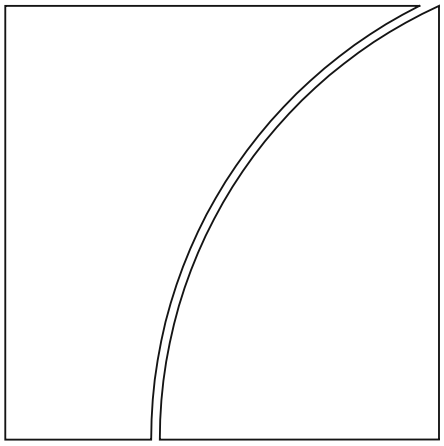


BIS Papers

No 166

From cash to crypto: towards a consistent regulatory approach to illicit payments

by Andrea Minto, Anneke Kosse, Takeshi Shirakami and Peter Wierts

Monetary and Economic Department

March 2026

JEL classification: E42, G18, G21, G23

Keywords: payments, cash, bank accounts, retail central bank digital currency (CBDC), crypto, stablecoins, anti-money laundering (AML), combating the financing of terrorism (CFT), integrity of the financial system

The views expressed in this publication are those of the authors and do not necessarily reflect the views of the BIS or its member central banks.

This publication is available on the BIS website (www.bis.org).

ISSN 1682-7651 (online)
ISBN 978-92-9259-933-1 (online)

From cash to crypto: towards a consistent regulatory approach to illicit payments

Andrea Minto, Anneke Kosse, Takeshi Shirakami and Peter Wierts[1]

March 2026

Abstract

The rapid evolution of cryptoassets, including stablecoins, and retail central bank digital currency (CBDC) has led to changes in regulatory frameworks to incorporate them. The expansion of options beyond bank deposits and cash calls for a holistic analysis of the effectiveness of anti-money laundering (AML) and combating the financing of terrorism (CFT) regimes across different payment instruments. To contribute to such analysis, this paper introduces a conceptual framework to assess the effects of AML/CFT frameworks, with a particular focus on differences in design between instruments, including the role of intermediaries. Our framework considers regulatory arbitrage between instruments. It also highlights behavioural responses to AML/CFT-related requirements that limit privacy and freedom in choosing a payment instrument. The framework is supported by a case study examining regulatory changes within the European Union (EU) that aim to increase the effectiveness of the EU AML/CFT regulatory framework across various payment instruments. Key challenges highlighted in the study include balancing privacy with integrity and ensuring consistent AML/CFT measures across payment instruments. We advocate for a consistent regulatory approach that is adaptable to future digital innovations and based on a combination of overarching principles ("lex generalis") and tailored instrument-specific measures ("lex specialis").

JEL classification: E42, G18, G21, G23

1. Introduction

Over time, technological innovations have expanded the range of instruments used for making payments, from cash, commercial bank deposits and e-money to cryptoassets and retail central bank digital currency (CBDC). Depending on their design and features, the emergence of new payment instruments can promote competition, financial inclusion and economic growth. However, a larger set of

[1] Andrea Minto (andrea.minto@unive.it): Ca' Foscari University of Venice and University of Stavanger. Anneke Kosse (anneke.kosse@bis.org): Bank for International Settlements (BIS), Takeshi Shirakami (takeshi.shirakami@bis.org), Peter Wierts (peter.wierts@bis.org): BIS. We thank Iñaki Aldasoro, José Aurazo, Danilo Bedotti, Johannes Ehrentraud, Jon Frost, Bénédicte Nolens, Andrei Pustelnikov and Daniel Rees for their valuable comments and Maureen Cramer, Fanni Leppanen, Amela Memetaj and Jirapat Siridhasanakul for excellent research assistance. The views expressed in this paper are those of the authors and do not necessarily reflect those of the BIS, the BIS Committee on Payments and Market Infrastructures (CPMI) or its member institutions.

available payment instruments also implies a larger set of means that can potentially be exploited by malicious actors to disguise the illegal origins of criminal proceeds or to finance terrorism.

The use of payment instruments for money laundering (ML) and terrorist financing (TF) undermines the integrity of the financial system. Public authorities have long worked to prevent illicit use of payment instruments and the financial system. In 1990, the Financial Action Task Force (FATF) developed recommendations to combat the misuse of the financial system for laundering drug money. Since then, payments have become subject to anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations that require customer due diligence (CDD), transaction monitoring and the reporting of suspicious transactions.

As with any financial regulation, AML/CFT frameworks have behavioural effects, both intended and unintended. According to a political economy approach, self-interested entities that become subject to regulatory constraints will re-optimise their behaviour within the new constraints. Behavioural responses are influenced by the expected costs and benefits of complying with regulatory requirements compared with alternative strategies, such as arbitrage, exploiting loopholes or outright non-compliance. For instance, emerging payment instruments such as stablecoins and other cryptoassets have been used to circumvent AML/CFT rules (Aldasoro et al (2025)).2 Policymakers are expected to address behavioural effects that weaken the effectiveness of the rules, for example by broadening the scope of application and/or increasing the expected costs of non-compliance (by increasing both the probability of detecting non-compliance and the expected penalty upon detection). This is why the effectiveness of AML/CFT frameworks has constantly been subject to extensive discussions, as a result of which frameworks have evolved over time.

The aim of this paper is to contribute to the literature on the effectiveness of AML/CFT frameworks by examining the dynamics between behavioural adjustments and regulatory responses. Our key question is: how may AML/CFT frameworks influence, or even distort, the choice of payment instruments? We develop a conceptual framework based on the idea that the payment instruments available to users can complement each other (eg cash and digital instruments) and act as imperfect substitutes due to their different design features.

Setting aside differences in terms of convenience, speed, financial costs and underlying technologies used,[3] we focus specifically on how payment instruments differ in terms of the involvement of intermediaries. This specific difference is inherent to the technical design of the instruments and key for AML/CFT purposes, as intermediaries could be held responsible for conducting CDD, monitoring transactions and reporting suspicious transactions. Therefore, this particular "difference by design" may prompt malicious actors to shift their activity towards the least monitored payment instruments in order to maximise the expected net return from non-compliance. As a side effect, legitimate actors may also change their choice of payment instrument to the least intermediated and monitored option if they have

[2] Cryptoassets are digital assets issued by the private sector that depend primarily on cryptography and distributed ledger technology (DLT) or similar technology (FSB (2020)). Stablecoins are a subcategory of cryptoassets that aim to maintain a stable value relative to a specified peg, eg by holding a pool of reserve assets to back their value or through algorithms to match the supply and market demand (Kosse et al (2023)). For a broader discussion on the limited effectiveness of AML/CFT frameworks, including factors that have hindered the effectiveness of the EU AML/CFT regulatory framework, see EC (2021b).

[3] See for instance ECB (2024).

concerns about their privacy or doubts about their intermediaries' ability and willingness to protect their payments data. A substantial shift towards the least monitored instruments under an AML/CFT framework would weaken its effectiveness and necessitate a regulatory response.

To better understand the dynamics between potential adjustments in the public's use of payment instruments and corresponding regulatory responses, we examine how the European Union's (EU) regulatory framework for AML/CFT evolved over time as a case study. In 2023, the European Union introduced uniform EU market rules for cryptoassets with its Markets in Crypto-Assets Regulation (MiCAR). In parallel, the European Commission has been working on a legal framework for a potential retail CBDC, ie the digital euro. The European Union therefore provides valuable insights into the entire spectrum of payment instruments. In particular, we study the evolution of the AML/CFT regulatory frameworks for cash, bank deposits and e-money; hosted and self-hosted cryptoassets (which include stablecoins); and the anticipated digital euro (which includes offline and online variants). This case study highlights how, all else being equal, payments may shift towards the instrument with the lowest probability of detecting illicit payments. We call this a "waterbed effect": if the water is pressed down in one area of a waterbed, it pops up in another. To avoid such an effect, we argue for a holistic, instrument-wide approach (lex generalis) to AML/CFT, complemented with tailored instrument-specific requirements (lex specialis) when necessary.

The remainder of this paper is organised as follows: Section 2 outlines our conceptual framework. Section 3 then examines the evolution of the EU AML/CFT regulatory framework for payments, starting with bank deposits (Section 3.1), followed by cash (Section 3.2), e-money (Section 3.3), hosted and self-hosted cryptoassets (Section 3.4) and digital euro payments, both online and offline (Section 3.5). Section 4 outlines considerations for a consistent AML/CFT approach across payment instruments and concludes with suggestions for further research.

2. Conceptual framework: AML/CFT measures and interaction with payment instrument choices

2.1 Payment instruments and the role of intermediaries

The implementation of AML/CFT measures generally relies on the existence of trusted intermediaries, or "obliged entities", that intermediate in transactions on behalf of their customers and act as gatekeepers. In this intermediary role, these entities are in a unique position to screen customers, monitor transactions and report suspicious transactions to financial intelligence units (FIUs).[4]

The presence or absence of intermediaries with these abilities is an inherent feature of the technical design of payment instruments.[5] Graph 1 provides a stylised

[4] Coelho et al (2021) investigates challenges related to supervising cryptoassets from an AML/CFT perspective.

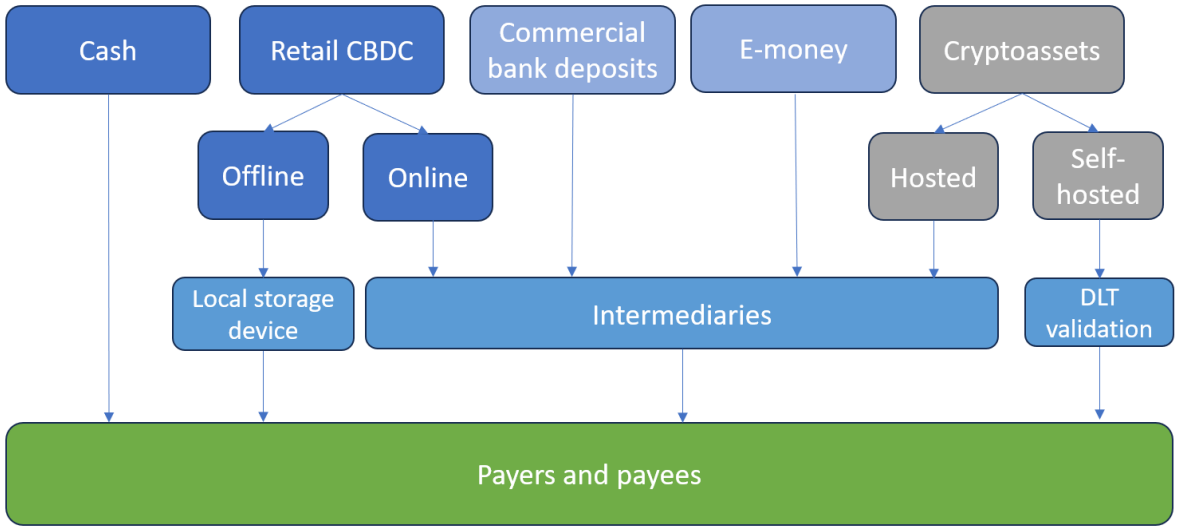
[5] This paper focuses on how payment instruments differ in terms of the involvement of intermediaries, setting aside differences in terms of convenience, speed, financial costs and underlying technologies, except in a few instances. Certain payment instruments (eg self-hosted stablecoins) may offer greater access, availability and speed compared with others in transferring illicit funds across borders.

overview of this specific difference by design across various payment instruments, including cash, retail CBDC (both online and offline), bank deposits, e-money and cryptoassets (both hosted and self-hosted). This difference provides the foundation for our analysis, as it determines the degree to which customers can be known, transactions can be monitored and AML/CFT measures can be enforced. By doing so, it forms the basis of our hypotheses on the use of different payment instruments by malicious actors and side effects on legitimate actors.

Graph 1 shows that not all payment instruments rely on intermediaries. We will discuss these in more detail in the next subsection. All else being equal, we expect malicious actors to be most inclined to use these payment instruments for their illicit activities.

Graph 1 also indicates the involvement of actors beyond intermediaries, such as issuers (top row) and payers/payees (bottom row). A question that we address later in this paper is whether such other actors could potentially also play a role in safeguarding the integrity of the financial system, especially where intermediaries do not play this role.

Types of payment instrument and the role of intermediaries Graph 1



DLT = distributed ledger technology.

Note: Cryptoassets include stablecoins. We use the definition and classification of cryptoassets and stablecoins from Kosse et al (2023). The different colour codes refer to instruments issued by central banks (dark blue), commercial banks and e-money issuers (light blue) and issuers of cryptoassets (grey).

Source: Authors' elaborations.

2.2 Malicious actors: arbitrage across payment instruments

To be effective while minimising side effects for legitimate actors, AML/CFT requirements should primarily target the behaviour of malicious actors and increase the expected costs of illicit activities. These costs depend on the expected probability of detection and the expected penalty upon detection. Due to the role that intermediaries generally play in detecting illicit transactions, the expected probability of detection may vary across the payment instruments illustrated in Graph 1. As a

result, the probability of these instruments being used for illicit purposes may also vary.

The level of involvement of intermediaries is lowest for cash, since only the payer and payee observe and validate the payment. This implies that efforts to enhance AML/CFT compliance commonly focus on the payer and payee themselves instead of on intermediaries.[6] However, assuming a self-interested malicious payer and/or payee, their incentives to self-restrict or regulate, or to report illicit transactions, would be minimal if not non-existent. Consequently, cash can be hypothesised to present the lowest probability of detection and enforcement by design. However, the physical nature of cash is likely to impose, by design, practical limitations on its usefulness for illicit purposes, which may cap the associated societal costs. Physical cash is often cumbersome and less portable than digital forms of money, making it impractical for large transactions, risky to store and transport, and time-consuming to handle.

E-money is broadly defined as an electronic store of monetary value on a technical device (which can be hardware-based or software-based) that can be widely used for making payments to entities other than the e-money issuer (ECB (2026)).[7] It involves, by design, intermediaries at the issuance stage and often also for distribution (eg through agents or e-money distributors). These intermediaries are responsible for complying with AML/CFT requirements. Likewise, for commercial bank deposits, responsibility for conducting AML/CFT checks and meeting related requirements is placed on the intermediary bank. As a result, transferring money using e-money or commercial bank deposits increases, by design, the probability of detection and enforcement relative to using cash.[8]

Transactions in cryptoassets, including stablecoins, were originally designed to replicate the properties of cash. However, their design differs from that of cash. A distinction can be made between hosted and self-hosted cryptoasset transactions. Self-hosted wallets are a type of wallet that is entirely controlled by the user, without reliance on an intermediary. Validation of self-hosted cryptoasset transactions takes place on a permissionless public blockchain, with no individual intermediary being accountable for updating accounts (see eg BIS (2025)). Individual intermediaries that could be required to act as obliged entities exist for hosted wallets. As a result, hosted crypto holdings and transactions can be subject to AML/CFT requirements. Hence, we hypothesise that, in the absence of additional or alternative AML/CFT measures, self-hosted crypto payments present the lowest probability of detection and

[6] Other options for detecting suspicious cash transactions include instances in which cash is withdrawn from an automated teller machine (ATM), exchanged for another currency or deposited with an intermediary. However, these are indirect approaches and would not provide the same degree of transaction-level detection.

[7] See Section 3.3 for the definition in the EU E-Money Directive.

[8] Note that this analysis is comparative in nature and does not directly represent the absolute probability of detection and enforcement. Intermediaries often lack a full picture of the information needed to fully understand the overall transaction network of a payment. As a result, detecting complex ML schemes can be particularly challenging for any single intermediary. Even when detection is possible, the speed of response remains a significant issue, especially as payment systems increasingly move to instantaneous 24/7 processing. Criminals may launder funds faster than AML detection and reporting processes can respond, making it difficult to trace and seize proceeds of crime. These challenges underscore the vital role of collaboration and intelligence-sharing in increasing the probability of detection and enforcement of AML measures for payments involving multiple intermediaries.

enforcement after cash.[9,10] Consequently, they may be the second most attractive payment instrument for malicious actors. Given the physical limitations associated with the use of cash, self-hosted wallets may be an even more attractive payment instrument for illicit use than cash.

When issued for general use, retail CBDCs need to be incorporated into AML/CFT frameworks. The probability of detecting illicit use of retail CBDCs will likely differ for online and offline CBDC payments. Online CBDC payments rely on validation by payment service providers (PSPs) that qualify as obliged entities under AML/CFT regulations. In contrast, offline CBDC payments likely require the CBDC to be loaded onto a local storage device, and transactions settle by linking the devices in physical proximity.[11] By design, these transactions could remain anonymous to all parties except for the payer and the payee. As a result, offline CBDC payments may be associated with a lower probability of detection than transactions conducted via commercial bank accounts, hosted crypto wallets or online CBDC, because no intermediary is involved in validating the transaction. However, offline CBDC payments will leave electronic traces. Therefore, we hypothesise that it would not present the same (lower) probability of detection as cash.[12]

2.3 Continuous dynamics between behavioural adjustment and regulatory response to avoid a waterbed effect

Our conceptual framework suggests that, all else equal, malicious actors would have the strongest incentives to use cash, self-hosted crypto and offline CBDC for illicit activities due to the absence of individually identifiable intermediaries responsible for identifying and servicing the payer and the payee and validating transactions. In contrast, transactions in commercial bank deposits, e-money, hosted cryptoassets and online CBDCs, which rely on such intermediaries, present a higher probability of detecting illicit transactions by design.

That said, the effectiveness of an AML/CFT framework and the potential for arbitrage also depend crucially on whether a payment instrument is covered by an AML/CFT framework at all, as well as on its specifics.[13] Regardless of whether a

[9] Graph 1 indicates potential anchor points for identifying users of self-hosted wallets and detecting suspicious transactions involving such wallets. These include (i) the payer and/or payee themselves and (ii) where cryptoassets are issued or redeemed (ie converted from or to fiat money using intermediaries). If criminals can spend illicit funds directly within crypto networks, they may bypass the need to convert these funds into fiat money through intermediaries.

[10] Since the history of transactions is recorded on a blockchain, it has been suggested that this information could be used to increase the effectiveness of AML/CFT frameworks (Aldasoro et al (2025)). Partly in response to this potential, there has been a rise in privacy solutions designed to obfuscate transaction details such as amounts or parties involved.

[11] Privacy in CBDC payments can be defined and achieved in different ways (DEA (2023), Tinn (2025)). Offline device-based systems are widely considered to come closest to achieving cash-like privacy (Darbha and Arora (2020), BISIH (2023)).

[12] The Eurosystem is exploring offline digital euro payments whose transaction details would remain known only to the payer and the payee (Cipollone (2025)). Offline digital euro payments are defined as digital euro payments made in physical proximity, in which authorisation and settlement take place in the local storage devices of both payer and payee (see Section 3.5).

[13] Other factors influencing the effectiveness of AML/CFT frameworks include the availability and cost of technology available to intermediaries as well as their incentives to invest in AML/CFT compliance and to perform their gatekeeper role. While this is a highly relevant topic, it falls outside the scope of this paper.

payment instrument involves an intermediary, no effort for detection would be made if it fell outside the scope of a regulatory framework, which is often the case for new emerging payment instruments.

Differences in the probability of detection – whether due to the presence or absence of intermediaries or because a payment instrument falls inside or outside the scope of a regulatory framework – can lead to arbitrage between payment instruments. This could be called a waterbed effect: if the water is pressed down in one area, it pops up in another. Over time, this dynamic weakens the overall effectiveness of AML/CFT frameworks and necessitates regulatory and supervisory intervention. This, in turn, would trigger another round of regulatory measures or updates, as is typically seen in other policy areas such as taxation or prudential banking regulation. In Section 3 we will investigate this regulatory dynamic using the European Union as a case study. The EU AML/CFT regulatory framework has been characterised by successive rounds of broadening the range of obliged entities and extending its coverage to include emerging payment instruments such as cryptoassets and CBDC.

2.4 Side effects on legitimate actors: privacy and the freedom of choice of payment instruments

Customer screening procedures, transaction monitoring and transaction reporting aim to identify illicit payments by malicious actors. To achieve this, all actors need to be subject to some degree of screening and monitoring. An unintended consequence of this is that AML/CFT measures are likely to also influence the choice of payment instruments by legitimate actors. Understanding these effects is important in designing a regulatory framework that maximises effectiveness while minimising side effects.

First, AML/CFT measures also limit the privacy of legitimate users of payment systems and instruments. Privacy is a complex concept that varies in meaning across individuals and contexts. For the purposes of this paper, we adopt the definition of informational privacy, which refers to the control or protection of personal information (Acquisti et al (2016)). As argued by Acquisti et al (2016, p 445), privacy "is not the opposite of sharing – rather, it is control over sharing". In general, sharing certain data may have potential benefits and/or costs for individuals, which may differ depending on the types of data and the individuals concerned. People value privacy for a variety of reasons. For example, payers may prefer not to have other persons (apart from the payee) observing their payments or underlying purchases, even when they are for perfectly legitimate purposes. Examples include purchases of medication, political donations or payment of services that are legal but not socially approved. Some individuals may consider their payments "nobody else's business" and reject data-sharing as a matter of principal (see Armantier et al (2025)). Moreover, people may be concerned about the use of their payment or purchasing information by third parties for commercial or political purposes. From a payee's perspective, the demand for privacy may be related to similar reasons.

While there is a public good aspect to privacy in payments (Garratt and van Oordt (2019)), unconditional and unbounded privacy is uncommon, as AML/CFT frameworks require intermediaries to record, screen and share certain data with enforcement authorities in accordance with regulatory requirements. Such data usage is permitted as a lawful basis for processing personal data, as it serves a public

purpose. From the personal perspective of legitimate users of payment instruments, this can be seen as an unintended consequence since it reduces the level of data protection that they would otherwise enjoy in the absence of the AML/CFT requirements. This creates a privacy-integrity trade-off.

To address this trade-off, AML/CFT frameworks are generally implemented alongside strong data privacy measures.[14] Banks and other regulated PSPs are generally subject to bank secrecy obligations given their role as trusted intermediaries. A strong data protection framework can help to reduce the social costs associated with the loss of privacy resulting from AML/CFT requirements. Moreover, general data protection frameworks, such as the EU General Data Protection Regulation (GDPR),[15] provide further protections for customers' data.

More generally, the extent to which AML/CFT requirements may encroach on privacy as well as the effectiveness of data protection measures will depend on the strength of the rule of law within a jurisdiction and the general public's trust in the government. The impact on privacy hinges on whether customers trust that their data will be used solely for their intended purpose (catching criminals) or fear the potential for misuse.

AML/CFT frameworks may also be perceived by legitimate actors to have undesirable consequences by limiting their freedom to choose payment instruments. This would occur when AML/CFT frameworks compel payers and payees to use certain payment instruments over others. For instance, payers and payees that particularly value privacy will be incentivised to use instruments subject to the lowest degree of monitoring. This behavioural response is similar to that of malicious actors but arises for different reasons.

3. Legal analysis: the case of the European Union

3.1 General evolution of the EU AML/CFT regulatory framework

Over the past 25 years, EU AML/CFT legislation has been developed through directives. EU directives are legal acts that set out goals that EU member states must achieve. Unlike with EU regulations, which are directly applicable across all member states without the need for national implementation, directives allow individual jurisdictions to devise their own laws to meet the goals set out in directives. As a result, directives leave a certain margin of jurisdictional discretion, which enables member states to address jurisdiction-specific issues and circumstances.

The scope of entities subjected to AML obligations in the European Union has been continuously updated over the years, taking account of evolving risks and shifts in the criminal economy across different sectors. The EU's first directive on AML, issued in 1991, was Council Directive 91/308/EEC (AMLD1). This directive laid down the three fundamental principles that continue to underpin EU AML legislation as it has been revised and expanded over time:

i. client identification;

[14] See for example Lumenalta (2025).

[15] For example, the GDPR allows intermediaries to process personal data when there is a legal obligation, such as for purposes stipulated by AML/CFT law.

ii. transaction monitoring and record-keeping; and

iii. reporting of suspicious transactions.

In 2001, Directive 2001/97/EC (AMLD2) was issued to broaden the scope of entities subjected to AML obligations beyond credit and financial institutions. In the light of the wide array of methods and practices used by money launderers to disguise illicit proceeds, AMLD2 extended AML obligations to a broader set of market participants (obliged entities) that could be exposed to AML risk. These include professionals such as accountants and lawyers, real estate agents, dealers in high-value goods and casinos.

In 2005, Directive 2005/60/EC (AMLD3) marked a paradigm shift by, among other things:

i. expanding the goals of the EU AML/CFT regulatory framework to include the "prevention of the use of the financial system for the purpose of money laundering and terrorist financing";

ii. formalising the risk-based approach as the overarching principle of AML/CFT rules and checks; and

iii. substituting client identification with fully fledged CDD and know-your-customer (KYC) obligations.

In 2015 and 2018, EU legislators enacted Directive (EU) 2015/849 (AMLD4) and Directive (EU) 2018/843 (AMLD5), respectively. AMLD4 consolidated the paradigms developed in the previous directives. It also increased the emphasis on the risk-based approach, which requires resources to be allocated based on the level of AML risk posed by specific customers, transactions or geographic areas. At the same time, AMLD4 adopted a more prescriptive approach to transaction monitoring. It outlined specific factors to consider and document during risk assessments for each customer and how these risk assessments must be kept up to date (Koster (2020)). AMLD4 also strengthened KYC obligations, particularly regarding beneficial owners and politically exposed persons. AMLD5 extended the scope of application of the AML/CFT rules to virtual currency service providers (see also Section 3.3).

Driven by large-scale cross-border ML cases[16] and substantial technology-driven developments in financial markets, EU legislators stepped up their efforts and revised the overall architecture of EU AML/CFT legislation and supervision. In 2024, the European Union issued three of the four building blocks of the so-called AML package: the AML Regulation (AMLR), the regulation establishing the Anti-Money Laundering Authority (AMLAR) and the sixth AML Directive (AMLD6). This legislation complemented the Travel Rule regulation (Regulation (EU) 2023/1113), which was issued in 2023 as the first building block of the AML package. The AML package set in motion a comprehensive overhaul of the institutional and substantive architecture of the EU AML/CFT regulatory and supervisory framework. In particular, it aimed to address the significant fragmentation across member states, which in part was the result of the reliance on directives instead of regulations (Tiemann (2024)).

[16] The Danske Bank case stands out as one of the largest ML cases in Europe in terms of the overall magnitude of ML transactions. Danske Bank, Denmark's largest bank, engaged in over EUR 200 billion (approximately USD 233 billion) in suspicious transactions through the non-resident portfolio in its Estonian branch. The case not only showed that the bank failed to maintain effective AML controls and checks; it also demonstrated the limited effectiveness of the AML regulatory and supervisory framework in addressing entities operating across borders.

EU regulatory framework for AML and CFT: evolution and key changes Graph 2

1991 Council Directive 91/308/EEC **"AMLD1"**	•Definition of key AML principles: •Client identification. •Transaction monitoring and record-keeping. •Reporting of suspicious transactions.
2001 Directive 2001/97/EC **"AMLD2"**	•Expansion of obliged entities beyond credit and financial institutions.
2005 Directive 2005/60/EC **"AMLD3"**	•Extension of goal of AML framework to include CFT. •Formalisation of risk-based approach as principle for rules and checks. •Replacement of client identification with CDD obligation.
2015 Directive (EU) 2015/849 **"AMLD4"**	•Increased emphasis on risk-based approach for AML rules and checks. •Definition of more prescriptive approach to transaction monitoring. •Strengthening of CDD obligations.
2018 Directive (EU) 2018/843 **"AMLD5"**	•Expansion of list of obliged entities with crypto exchanges and custodian wallet providers.
2023 Regulation (EU) 2023/113 **"Travel Rule"** **(First building block of AML package)**	•Expansion of application of legislation on information accompanying funds transfers to transfers of virtual assets. •Replacement of notion of "virtual currency" with "cryptoasset".
2023 Proposal COM (2023) 369 final **"DigEuro-Reg"**	•Expansion of scope of existing AML regulation to digital euro payments. •Distinction of exact treatment depending on definition and form of digital euro payments.
2024 •Regulation (EU) 2024/1624 **"AMLR"** •Regulation (EU) 2024/1620 **"AMLAR"** •Directive (EU) 2024/1640 **"AMLD6"** **(Remaining building blocks of AML package)**	•Embedding of AML requirements in directly applicable legal act. •Creation of EU-wide authority for the application and enforcement of AML rules. •Introduction of EU-wide cash payment limit. •Introduction of new sanctions compliance obligations, ad hoc measures for cryptoassets and new CDD.

Note: AML = anti-money laundering; CDD = customer due diligence; CFT = combating the financing of terrorism; KYC = know-your-customer.

Source: Authors' elaborations.

3.2 The EU AML/CFT regulatory framework for cash

The reform of the EU AML/CFT regulatory framework also introduced rules specific to cash. The AMLR lays down an EU-wide cash payment limit of EUR 10,000 for the exchange of goods and services. These transaction limits (or cash thresholds) are designed to direct all transactions above the limit towards payment instruments in which integrity prevails over privacy. This limit was introduced to mitigate risks associated with the illicit use of large cash sums. For example, if someone wishes to make a payment exceeding the cash limit, they would need to use a bank transfer or

another suitable payment instrument that involves an intermediary responsible for performing the required AML/CFT checks and monitoring.[17]

Before the introduction of EU-wide cash limits, the EU's AML/CFT regulatory approach towards cash was relatively lenient. It did not impose a uniform transaction limit for cash payments across the European Union, but did require buyers and sellers to apply KYC requirements and conduct transaction monitoring for cash payments above EUR 10,000. Member states had an option to extend these requirements to lower amounts. In addition, member states could set their own cash transaction limits in their jurisdictions.

However, the discretion granted to member states in setting cash transaction limits raises critical questions, since it could conflict with other general principles of law. For example, a question may arise regarding whether it would be permissible for a jurisdiction to set a cash limit at EUR 1, effectively phasing out cash payments in favour of payments intermediated by obliged entities. Such measures could potentially conflict with the legal tender status of euro banknotes and coins and the associated obligation to accept cash payments.[18] The European Court of Justice (ECJ) addressed this issue by considering the concept of legal tender. It concluded that member states are permitted to introduce measures that, on public interest grounds, derogate from the obligation in principle to accept euro banknotes and coins, provided that certain conditions are satisfied.[19] According to these conditions and European Central Bank (ECB) Opinion CON/2017/27 (ECB (2017c)), AML/CFT measures should generally constitute "public reasons" justifying the establishment of cash limits. Furthermore, the ECB emphasised that any limitations on the use of cash must comply with the principle of proportionality. As stated by the ECB, "when limiting the possibility, recognised by Union law, of generally discharging a payment obligation in banknotes and coins denominated in euro, Member States must ensure that any measures taken comply with the principle of proportionality, which, in particular, requires them to be appropriate for achieving the legitimate objective(s) pursued by the legislation at issue and not to go beyond what is necessary in order to achieve those objectives" (ECB (2022b)).

The AMLR not only introduces an EU-wide limit on cash transactions; it also specifies a threshold of EUR 10,000, which is considered compliant with EU law and consistent with the proportionality principle mentioned above. Still, member states may adopt lower limits after consulting the ECB. The ECB has emphasised that "the threshold for the intended prohibition of consumer-to-business and business-to-business transactions is to be set sufficiently high to avoid a factual impact leading to the abolition of euro banknotes. The de facto abolition of euro banknotes may occur, inter alia, if thresholds were set so low as to threaten the economic viability of cash as a general and widely accepted means of payment and endanger the

[17] The cash limit aims to direct transactions towards those payment instruments that enable monitoring. The cash limit does not prohibit individuals from conducting transactions above the set threshold; rather, it requires them to use a payment instrument that involves a financial intermediary.

[18] See ECB (2017a,b,c,d), ECB (2019a,b).

[19] The conditions established by the ECJ for imposing restrictions on the legal tender status of euro banknotes in particular require that the introduction of a national measure: (a) does not affect the status of legal tender; (b) does not lead to the abolition of those banknotes, in particular by calling into question the possibility, as a general rule, of discharging a payment obligation in cash; (c) is justified by reasons of public interest; (d) is appropriate for attaining the public interest objective pursued; and (e) does not go beyond what is necessary in order to achieve that objective (ECJ (2021a,b), ECJ (2022)).

functioning of the cash cycle, ultimately also affecting transactions below the threshold" (ECB (2022a,b)).

3.3 The EU AML/CFT regulatory framework for e-money

Article 2(2) of Directive 2009/110/EC (E-Money Directive) defines e-money as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions […] and which is accepted by a natural or legal person other than the electronic money issuer". Entities that issue and/or distribute e-money are classified as obliged entities under the EU AML/CFT regulatory framework and are thus required to fulfil all relevant requirements.

While the anonymity associated with certain e-money products exposes them to ML/TF risks, the AMLR acknowledges that the e-money sector is heterogeneous and that not all e-money products carry the same level of ML/TF risk. For instance, prepaid gift cards or vouchers used for low-value payments may present a comparatively low risk of ML/TF. To ensure that regulatory requirements remain proportionate to the actual risk and do not unduly hinder the functioning of the e-money sector, the AMLR allows for an exemption of certain e-money products from specific CDD measures provided the risks are demonstrated to be low and strict conditions are met. More specifically, supervisors may exempt obliged entities from applying, in full or in part, CDD measures with respect to e-money on the basis of a proven low risk posed by the nature of the product where all of the following risk-mitigating conditions are met:

i. the payment instrument is not reloadable and the amount of e-money stored does not exceed EUR 150 or the equivalent in national currency;

ii. the payment instrument is used exclusively to purchase goods or services provided by the issuer or within a network of service providers;

iii. the payment instrument is not linked to a payment account and it does not permit any stored amount to be exchanged for cash or cryptoassets; and

iv. the issuer carries out sufficient monitoring of transactions or business relationship to enable the detection of unusual or suspicious transactions.

3.4 The EU AML/CFT regulatory framework for crypto

The growing use of cryptoassets has prompted international, European and national policymakers to issue numerous warnings concerning the AML/CFT risks associated with crypto (FATF (2014), ESMA et al (2018)). In response, EU lawmakers enacted AMLD5 in 2018 to amend AMLD4. AMLD5 introduced, among other things, a definition of virtual currency and broadened the list of obliged entities to include crypto exchanges and custodian wallet providers.

However, in 2024, the EU AML/CFT regulatory framework underwent a complete overhaul, both institutionally and substantively. One of the motivations for the reform was the increasing number of suspicious transactions channelled towards innovative, unregulated payment instruments. The reform therefore aimed to adapt the AML/CFT regulatory framework to new and emerging challenges stemming from technological innovation, in particular in relation to virtual currencies and cryptoassets in general

(EC (2021a)). The goal was to create a comprehensive and consistent regulatory and supervisory framework, with a package of measures designed to align with technological developments in finance.

The reform introduced a new European Anti-Money Laundering Authority (AMLA), headquartered in Frankfurt, for the application and enforcement of EU AML rules. The AMLA directly supervises cross-border high-risk obliged entities. Moreover, it facilitates cooperation between European FIUs, eg by creating standards for reporting and data exchange and a central online system.

The reform also established a new regulation (AMLR) that incorporates all AML/CFT requirements into a directly applicable legal act to address the regulatory fragmentation resulting from national implementation of the earlier directives. The AMLR also replaces the concept of "virtual currency" used in AMLD5 with the term "cryptoasset", defined in MiCAR as "a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".

In Section 2.2, we argued that the probability of detection and enforcement differs for hosted and self-hosted cryptoasset wallets. These instruments are treated differently under the EU AML/CFT regulatory framework.

Hosted cryptoasset wallets

The EU AML/CFT reform extended the regulatory scope from crypto exchanges and custodial wallets to encompass all "cryptoasset service providers" (CASPs) that are involved with cryptoassets.[20] This extension was driven by the aim to create future-proof legislation that would be able to keep pace with technological developments and is founded on an incentive-based approach. The reform also defines the terms "cryptoasset" and "distributed ledger technology" as broadly as possible in order to capture all types of both. As a result, transaction monitoring rules now also apply to hosted cryptoassets and are to be implemented by CASPs or other obliged entities that may be involved in a cryptoasset transaction.

The AMLR regards the pseudonymous nature of cryptoassets as a threat to the integrity of the financial system due to their potential misuse for criminal purposes. Pseudonymous cryptoasset wallets obstruct or complicate the traceability of cryptoasset transfers. Such wallets also hinder the identification of linked and suspicious transactions and the application of an adequate level of CDD. Therefore, the AMLR prohibits the provision and custody of hosted cryptoasset wallets, as well as any wallets, that allow for the anonymisation of the customer account holder.[21] It also bans wallets that allow for the anonymisation or obfuscation of transactions by

[20] The regulatory requirements do not apply to providers of hardware and software if they do not have access to or control over cryptoasset wallets. Moreover, under MiCAR, issuers of asset-referenced tokens (ARTs) could be either credit institutions or ART issuers authorised in accordance with an ad hoc license. If the issuer is a credit institution, AML rules will apply to this entity as credit institutions are considered obliged entities for AML purposes. If the issuer is an ART issuer, however, the AML framework does not apply since the AMLR does not mention ART issuers or offerors as obliged entities. Only if ART issuers also decide to provide services in relation to their ARTs, ie obtain a CASP license, will they be classified as obliged entities under the AML framework.

[21] Likewise, the AMLR prohibits credit institutions, financial institutions and CASPs from keeping anonymous bank and payment accounts, anonymous passbooks, anonymous safe deposit boxes or anonymous cryptoasset accounts (see Article 79).

CASPs, including through anonymity-enhancing coins, such as cryptoassets designed to anonymise transfer information, whether systematically or optionally.

To enhance the effectiveness of the AML/CFT regulatory framework, Regulation (EU) 2023/1113 (the Travel Rule regulation) expanded the scope of legislation on the information accompanying transfers of funds. Initially, legislation was limited to transfers involving banknotes and coins, commercial bank money and electronic money (funds), but it now also applies to transfers of virtual assets.

Self-hosted cryptoasset wallets

Since transaction monitoring relies on AML/CFT checks and activities performed by intermediaries, the AMLR takes a strict stance towards self-hosted cryptoasset wallets. Transactions with self-hosted cryptoasset wallets are not subject to CCD and transaction monitoring unless they involve a CASP at one end of the transaction. To mitigate risks from transactions with self-hosted cryptoasset wallets, the AMLR requires CASPs to identify and assess the risk of ML/TF associated with cryptoasset transfers to or from self-hosted wallets and to adopt risk-mitigating measures that are commensurate with the risks identified.

Overall, a noticeable feature is that the regulatory approach for self-hosted cryptoasset wallets differs from that applied to cash (Section 3.2). In both cases, there is no intermediary that is well placed to act as an obliged entity. For cash, the main regulatory response has been the introduction of transaction limits, while similar limits have not been introduced for self-hosted cryptoassets. Following the discussion in Section 2, this may provide an incentive for malicious actors to shift from cash to self-hosted cryptoasset wallets.

3.5 The AML/CFT regulatory framework for retail CBDC according to the proposal for a regulation on the establishment of the digital euro

In June 2023, the European Commission published the so-called digital euro package. This package included, among other legislative initiatives, a "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro" (DigEuro-Reg). The digital euro is an example of a retail CBDC and aims to complement euro banknotes and coins (cash) rather than replacing them. As such, it fits within our conceptual framework of payment instruments discussed in Section 2.

The DigEuro-Reg states that digital euro payments are, in principle, subject to EU AML/CFT legislation. However, there are several outstanding legal and regulatory questions. One of the most pressing policy issues relates to the consistency between the DigEuro-Reg and existing financial regulatory frameworks, including current AML/CFT legislation (EC (2023)). The application of the AML/CFT regulatory framework to digital euro payments hinges on the definition and form of digital euro payments. The DigEuro-Reg defines a digital euro payment as "an act, initiated by a payer or on his or her behalf, or by the payee, of placing, transferring or withdrawing digital euro, irrespective of any underlying obligations between the payer and the payee". It also distinguishes between online and offline digital euro payments. Online digital euro payments are settled (ie are validated and recorded) in the digital euro settlement infrastructure adopted by the Eurosystem. Offline digital euro payments are defined as digital euro payments made in physical proximity, where authorisation and settlement take place in the local storage devices (secure hardware) of both payer and payee.

The distinction between online and offline digital euro payments is essential for the appropriate application of the AML/CFT regulatory framework, especially in the light of the risk-based approach that underpins it. While online digital euro payments will be settled in accordance with the rules set out by the Eurosystem, the settlement of offline digital euro payments would rely on local storage devices and not involve an intermediary. Consequently, and as discussed in Section 2, offline digital euro payments could, all else being equal, pose greater AML/CFT risks compared with online digital euro payments or payments made using commercial bank deposits or hosted cryptoasset wallets. In addition, offline digital euro payments could pose greater AML/CFT risks than cash payments, which are constrained by the inherent limited portability of cash. Therefore, in order to ensure an effective application of AML/CFT requirements to the digital euro, it is vital to consider the different AML/CFT risk profiles associated with online and offline digital euro payments.

Online digital euro payments

Online digital euro payments between a payer and a payee are settled with the operational intervention of a PSP. This PSP would be in the position and obliged to conduct checks and fulfil the obligations established in the EU AML/CFT regulatory framework. This means that PSPs would act as obliged entities and be responsible for performing the appropriate level of CDD, reporting suspicious transactions, storing and processing personal data for AML/CFT purposes, and sharing information with competent authorities (ECB (2020)). As with other intermediated payments, PSPs would be required to apply CDD measures and fulfil obligations using a risk-based approach.

Offline digital euro payments

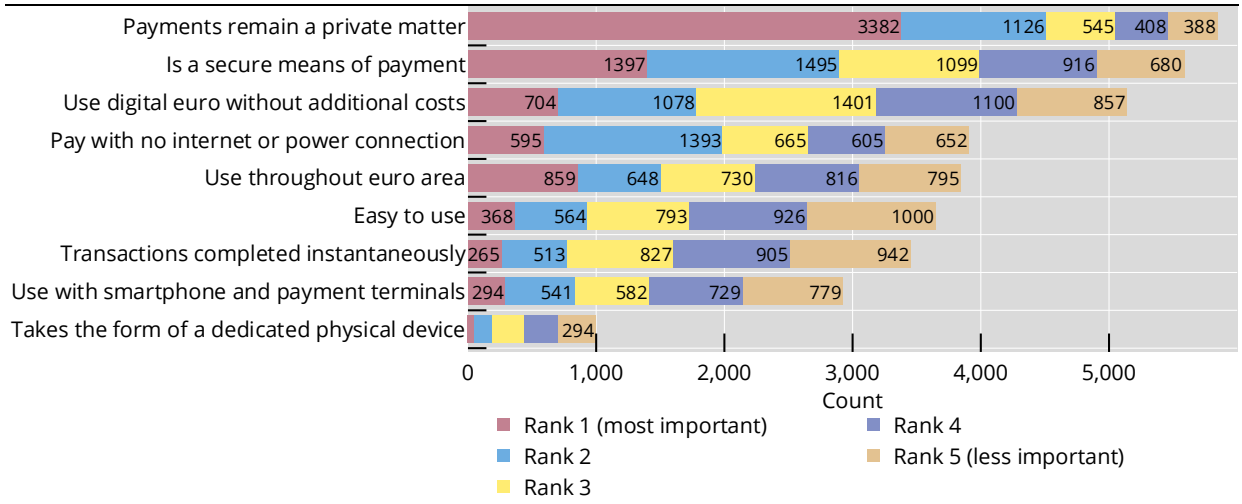
Offline digital euro payments provide users with a degree of privacy regarding their transactions and holdings, as transactions would be conducted person-to-person without the involvement of an intermediary. Consultations conducted by the ECB and the European Commission have shown that European citizens have a clear preference for a high level of privacy and that they favour privacy-enhancing features such as the ability to conceal the identity of the payer and the payee (ECB (2020), ECB (2021), EC (2023)) (see Graph 3). However, in the effort to strike the right balance between privacy and integrity, the ECB clarified that "full anonymity is not considered a viable option from a public policy perspective" (ECB (2022c)). Therefore, the DigEuro-Reg provides a bespoke AML/CFT framework for offline digital euro transactions.

According to the DigEuro-Reg's provisions for offline transactions, neither the ECB, national central banks nor PSPs will retain transaction data related to offline transactions. PSPs will only have access to funding and defunding data, which should be transmitted, upon request, to FIUs and other competent authorities when users are suspected of ML/TF.[22] Such funding and defunding data can only include (i) the amount funded or defunded; (ii) the identifier of the local storage device for the offline digital euro payment; (iii) the date and time of the funding and defunding transaction; and (iv) the account numbers used for funding and defunding.

[22] In the DigEuro-Reg, funding means "the process whereby a digital euro user acquires digital euros, in exchange for either cash or other funds, creating a direct liability of the European Central Bank or a national central bank towards that digital euro user" and defunding means "the process whereby a digital euro user exchanges digital euro with cash or other funds".

Preference for digital euro features

Graph 3



"Payments remain a private matter" = I want my payments to remain a private matter; "is a secure means of payment" = I want it to be a secure means of payment; "use digital euro without additional costs" = I want to use a digital euro without having to pay additional costs; "pay with no internet or power connection" = I want to be able to pay even when there is no internet or power connection; "use throughout euro area" = I want to be able to use it throughout the euro area; "easy to use" = I want it to be easy to use; "transactions completed instantaneously" = I want my transactions to be completed instantaneously; "use with smartphone and payment terminals" = I want to be able to use it with my smartphone and at payment terminals; "takes the form of a dedicated physical device" = I want it to take the form of a dedicated physical device.

Number of respondents not shown for the option "takes the form of a dedicated physical device": 47 (rank 1), 139 (rank 2), 254 (rank 3), 263 (rank 4).

Source: ECB (2021).

Considering the characteristics and specific ML/TF risks associated with offline digital euro payments, the DigEuro-Reg empowers the European Commission to set transaction and holding limits for the offline digital euro. Setting such limits involves balancing the need to prevent ML/TF with the goal of facilitating the use of the offline digital euro as a means of payment.

In this context, the AML/CFT framework embedded in the DigEuro-Reg constitutes a "lex specialis" (ie special legal framework that serves as an exception) in comparison with the general AML/CFT framework, ie the "lex generalis". This approach was taken to find the appropriate balance in the privacy-integrity trade-off. Furthermore, since this special AML/CFT framework for offline transactions will be applied without the operational intervention of PSPs, there is a shift in responsibility from third parties to the payer and the payee. Similar to cash transactions, it becomes the responsibility of the users to comply with the transaction limits set for offline digital euro payments.

Our case study highlights how the EU AML/CFT regulatory framework evolved over time to address ML/TF risks posed by existing and emerging payment instruments. Still, the approaches differ by instrument (see Table 1). Taken at face value, and without additional measures, these differences would provide an incentive for malicious actors to use self-hosted cryptoasset wallets for their illicit activities. This adds to the heightened integrity risks related to the use of cryptoassets (BIS (2025)).

EU AML/CFT regulatory approaches for payment instruments for which reliance on intermediaries as obliged entities is not a design feature Table 1

Instrument	AML/CFT measures
Cash	EUR 10,000 cash transaction limit.
Self-hosted cryptoassets	No transaction or holding limits. CASPs, if involved in one end of the transaction, should identify and assess the risk of ML/TF associated with transfers directed to and originating from a self-hosted wallet.
Offline digital euro	DigEuro-Reg empowers the European Commission to set offline digital euro transaction and holding limits.

Sources: Authors' elaboration.

4. Considerations for a consistent AML/CFT regulatory approach across payment instruments

This paper examined how payment instruments vary in design, giving rise to different ML/TF risk profiles. There is a key distinction between:

i. instruments that involve intermediaries subject to AML/CFT requirements related to screening customers, monitoring transactions and reporting suspicious transactions (ie e-money, commercial bank deposits, online retail CBDC and hosted cryptoasset wallets); and

ii. those that do not involve intermediaries (ie cash, offline retail CBDC and self-hosted cryptoasset wallets).

We advocate a consistent regulatory approach that considers the similarities and differences in design across payment instruments, an approach similar to the Aristotelian principle of justice: treating equals equally and unequals unequally, with a crucial emphasis on proportionality.

Our approach combines the need for a consistent regulatory approach (lex generalis) with specific provisions (lex specialis) tailored to the unique features of each instrument. The lex generalis would establish a consistent approach for instruments with intermediaries and those without, respectively, while the lex specialis would address individual instrument characteristics. By design, it is natural that different payment instruments are subject to different requirements. At the same time, if not well calibrated, such differences in requirements may give rise to arbitrage and a waterbed effect and weaken the effectiveness of regulatory frameworks. In the end, it is a matter of finding the right balance between lex specialis and lex generalis.

Our approach suggests applying uniform AML/CFT regulatory requirements across all payment instruments involving individually identifiable intermediaries. Commercial banks, e-money institutions, PSPs that intermediate online CBDC and wallet service providers alike should be subject to the same set of regulatory requirements regarding CDD, transaction monitoring and the reporting of suspicious

transactions. Similarly, the approach suggests harmonising privacy and data protection requirements across these entities to address the privacy-integrity trade-off consistently.

Several conceivable regulatory options can apply consistently across payment instruments without intermediaries. First, for all instruments in this group, AML/CFT frameworks can leverage touch points, or entry/exit points, where illicit funds interact with those intermediaries in the first group of instruments, while acknowledging that this is a partial solution as it only allows for the monitoring of incoming and outgoing transactions.[23] Examples of such touch points include cash withdrawals or deposits with commercial banks and the conversion between self-hosted stablecoins and commercial bank deposits or e-money.

Next, AML/CFT frameworks could involve entities/actors other than intermediaries for each instrument. The clearest example is cash, for which transaction limits have been imposed on payers and payees. One option involves imposing a uniform transaction limit across instruments to mitigate the waterbed effect, although enforceability challenges vary by instrument.[24] For example, transaction limits can be programmed into the design of an offline CBDC and protocols and/or smart contracts on DLTs, ensuring compliance by default. While applying transaction limits to self-hosted cryptoassets is technically feasible, enforcing such requirements would likely prove challenging. Still, enforcing transaction limits for cash payments presents even greater challenges, primarily due to their anonymous and non-electronic nature.

A stronger emphasis could be placed on the responsibilities of and enforcement by the issuers of payment instruments. As issuers of banknotes, central banks have a role to play, as illustrated by the decision of the Eurosystem to discontinue the issuance of EUR 500 notes in 2019 to address AML/CFT concerns. Similarly, stablecoin issuers have complied with requests from authorities to freeze the coins in self-hosted wallets associated with illicit activities.

Another complementary approach for addressing the challenges associated with payment instruments without intermediaries could involve increasing the costs associated with non-compliance for private-sector issuers, payers, payees and entities that provide services or a platform for settling cryptoasset transactions, especially those engaged in professional activities.[25] These exemplify the possible roles of lex specialis in addressing individual instrument characteristics.

In addition, policy objectives beyond AML/CFT can intersect with AML/CFT regulatory requirements. For example, the legal tender status of central bank-issued instruments (ie cash and CBDC) may interact – or potentially conflict – with AML/CFT requirements. In addition, CBDCs may be subject to a transaction limit from the financial stability perspective, eg to mitigate risks of disintermediation or digital bank runs, and such limits may differ from those set for AML/CFT purposes.

[23] For stablecoins, as proposed by Aldasoro et al (2025), transaction histories on public blockchains could be used to identify potentially malicious users based on deny- or allow-listed wallets (since the underlying identities of the users are hidden). These public databases inherently include transaction amounts, although strategies like "smurfing", or using many small transactions to evade detection, must also be taken into account as a complicating factor.

[24] Note that a transaction limit harmonised across payment instruments may vary across jurisdictions, reflecting differing ML/TF risks and policy preferences.

[25] This approach aligns with approaches taken by financial supervisors in incentivising banks to step up their efforts as obliged entities (see Introduction and Section 3.1).

Lastly, an AML/CFT framework in line with our approach could incorporate general principles with overarching high-level definitions of the entities or activities subject to regulation. This would help the framework to adapt to the emergence of innovative instruments, which – provided they fulfil a payment function by design – could be included within the regulatory framework by default. This approach could help to hinder the cycle in which innovation aims to circumvent existing rules, prompting reactive and piecemeal adjustments to the regulatory framework. A consistent and forward-looking approach could channel innovation towards a more productive direction that is not motivated by regulatory arbitrage, but rather by better outcomes for end users.

This paper introduced a high-level conceptual framework and examined the EU AML/CFT regulatory framework as a case study. There are numerous avenues for future research. First, studying the development of AML/CFT frameworks in other jurisdictions could provide valuable insights by comparing their experiences with those in the EU. Second, and relatedly, examining the similarities and differences in AML/CFT frameworks across jurisdictions would also be useful, in particular in understanding the potential for geographical arbitrage of ML/TF activities. Third, an empirical analysis of the waterbed effect could offer important findings that can be used to test our conceptual framework, although challenges related to data collection and interpretation will likely arise. Further research could also focus on recent technologies, examining those that may be exploited by malicious actors on one hand and those that could assist obliged entities in effectively monitoring and identifying suspicious transactions on the other.

References

Acquisti, A, C Taylor and L Wagman (2016): "The economics of privacy", Journal of Economic Literature, vol 54, no 2, June.

Aldasoro, I, J Frost, S H Lim, F Perez-Cruz and H S Shin (2025): "An approach to anti-money laundering compliance for cryptoassets", BIS Bulletin, no 111, August.

Armantier, O, S Doerr, J Frost, A Fuster and K Shue (2025): "Nothing to hide? Gender and age differences in willingness to share data", BIS Working Papers, no 1187, October.

Bank for International Settlements (BIS) (2025): "The next-generation monetary and financial system", Annual Economic Report 2025, Chapter III, June.

BIS Innovation Hub (BISIH) (2023): Project Tourbillon demonstrates cash-like anonymity for retail CBDC, November.

Centre for European Policy Studies (CEPS) and European Credit Research Institute (ECRI) (2021): Anti-money laundering in the EU: Time to get serious, January.

Cipollone, P (2025): "Digital euro: The future of money", April.

Coelho, R, J Fishman and D Garcia Ocampo (2021): "Supervising cryptoassets for anti-money laundering", FSI Insights on policy implementation, no 31, April.

Darbha, S and R Arora (2020): "Privacy in CBDC technology", Bank of Canada Staff Analytical Note, no 2020-9, June.

Digital Euro Association (DEA) (2023): Privacy and central bank digital currencies, January.

European Central Bank (ECB) (2017a): "Opinion of the European Central Bank of 22 May 2017 on limitations to cash payments in Portugal", CON/2017/18, May.

——— (2017b): "Opinion of the European Central Bank of 30 May 2017 on the limitation of cash payments", CON/2017/20, May.

——— (2017c): "Opinion of the European Central Bank of 11 July 2017 on limitation of cash payments", CON/2017/27, July.

——— (2017d): "Opinion of the European Central Bank of 6 October 2017 on limitations to cash payments", CON/2017/40, October.

——— (2019a): "Opinion of the European Central Bank of 1 February 2019 on limitations to cash payments", CON/2019/4, February.

——— (2019b): "Opinion of the European Central Bank of 30 December 2019 on limitations to cash payments", CON/2019/46, December.

——— (2020): Report on a digital euro, October.

——— (2021): Eurosystem report on the public consultation on a digital euro, April.

——— (2022a): "Opinion of the European Central Bank of 16 February 2022 on a proposal for a directive and a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing", CON/2022/5, February.

——— (2022b): "Opinion of the European Central Bank of 15 March 2022 on limitations to cash payments", CON/2022/9, March.

——— (2022c): Progress on the investigation phase of a digital euro, September.

——— (2024): Study on the payment attitudes of consumers in the euro area (SPACE) – 2024, December.

——— (2026): Electronic money, data.ecb.europa.eu/methodology/electronic-money, accessed on 16 January 2026.

European Commission (EC) (2021a): "Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules", 20 July.

——— (2021b): "Introduction of cash limits", Commission Staff Working Document: Impact Assessment accompanying the anti-money laundering package, SWD(2021) 190 final, July, Annex 9.

——— (2023): Commission Staff Working Document: Impact Assessment Report accompanying the documents "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro" and "Proposal for a Regulation of the European Parliament and of the Council on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro and amending Regulation (EU) 2021/1230 of the European Parliament and the Council" and "Proposal for a Regulation of the European Parliament and of the Council on the legal tender of euro banknotes and coins", SWD(2023) 233 final, June.

European Court of Justice (ECJ) (2021a): Joined cases C-422/19 and C-423/19, January.

——— (2021b): Case C-544/19, October.

——— (2022): Case C-184/20, August.

European Securities and Markets Authority (ESMA), European Banking Authority (EBA) and European Insurance and Occupational Pensions Authority (EIOPA) (2018): "Warning: ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies", press release, 12 February.

Financial Action Task Force (FATF) (2014): Virtual currencies: key definitions and potential AML/CFT risks, June.

Financial Stability Board (FSB) (2020): Regulation, supervision and oversight of "global stablecoin" arrangements – final report, October.

Garratt, R and M van Oordt (2019): "Privacy as a public good: a case for electronic cash", Bank of Canada Staff Working Paper, no 2019-24, July.

Kosse, A, M Glowka, I Mattei and T Rice (2023): "Will the real stablecoin please stand up?", BIS Papers, no 141, November.

Koster, H (2020): "Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework", Journal of Money Laundering Control, vol 23 no 2, March.

Lumenalta (2025): "Data privacy in banking", 9 February, lumenalta.com/insights/data-privacy-in-banking, accessed on 16 January 2026.

Rice, T, G von Peter and C Boar (2020): "On the global retreat of correspondent banks", BIS Quarterly Review, March.

Tiemann, M (2024): "A commentary on the EU money laundering reform in light of the subsidiarity principle", Journal of Financial Regulation and Compliance, vol 32, no 3, May.

Tinn K (2025): "A theory model of digital currency with asymmetric privacy", Management Science, August.

LEGISLATION REFERENCES

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering ("AMLD1").

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering ("AMLD2").

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing ("AMLD3").

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC ("AMLD4").

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU ("AMLD5").

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 ("AMLD6").

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("AMLR").

Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 ("AMLAR").

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 ("Travel Rule").

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ("MiCAR").

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