Princeton University in candidacy for the degree of Doctor of Philosophy.

Möser M. and A. Narayanan (2022). Resurrecting Address Clustering in Bitcoin. In: I. Eyal and J. Garay (eds). *Financial Cryptography and Data Security*. FC 2022. Lecture Notes in Computer Science. vol 13411. Springer. Cham. https://doi.org/10.1007/978-3-031-18283-9_19.

Möser M., K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan and N. Christin (Möser et al., 2018). An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*. Vol. 3: 143–163.

Möser M., R. Böhme and D. Breuker (2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *APWG eCrime Researchers Summit*. San Francisco. CA. USA. 2013. pp. 1-14.

Mosna A. and G. Soana (2023). NFTs and the virtual yet concrete art of money laundering. *Computer Law & Security Review*. Vol. 51.

Nakamoto S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf.

Palley T.I. (2007). Financialization: What It Is and Why It Matters. *The Levy Economics Institute of Bard College. Working Paper*, no. 525.

Phillips P.C.B. and D. Sul (2007). Transition Modeling and Econometric Convergence Tests. *Econometrica*. Vol. 75(6): 1771-1855.

Schwarz N., K. Chen, K. Poh, G. Jackson, K. Kao, F. Fernando and M. Markevych (Schwarz et al.) (2021). Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism. Effective Anti-Money Laundering and Combating the Financing of Terrorism. Regulatory and Supervisory Framework - Some Legal and Practical Considerations. Volumes 1 and 2. *IMF. Fintech Notes Series*.

Soana G. (2024). *The Anti Money Laundering Regulation of Crypto-assets in Europe*. Wolters Kluwer – CEDAM.

Talha H. (2025). Crypto currency in 2024: Revolution, Regulation, and the Road Ahead. Available at https://www.linkedin.com/pulse/crypto-currency-2024-revolution-regulation-road-ahead-talha-haroon-wxhhf/.

Taskinsoy J. (2019). *Blockchain: A Misunderstood Digital Revolution. Things You Need to Know about Blockchain*. Available at SSRN: https://ssrn.com/abstract=3466480 or http://dx.doi.org/10.2139/ssrn.3466480.

van der Linden T. and T. Shirazi (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*. Vol. 9(22).

Vasselin F. (2024). *Crypto-Asset Market: Classification. Composition. and Competition*. Available at SSRN: https://ssrn.com/abstract=5048914 or http://dx.doi.org/10.2139/ssrn.5048914.

Vianelli A. and A. Pantaleo (2024). *(Regulatory) History in the Making: the path to MiCAR*. Available at SSRN: https://ssrn.com/abstract=4714854 or http://dx.doi.org/10.2139/ssrn.4714854.

Vujičić D., D. Jagodić and S. Ranđić (2018). Blockchain Technology. Bitcoin. and Ethereum: A Brief Overview. *Proceedings of the 17th International Symposium INFOTEH-JAHORINA (INFOTEH).*

Wronka C. (2022). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*. Vol. 25(1): 79-94.

Yadav S.P., K.K. Agrawal, B.S. Bhati, F. Al-Turjman and L. Mostarda (Yadav et al.) (2022). Blockchain-Based Cryptocurrency Regulation: An Overview. *Computational Economics*. Vol. 59: 1659–1675.

Zetzsche D.A., F. Annunziata, D.W. Arner and R.P. Buckley (2020). The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy. *European Banking Institute (EBI), Working Paper Series,* no. 2020-077.

Zetzsche D.A., R.P. Buckley, D.W. Arner and M.C. van Ek (2023). Remaining Regulatory Challenges in Digital Finance and Crypto-Assets after MiCA. *UNSW Law & Justice Research Series*, no. 27.