Journal of Banking Regulation
https://doi.org/10.1057/s41261-024-00241-2

ORIGINAL ARTICLE

Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture

Giulio Soana[1,2] · **Thomaz de Arruda**[2,3]

Accepted: 21 February 2024

Abstract
In an increasingly digitised world, and within the new reality of digital finance, a fully digitised public currency seems to be a natural step. To this end, central banks have been testing the possibility to issue a digital form of the traditional *fiat* currency (so-called Central Bank Digital Currency-CBDC). As these projects steadily progress, and in some cases, reach the implementation phase, a myriad of questions, from legal to macroeconomic, arise. This paper aims to focus, in particular, on two complementary and co-related aspects involving CBCDs: (i) how can the full digitalisation and centralisation of the transaction ledger be combined with privacy and (ii) to what extent CBDCs affect the allocation of burden and the responsibility over supervision of retail transactions. Eminently, the use of cash ensures a form of default privacy that protects the individual against State and private intrusion. While this privacy has caused concern, due to its criminogenic potential, and has been consequently limited by anti-money laundering (AML) regulations, the remaining cone of shadow cash guarantees is a crucial limit to control. In the context of a shifting financial system, undergoing deep transformation due to increasing datafication and decentralisation of the market, a new governance of financial supervision and record-keeping—up to now based on a unique and centralised ledger—is crucial to redefine the trade-off between financial integrity and privacy. This article will examine the origins and characteristics of CBDCs, to then analyse how the trade-off between control and privacy is set to reshape this new architecture.

✉ Giulio Soana
giulio.soana@kuleuven.be

[1] KU Leuven/LUISS, Rome, Italy

[2] EBI Young Researchers Group, Frankfurt, Germany

[3] Bocconi University, Milan, Italy

Published online: 20 March 2024

CBDC: an introduction

Over the last few years, authorities and academics have been analysing the economic and financial effects stemming from the potential implementation of Central Bank Digital Currencies (CBDCs)[1] by national governments.[2] To that extent, even though much attention has been brought forward in terms of macroeconomic consequences of such undertaking, research has been scarce in the field of financial integrity. Indeed, as different CBDC designs start taking shape, each of them bears direct implications to the regulatory treatment of underlying anti-money laundering, combating the financing of terrorism (AML/CFT) and privacy considerations.

This study will focus on the CBDC currently developing within the European Union (EU), where also the regulatory regimes governing digital privacy and digital finance in general—especially with the adoption of the MiCA,[3] Pilot Regime[4] and DORA[5] regulations—lead to a highly intricate legal scheme, aiming to safeguard distinct (and, in some cases, conflicting) interests, which need to coexist with equally complex AML/CFT frameworks, including under the auspice of a new centralised European supervisor for AML/CFT (the so-called Anti-Money Laundering Authority, AMLA).[6]

The purpose of this paper is not to provide a guideline on the financial integrity standards that should be tailored to CBDCs architectures, but rather to analyse what the model under discussion in the EU may entail to stakeholders and society. More importantly, depending on the way they are ultimately structured, the advent of CBDCs in Europe may radically change the allocation of burden and the responsibility over the supervision of retail transactions, from an AML/CFT standpoint. This implies recalibrating the traditional roles played by the European Central Bank (ECB), European Supervisory Authorities (ESAs), national competent authorities (NCAs), financial intelligence units (FIUs) and financial intermediaries on securing financial integrity, in a shift from the paradigm that has marked financial integrity regulation since its creation.

Challenges posed by decentralised finance

Understanding how financial supervision should adapt to the CBDC phenomenon should not prescind from a previous analysis on how the pillars that support the financial system have been changing, and in account to which larger set of factors. Indeed, we may argue that CBDCs are merely a reflection of certain patterns of technological evolution that have been disrupting the dynamics of the financial system and inserting new elements into its playing field. As data become increasingly important and lead the global economy to what some call the fourth industrial revolution,[7] the financial sector itself is struggling to deal with a new kind of economy, based primarily on datafication[8] and decentralisation.[9] Accordingly, datafication refers to the process of attributing economic value to data, leading to the possibility of generating resources by transacting on data. Moreover, it relates to both Moore's and Kryder's laws,[10] which respectively sustain the assumptions that the amount of data processing power and data storage capacity grows exponentially, leading to ever-lower costs for both. As production costs of network components gain more efficiency, hardware becomes increasingly virtualised, thus leading

[1] IMF Staff defined CBDC as "a new form of money issued digitally by the central bank and intended to serve as legal tender". See IMF Staff, "Casting Light on Central Bank Digital Currency, IMF", SDN/18/08.

[2] To date, the most advanced retail CBDC projects in place are the DCash in Eastern Caribbean and the Sand Dollar in the Bahamas, asides from the Chinese E-Yuan. However, several projects are already in an advanced phase, such as the Bakong Project (Cambodia), DC/EP (China), E-hryvnia (Ukraine), E-peso (Uruguay), Dinero Electrónico (Ecuador), E-Krona (Sweden), E-won (Korea) and the Digital Lira (Turkey). For wholesale CBDCs, mature initiatives include the Inthanon-LionRock project (Hong Kong SAR and Thailand), Ubin (Singapore), Jasper (Canada), TBC (UK and Northern Ireland), Jura (France and Switzerland), Khokha (South Africa), Stella (EU and Japan), Aber (United Arab Emirates). Many other jurisdictions and private players are also sponsoring significant initiatives in the field.

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

[4] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

[5] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

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

[7] R. Morrar—H. Arman—S. Mousa, "The fourth industrial revolution (Industry 4.0): A social innovation perspective", *Technology Innovation Management Review,* Vol. 7(11), 12-20, 2017.

[8] See, among others, M. Zachariadis -P. Ozcan, "The API Economy and Digital Transformation in Financial Services: The case of Open Banking". SWIFT Institute Working Paper 2016-001, 2017.

[9] See F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets", *Federal Reserve Bank of St. Louis*, Vol. 103(2), 153-174, 2021. See also D. Zetzsche -W. Arner—R. Buckley—"Decentralized Finance", University of Hong Kong Faculty of Law Research Paper No. 2020/010, 2020.

[10] See G. Moore GE, "Progress in digital integrated electronics", *Proceedings of the IEEE electron devices meeting*, Vol 21, 1975, 21–25; C. Walter, "Kryder's law", *Scientific American, 293* 2005, 32-3.

to a decentralisation of servers and hosts that run software on a non-local basis and favour architectures which are service-oriented.[11]

Datafication and decentralisation form the core of what may be referred to as decentralised finance (DeFi),[12] which comprises a number of technologies spanning from artificial intelligence (AI), distributed ledgers, cloud services and big data. These, in turn, lead to crypto-assets and the multitude of services and products that inhabit the constantly evolving environment of FinTech and crypto-assets. Driven by such rapid technological developments, financial services have been subverting traditional banking models with disruptive approaches to finance.

At the heart of the concept of DeFi lies a wide set of challenges that are yet to be addressed by players, consumers and regulators. The terrain is far from yielding its full potential and the market is still likely to experience major shifts and accommodations before maturing into a more stable scenario. In this sense, DeFi sheds light upon issues now faced by the financial system, such as the role of intermediaries, trust and confidence on technology infrastructures, data privacy and digital sovereignty, competition among incumbents and newcomers (with the issue of hyper-concentration in BigTech firms), innovation and the role of the State. We believe that CBDCs are part of this trend and should be analysed under the optics of both datafication and decentralisation. Particularly when it comes to understanding the role of financial intermediaries in this shifting scenario, it is interesting to observe that CBDCs are not the cause of the need to rethink distribution of traditional competences, but rather a consequence of a redistribution of powers that has already been operating from within the financial system.

For financial integrity, to perceive the shift of power dynamics in the market and to understand how different players interact with each other, how new service-chains function, potentially expanding the role of public institutions, notably of the central banks and FIUs, and where the higher risks actually reside, might be the biggest challenge in the hands of legislators and regulators. It is thus necessary to consider the sensibility of debates revolving around centralisation and decentralisation, especially when data protection, cybersecurity and digital privacy are at stake and intertwined with the sensitive topic of government control that arises from the nationalisation of core infrastructures. In a world where data gradually become the most valuable asset to be traded, financial intelligence is certainly a type of information that should be treated with extreme caution and prudence.

The analysis of CBDCs from an AML/CFT standpoint requires an understanding of how these infrastructures will be designed and implemented. AML/CFT policies will be facing a new architecture and nexus of economic market players, which are raising unexplored challenges in terms of management of AML/CFT risks. Although scholars and regulators may sustain that certain models are inherently superior for their operational advantages[13] or even for the purposes of safeguarding against money laundering and other illicit uses,[14] ultimately, there will always be colliding principles to be balanced by competent authorities, such as the protection of privacy, the maintenance of financial integrity and the stability of the system, only to name a few. The CBDC design ultimately adopted in the Union will, therefore, be a consequence of the weight and value attributed to a certain regulatory objective, in detriment of others. In this sense, this paper sustains that an AML/CFT regulation should not advocate for a particular design, but rather understand what each regulatory choice entails in terms of distribution of competences between stakeholders, to achieve the highest standards of financial integrity while preserving the desired level of privacy.

[11] D.Zetzsche -D. Arner—R. Buckley, "Decentralized Finance (DeFi)", *Journal of Financial Regulation,* Vol. 6, 2020, 172-203.

[12] The term decentralised finance (DeFi) refers to an open, permissionless and highly interoperable protocol stack built on blockchain-based infrastructure and public smart contract platforms. More broadly, the term has been used to refer to the different disruptive technology-based models for financial services, heavily underpinned by their decentralised infrastructure. DeFi enables financial services to be carried out in a more open and transparent manner, relying on open protocols and decentralised applications (DApps), whereby agreements are enforced by code, transactions are executed in a secure and verifiable way and legitimate state changes persist on a public blockchain. This may create different set of architectures characterised by highly interoperable financial systems, with little to low need for custodians, central clearing houses or escrow services, i.e. traditional intermediaries and counterparties.

DeFi uses a multi-layered architecture, where every layer serves a distinct purpose. The layers build on each other and create an open and highly composable infrastructure that allows stakeholders to build on, rehash, or use other parts of the stack. It is also crucial to understand that these layers are hierarchical: they are only as secure as the layers below. A possible conceptual framework for understanding protocol layers in greater detail was proposed by F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets", cit., and divides layers between settlement, asset, protocol, applications and aggregation functions. Other categorisation classifies layers into public base layer with digitally native tokens, software protocols that codify agreed rules, smart contracts that implement financial logic and stablecoins backed by reserves held at banks. See N. Carter -L. Jeng, DeFi Protocol Risks: The Paradox of DeFi, in B. Coen—D. Maurice (eds.), *Regtech, Suptech and Beyond: Innovation and Technology in Financial Services*, RiskBooks.2021.

[13] As recently recognised by the IMF staff, there is "no universal case for CBDC adoption yet". IMF Staff, "Digital Money Across Borders: Macro-Financial Implications". IMF, 2020. See also IMF Staff, "Casting Light on Central Bank Digital Currency, IMF", SDN/18/08.

[14] A. Berentsen -F. Schär, "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies", *Federal Reserve Bank of St. Louis*, Vol. 100, No. 2, 2018.

A brief history: the CBDC revolution on financial integrity supervision

Traditionally, the relationship between credit institutions and customers was mostly protected by the principles of banking secrecy, which were ensured by statutory guarantees in the majority of jurisdictions. Since at least 1989, the need to strengthen financial systems and safeguard financial integrity was shifted to the centre of international efforts on supervision, culminating in a call for action by the G7 at the Lyon Summit in June 1996. The basic pillar that money laundering should be criminalised by jurisdictions can be dated at least from the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,[15] as further developed by the UN Convention against Transnational Organized Crime, the so-called Palermo Convention.[16]

While the concept of obtaining the cooperation of financial institutions in detecting money laundering operations may be traced to the UN Declaration on Crime and Public Security, adopted by the General Assembly through Resolution 51/60,[17] the idea was internationally ratified through Article 7 of the Palermo Convention, which expressly called States to "institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasise requirements for customer identification, record-keeping and the reporting of suspicious transactions".[18] From that moment onwards, States recognised the need to limit the application of bank secrecy laws with respect to criminal operations, and to require financial institutions to act to ensure the integrity of banking systems.[19] Further international instruments, such as the UN Convention Against Corruption (UNCAC), the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (so-called Strasbourg Convention) and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions paved the way for other bilateral agreements, memoranda of understanding and international mechanisms destined to safeguard financial integrity and establish effective measures for supervision and law enforcement.

Literature commonly identifies four main phases for AML regulation[20]: (i) during the 1970s it was in its incipient stage, where the emphasis was regulatory and preventive in nature (i.e. record-keeping and suspicious transaction reporting by banks); (ii) the second stage, started in 1980s, produced criminalisation and internationalisation; (iii) in 1989, the AML regime entered a third phase (supra-nationalisation) with the establishment of the Financial Action Task Force (FATF) in 1989, whose purpose was to develop and coordinate the efforts to counter ML by identifying the trail of money flows in order to seize and confiscate illicit capitals systematically. This ad hoc informal inter-governmental body was later to become the institutional centre of a global supra-national legal regime. Finally, (iv) following 9 November 2001, a new phase emerged when the FATF mandate was extended to also cover terrorism financing.

With the establishment of the FATF and the subsequent issuance of the Forty Recommendations,[21] the role of financial institutions and certain businesses and professions in securing the effectiveness of AML/CFT systems was solidified as a minimum standard for the framework of the financial system. In this regard, early FATF rules already contained key-concepts that are essential for current supervision standards. This is the case for R. 4 of FATF's Forty Recommendations, which established that "countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations". Similarly, R. 5 provided for obligations to undertake CDD measures and prohibited financial intermediaries from keeping anonymous accounts.[22]

[15] UN, *Convention against illicit traffic in narcotic drugs and psychotropic substances,* 1989, available at: https://www.unodc.org/pdf/convention_1988_en.pdf.

[16] UN, *Convention against transnational organized crime and the protocols thereto*, 2000, available at: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf.

[17] UN, *Declaration on crime and public security*, 1997, available at: https://digitallibrary.un.org/record/234810?ln=en#record-files-collapse-header.

[18] UN, *Convention against transnational organized crime and the protocols thereto*, cit., art. 7.

[19] See also the landmark case in the context of the Commonwealth, *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461, which established the conditions under which banks owed confidentiality to their clients. The decision held that banks were not required to guard privacy in four circumstances, namely where compelled either by law, public duty, the interest of the bank or where the client had consented to disclosure (even implicitly). See, ex multis, Shuman, D.W., "The Origins of the Physician–Patient Privilege and Professional Secret", *Southwestern L.J.,* Vol. 29, 661–687, 1985; Wood, P.R., "Chapter 17 International Law of Bank Secrecy", in *Current Legal Issues Affecting Central Banks*, Vol. V, International Monetary Fund, 1998; Lytvynenko, A.A., "Data Privacy and Banking Secrecy: Topical Issues in Commonwealth, Continental Europe and International Jurisprudence", *Athens Journal of Law*, Vol. 5, Issue 3, 303–322, 2019.

[20] H. Shams, "Legal Globalization: money laundering law and other cases", *Sir Joseph Gold Memorial Series,* Vol. 5, London, 2004.

[21] FATF, *The forty recommendations*, 1990, available at: https://www.oecd.org/newsroom/2789371.pdf.

[22] (Id.

The Basel Committee's Core Principles for Effective Banking Supervision,[23] issued with the aim of providing guidance for jurisdictions wishing to strengthen their supervisory regimes, also enshrined similar obligations in its Principle 29, which stated that "the supervisor determines that banks have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the financial sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities".[24] Insofar as these principles and recommendations began to be transposed to national legislations, intermediaries started to exercise a fundamental role in financial supervision, giving rise to the current scenario.

From the last decades of the past century, authorities seem to have understood that money laundering poses threats to both economies and financial institutions. As largely demonstrated by economists, criminalisation of money laundering rests upon legitimate economic and public interests of jurisdictions,[25] causing direct and indirect costs to society. Concerning specifically financial intermediaries, ML brings at least two critical problems: (i) it erodes intermediaries from within, as there is often a positive correlation between ML and fraudulent activities undertaken by employees,[26] and (ii) it erodes customer trust, by increasing the perceived risk to depositors and investors with regards to institutional fraud and corruption, thus leading to reputational risks. In addition, the inadequacy of financial intermediaries' compliance policies may result in direct monetary damages due to the combined effects of fines and fall in share prices. These microeconomic aspects of ML, which may be characterised as an economic phenomenon,[27] justifies the now widely-accepted participation of banks in AML/CFT.

Although banks were the first victims (and facilitators) of ML activities, other agents are vulnerable to the use of legitimate payment and banking channels to stream flows of illicit origin. As the system evolves into a highly digitalised environment and retail transactions become increasingly influenced by the diversification of payment services, with growing numbers of cross-border operations and virtual assets-led solutions, the concept of "intermediary" widens considerably in scope, shifting from traditional banks to service providers and technology firms.

The reliance upon the financial sector to monitor suspicious transactions and ensure minimum standards for AML/CFT is a crucial feature of international and domestic financial integrity frameworks. The cooperation between competent authorities and financial intermediaries (whether banks or non-banks) enables supervisors to have proper oversight upon the financial system. By shifting part of the burden on monitoring and reporting of transactions to financial institutions and establishing requirements that prevent money flows from illicit activities to freely circulate in the economy, countries have made considerable progress on curbing money laundering and related offenses.

While the current model, combining joint efforts of public and private stakeholders, has been subject to constant review and enhancement, especially in view of technological development and the sophistication of infractions, it has not suffered any particular disruption in terms of its essential structure (i.e. that of using financial intermediaries as key-players in AML/CFT supervision).

As seen, traditional finance, or market-based finance, is characterised by major intermediaries centralising functions and financial resources. Banks and securities exchanges bring together a range of financial market participants, in particular those with resources (e.g. savers, lenders and investors) and those seeking financial resources (e.g. borrowers, entrepreneurs, etc.). The intermediary is, in this sense, a central point in traditional market-based financial systems, present in their traditional sectors of currency, payments, banking, securities and insurance.

Financial intermediation relies on trust and confidence in order to function. While regulation of these systems originally evolved as forms of private ordering or self-regulatory frameworks, over time, the State has taken an increasingly central role. This is mostly a result of failures and systemic risks that tended to come to the surface periodically in the context of financial crises. The role of government regulation in almost all aspects of finance, in particular in the aftermath of the 2008 financial crisis that elucidated the now-known too-big-to-fail risks,[28] is a reflection of such

[23] Although the original version dates from1997, the document has been updated subsequently. See current version, BCBS, *Core principles for effective banking supervision*, 2012, available at: https://www.bis.org/publ/bcbs230.htm..

[24] Id.

[25] See D. Masciandaro, "Economics of Money Laundering: A Primer", Bocconi University Working Paper No. 171, 2007; L. Borlini, "Issues of the International Criminal Regulation of Money Laundering in the Context of Economic Globalization", Paolo Baffi Centre Research Paper Series No. 2008-34, 2008.

[26] B. Barlett, "The negative effects of money laundering on economic development", Asian Development Bank, Regional Technical Assistance Project No. 5967, May 2002, available at: http://www.apgml.org/Index_files/ann_meet_doc_2002_public/pdf/ADB's%20Economic%20Research%20Report%20F
inal.pdf.

[27] M. Arnone—L. Borlini, "International Anti-Money Laundering Programs: Empirical Assessment and Issues in Criminal Regulation", Bocconi Legal Studies Research Paper No. 1933557, 2011; D. Masciandaro, "Money laundering regulation: the micro economics", *Journal of Money Laundering Control,* Vol. 2, No. 2, 49: D. Masciandaro, "Money laundering: the economics of regulation", *European Journal of Law and* Economics, Vol. 7, No. 3, 225-40, 1998.

[28] See, *ex multis*, D. Arner, "Towards a new design for international financial regulation", *Journal of International Economic Law,* Vol. 29, 391-453, 2007.

process. Market-based financial systems are thus often seen as unstable, with instability and other forms of market failures being addressed by regulation, albeit never entirely successfully. States, governments and regulators therefore assume an increasing stake in maintaining the financial system's stability and integrity, becoming a crucial part of the dynamics of the sector.

The dominance of concentrated intermediaries and the reluctance over the centralisation and reliance of finance in the hands of the State fuelled the idea of DeFi and its vision of finance without intermediation.[29] Under such view, technology could replace the complex net of regulatory burden with simple automatised solutions that enable a peer-to-peer network for financial activities. For proponents of the idea, the design would also help mitigating the risks inherent to concentrated systems. Although innovative technology does not necessarily entail disintermediation, decentralised solutions (including, for instance, smart contracts, DLT and decentralised autonomous organisations) have gradually gained space in financial markets over the past years. Finance without intermediation brings with it many implications for traditional regulation which the global AML/CFT network is responding to. From an enforcement perspective, if there is no intermediary then who is responsible for complying with AML/CFT requirements? The change in fact represents a significant shift in how traditional regulation functions. Recent regulatory measures seem to take a "where's wally" approach to DeFi, which relies on the assumption that somewhere in the DeFi infrastructure there is probably an identifiable person or entity providing a service that would render them subject to compliance with AML/CFT requirements. While it is premature to say whether this will always be the case, it certainly indicates that AML/CFT regulators and policy makers will have a role to play in shaping the evolution of DeFi. On the one hand, this role could be viewed as erosive in that it may drive developers to move away from truly decentralised solutions, but, on the other, without some degree of accountability such platforms may become particularly vulnerable to abuse by criminals for ML/TF.

In many ways, CBDCs emerge as a reaction to DeFi and its increasingly fast development and scalability. By launching CBDC initiatives, national authorities seemingly aim to regain space in retail transactions, notably in the digital environment, thus competing with stablecoins and other crypto-assets in order to safeguard monetary and financial stability, as well as each jurisdiction's legal tender. The development, provision, participation and/or control over CBDCs are a radical step not only for monetary policy, but also for financial integrity. The idea that governments may be able to fully control financial and payment transactions triggers many issues, spanning from matters of government trust to privacy and informational advantages. Before examining these topics, it is important to briefly summarise how the structuring of CBDCs is actually being considered by authorities, since each architecture implies different consequences for our analysis.

On a broad level, the architectures for CBDCs vary fundamentally in accordance with the technology, accessibility and distribution of operational functions attributed to each structure. Other elements, such as anonymity, the domestic or cross-border nature of the structure, transfer mechanisms, interest policy, availability and limits, may also be balanced in each design, depending, nonetheless, on the definition of the fundamental features mentioned above.

One or many: a physiognomy of CBDCs

As we embark in our analysis of CBDCs within the prism of the AML/CFT regulation, it is imperative to frame the object of our study by drawing the external and internal boundaries of this concept and to define the taxonomy of the terms employed herein.

From an external perspective, the world of crypto-assets[30] is vast and varied, encompassing instruments as different as Bitcoin and Diem. Furthermore, this is a sector in constant evolution that has experienced telluric transformations in the last decades. From an internal perspective, scanning through Central Banks' white papers, it is apparent that there is not one type or uniform definition of CBDC. Rather, CBDCs can be better understood as a type of digitalised currency, with legal tender status,[31] whose purpose and technical aspects can vary widely.[32]

[29] See, among others, M. Zachariadis—P. Ozcan, "The API Economy and Digital Transformation in Financial Services: The case of Open Banking". SWIFT Institute Working Paper 2016-001, 2017.

[30] For the purposes herein, we employ the term "crypto-asset" as defined in Article 3(1)(5) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (so-called MiCA Regulation), accordingly: "'crypto-asset' means 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". See, *ex multis*, Annunziata, F., "An Overview of the Markets in Crypto-Assets Regulation (MiCAR)", European Banking Institute Working Paper Series No. 158, 2023.

[31] Regarding legal tender, see, in the UK, section 1 of the Currency and Bank Notes Act 1954; in the US, section 16(1) of the Federal Reserve Act (in conjunction with section 102 of the Coinage Act); and in the EU, Article 128 TFEU.

[32] Norges Bank, *Central Bank Digital Currencies,* 1, 2021, 5; D. Legal—G. Ortiz Ibarrola—C. Blanco, *Moneda Digital del Banco Central: Implicancias para la estabilidad financiera y la politica monetaria en Paraguay,* Documentos de Trabajo n. 27 Banco Central del Paraguay, 2022, 4.

Let us then start by drawing the external margins of the notion of a CBDC to subsequently identify its internal categories.[33]

While there is not, currently, one settled definition,[34] there are two key features that are commonly understood as sitting at the core of the notion of CBDCs and that distinguish them from other types of crypto-asset.[35] These are that CBDCs are issued by a Central Bank, as their liability,[36] and serve as a legal tender within a defined jurisdiction.[37]

These two characteristics are key in understanding the fundamental innovation bore by this new form of currency. In effect, crypto-assets have been in circulation for decades.[38] However, their issuance and management has always been within the purview of the private sector. In contrast, CBDCs could be the first digital equivalent of the traditional "paper" fiat currency.[39] This means that their risk profile would coincide with that of fiat currencies and their management and issuance would rest solely with the Central Bank. CBDCs would, thus, be the first digital currency free from liquidity and creditor risk,[40] necessarily stemming from the reliance on a private intermediary, and that operates on a single technological infrastructure for an entire currency area.

Having drawn the external boundary, it is now time to dive into the domain of CBDCs to trace some internal distinctions. Eminently, the analysis of the white papers published by Central Banks worldwide reveals that CBDCs are far from a homogeneous group. Apart from the, above detailed, two common features, the concrete implementations proposed vary widely depending on the needs identified at a regional level and the values considered preeminent by each jurisdiction.[41]

The main categories of CBDCs are the following: wholesale/retail; direct/indirect; centralised/decentralised; and domestic/cross-border. It must be underlined that these categories represent an abstraction of the concrete models proposed and should not be seen as a black and white distinction. Rather, most of the proposed implementations sit somewhere in-between these theoretical pairs.

Let us now briefly analyse each category.

A wholesale[42] CBDC is characterised by not being directly distributed to the public but rather to identified intermediaries, for the purpose of streamlining their reciprocal settlement process.[43] A retail CBDC,[44] on the other hand, is distributed directly to all participants of the market and used in day-to-day transactions. It is the latter, therefore, the currency that we could truly assimilate to a traditional *fiat* currency.

Moreover, a direct CBDC is one that is directly distributed by the Central Bank to its final users.[45] The system in

[33] On the evolution and classification of CBDCs, see, inter alia, Geva, B., "Cryptocurrencies and the Evolution of Banking, Money and Payments" in Brummed, C., (ed.), *Crypto-assets—Legal, regulatory and monetary perspective*, Oxford University Press, 2019; Geva, B., Grünewald, S., Zellweger-Gutknecht, C., "The E-Banknote as a 'Banknote': A Monetary Law Interpreted", 41:4 Oxford Journal of Legal Studies 1119, 2021.

[34] For a review of some of the existing definitions see S. Allen, et al. *Design choices for central bank digital currency: Policy and technical considerations*, No. w27634. National Bureau of Economic Research, 2020, 11.

[35] See the definition provided by the International Monetary Fund, "*CBDC is a new form of money, issued digitally by the central bank and intended to serve as legal tender*" in IMF Staff Discussion Note, *Casting Light on Central Bank Digital Currencies*, 2018; see also the definition provided by the US Federal Reserve, "*CBDC is defined as a digital liability of the Federal Reserve that is widely available to the general public*" in Federal Reserve, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation,* 2022.

[36] Bank for International Settlements, *Central Bank Digital Currencies: system designs and interoperability,* Basel, 2021, 4.

[37] Norges Bank, *Central Bank Digital Currencies,* cit., 5, 13.

[38] So-called Commercial Bank Money are a classic example of privately issued currencies, see M. Klein—J. Gross—P. Sandner, *The digital euro and the role of DLT for central bank digital currencies* in *Frankfurt School of Finance & Management GmbH, FSBC Working Paper,* 2020, 4.

[39] S. Allen, et al. *Design choices for central bank digital currency: Policy and technical considerations*, cit., 10. See also Geva, B., Grünewald, S., Zellweger-Gutknecht, C., "The E-Banknote as a 'Banknote': A Monetary Law Interpreted", cit.

[40] On the risk-free nature of Central Bank money, M. Klein—J. Gross—P. Sandner, *The digital euro and the role of DLT for central bank digital currencies,* cit., 4, 12, "*a retail CBDC is, like cash, a risk-free means of payment, but in a digital form*"; R. Auer—R. Böhme, *Central bank digital currency: the quest for minimally invasive technology*, *No. 948. Bank for International Settlements*, 2021, 5; European Central Bank, *Report on a digital Euro*, October 2020, 7. While it is true that a digital form of Central Bank money already exists, i.e. Central Bank reserves, these are only accessible to a very limited number of intermediaries and can, thus, not be compared to classic fiat currencies, Bank of England, *Central Bank Digital Currency Opportunities, challenges and design*, cit., 7.

[41] M. Klein—J. Gross—P. Sandner, *The digital euro and the role of DLT for central bank digital currencies,* cit., 12-13.

[42] Ibid., 11.

[43] For an example see the mBridge project jointly developed by BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates, Bis Innovation Hub, *Project m-Bridge. Connecting economies through CBDC,* October 2022.

[44] N. Pocher—A. Veneris, *Privacy and transparency in cbdcs: A regulation-by-design aml/cft scheme*, in *IEEE Transactions on Network and Service Management*, 2021, 1; D. Legal—G. Ortiz Ibarrola—C. Blanco, *Moneda Digital del Banco Central: Implicancias para la estabilidad financiera y la politica monetaria en Paraguay*, cit., 4.

[45] For a visual representation of these three models see R. Auer—R. Böhme, *Central bank digital currency: the quest for minimally invasive technology,* cit., 10.

this model has one layer[46]: the Central Bank manages the network and provides the services—safekeeping, exchange etc.—and the users transact within this environment in a peer-to-peer fashion. In the indirect model, an intermediate layer is introduced.[47] While the issuance and the maintenance of the underlying network is still in the hands of the Central Bank, all user-facing activities are performed by authorised intermediaries.[48] This implementation discharges the Central Bank from all customer-related activities and, in a way, replicates the organisational structure of traditional financial markets.[49] A third hybrid model is also possible. Within the latter, users can both avail themselves of intermediaries and transact peer-to-peer. Usually, the peer-to-peer function is only provided for small deposits and low-value transactions, whereas, for larger deposits, customers must use intermediaries.[50]

The crucial difference between the centralised and decentralised model rests in the technology used by the Central Bank. Eminently, if the Central Bank chooses to implement the currency through a decentralised ledger or through a "traditional" centralised ledger.[51] It is important to underline that, even when a DLT is chosen, it will probably not resemble the public blockchain of the main crypto-assets, as Bitcoin or Ethereum.[52] Rather, to preserve the public control over the currency's issuance and management, CBDCs tend to implement a permissioned blockchain that affords a varying level of centralised control and governance to the Central Bank.[53]

Finally, the CBDC can be designed as domestic, cross-border[54] or as indifferent to geographical location. This depends on whether the currency can be spent, acquired, and used outside the geographical borders of the issuing jurisdiction. A domestic CBDC is one that can only be used inside the issuing jurisdiction.[55] An exclusively cross-border CBDC is one that can only be used for transnational transactions. Finally, a CBDC is indifferent to geographical location when, just like cash, can be spent everywhere, solely based on the acceptance by the payee.

It is clear how each of these implementations poses a substantially different risk in terms of anti-money laundering. The capillarity of the CBDC's distribution (retail/wholesale), its territorial scope and the presence of reliable intermediaries are key in the assessment of the anti-money laundering risk. Apart from the risk-factor, the way a CBDC is designed impacts the structure of the anti-money laundering governance and controls. For instance, a direct coin would profoundly redesign the governance of anti-money laundering, as the Central Bank would be the sole entity able to identify and monitor users. In contrast, an indirect CBDC would resemble much more the classic model with intermediaries managing user-facing activities and the Central Bank acting as supervisor.[56]

In this sense, when speaking about CBDCs and AML, it is crucial to distinguish between each type of implementation. We should not tar all crypto-assets with the same brush

[46] N. Pocher—A. Veneris, *Privacy and transparency in cbdcs: A regulation-by-design aml/cft scheme,* cit, 2.

[47] S. Allen, et al. *Design choices for central bank digital currency: Policy and technical considerations,* cit., 10, "*central banks would disseminate CBDC to commercial banks–just as they now do with cash–and commercial banks would distribute these to individuals and businesses by setting up and managing digital wallets*".

[48] D. Legal—G. Ortiz Ibarrola—C. Blanco, *Moneda Digital del Banco Central: Implicancias para la estabilidad financiera y la politica monetaria en Paraguay,* cit., 5; see the model proposed by European Central Bank, *Report on the Digital Euro,* cit., 25.

[49] Direct/indirect CBDCs should not be confused with so-called synthetic CBDCs—where the CB only manages the issuance of the currency to financial institutions with the management of accounts and funds entirely left to these entities—which are out of the purview of the present article, for an analysis synthetic CBDCs, see Bank of International Settlements et. al., Central bank digital currencies: foundational principles and core feature, 2020,4.

[50] The White House, *Technical evaluation for a U.S. Central Bank digital currency system,* Washington, 2022.

[51] Bank of England, *Central Bank Digital Currency Opportunities, challenges and design*, London, 2020, 6.

[52] M. Klein—J. Gross—P. Sandner, *The digital euro and the role of DLT for central bank digital currencies*, cit., 7.

[53] See, The White House, *Technical evaluation for a U.S. Central Bank digital currency system,* cit., 11, "*a permissionless approach does not make sense for a system that has at least one trusted entity (i.e. the central bank). It is possible that the technology underpinning a permissionless approach will improve significantly over time, which might make it more suitable to be used in a CBDC system. However, given the state of the technology, most of the analysis that follows assumes that there is a central authority and a permissioned CBDC system*"; Norges Bank, *Central Bank Digital Currencies,* cit., 30.

[54] Exclusively international CBDCs are usually also wholesale and are proposed as a means to streamline large cross-border transactions among two or more jurisdictions. See, as an example, the MBridge project developed by the Bank for International Settlements in cooperation with the Bank of China, the Bank of Thailand, Hong Kong Monetary Authority, and the Central Bank of the UAE at https://www.bis.org/publ/brochure_mbridge.pdf

[55] Bank of England, *Central Bank Digital Currency Opportunities, challenges and design,* cit., 21.

[56] See the model proposed by, Bank of England, *Central Bank Digital Currency Opportunities, challenges and design*, cit., 27. It is important to underline that, with respect to the Central Bank, the issuance of a CBDC would, in any case, redefine its role. Even in a two-layered infrastructure the CB would have direct access and manage a ledger recording all transactions carried out with the connected digital currency. This would be substantially different to the current model where digital ledgers are privately held by financial institutions and CBs only record the issuance of cash without any control on transactions. See also, Bank for International Settlements, *Central Bank Digital Currencies: system designs and interoperability,* cit., 5, "*in any CBDC system, the central bank would face additional operational or oversight tasks and accompanying challenges regardless of the division of responsibilities among the various actors*".

as some may pose a fundamentally new risk, while others may not alter the traditional infrastructure in any significant way.

There is, in particular, one distinction that is of key relevance for financial flows monitoring: the retail/wholesale binomial.

A wholesale CBDC does not create new fundamental avenues neither for control nor for evasion. The transactions processed are large exchanges among identified and strictly regulated entities—usually financial institutions. They do not reveal much about the underlying retail transactions, and the connected sensitive data, and do not facilitate any movement of value among individuals. The main function of such a system is to facilitate settlement among regulated institutions on a national or transnational basis.

In contrast, a retail CBDC would process extremely detailed personal data—location, spending habits, income, etc.—on individuals and private entities.[57] It would do so within a technological infrastructure that is more centralised—at least logically—and to which the State would have direct access.[58] At the same time, the digitalisation of a fiat currency would present a significant money laundering risk due to the capillarity of its distribution and the dematerialisation and volatility typical of digital assets.

Retail CBDCs are, then, the crux of the transparency vs. privacy trade-off that underlies the development of these currencies. For this reason, the present paper will focus on retail CBDCs. As this implementation is the one that fundamentally alters the current architecture of control tilting the previous trade-off between privacy and transparency.

The legal boundaries of CBDCs: a legislative patchwork

Concerns over the legal treatment conferred to CBDCs often permeate the discussions on the structuring of digital currencies, especially in relation to monetary law and the mandates of central banks.[59] In order to issue a CBDC, the principles of attribution of powers and legality require a firm anchor in the mandate established by the applicable central bank law. This means that for several jurisdictions,[60] the implementation of CBDCs will be conditioned to the passing of amendments to rules governing central bank powers, which, in some cases, are even enshrined within constitutional texts. The acknowledgement that the CBDC endeavour may require major legislative efforts assumes even greater implications when we consider the ancillary roles taken by central banks to execute the project. Particularly for direct CBDC models, central banks are likely to undertake several tasks that are currently atypical for monetary authorities, such as carrying out CDD measures, maintaining records of transactions, monitoring transactions conducted by politically exposed persons and generating suspicious transaction reports. For tiered models and intermediated designs, some degree of central bank participation in AML/CFT supervisory activities is also expected to occur. In order to avoid legal challenges to the structure, jurisdictions should undertake to establish a solid legal foundation for retail CBDCs, encompassing financial integrity aspects.

In practical terms, the greater the powers invested in central banks to operate retail CBDCs, the greater the need to carry out substantive reforms to their mandates, with increasing chances of running into more rigid legal texts, which, in turn, require more political efforts to be changed.

The legislative challenge faced by jurisdictions not only consists of reviewing the mandate of central banks, as to provide the legal foundations for a fully fledged or partial financial integrity function, but also to articulate the new tasks with existing AML/CFT laws and regulations, as well as data protection and privacy statutes, and, where applicable, also the frameworks for payments, cybersecurity and crypto-assets. Furthermore, it should be noted that the current structures of AML/CFT will continue to be applicable for operations, transactions and relationships covered by the existing framework. Retail CBDC transactions will only integrate the plethora of possible financial and payment transactions, gaining a special regime subject to direct or partial central bank engagement, depending on the specific design chosen by each jurisdiction. However, their introduction will not change the pre-existing AML/CFT regime or entail any type of exclusion. In view of the coexistence

[57] Bank for International Settlements, *Central Bank Digital Currencies: system designs and interoperability,* cit., 8; D. Ballaschk—J. Paulick, *The public, the private and the secret: Thoughts on privacy in central bank digital currencies,* in *Journal of Payments Strategy & Systems*, 15/3, 2021, 280.

[58] Such a centralisation does not depend on the data archiving technology used—DLT, blockchain, or centralised ledger—but rather on its structure. Eminently, what matters for privacy purposes is that the ledger where transaction information are recorded would live a process of centralisation. The traditional EFT system is rooted in a myriad of proprietary ledgers each held by the financial institution. In contrast, a CBDC would be rooted in a single ledger where all transactions with a certain currency are recorded. The key point is, hence, the shift from multiple ledgers to a single ledger. If such a ledger is then stored in a centralised or decentralised fashion (e.g. through blockchain) is not crucially important.

[59] See Bossu et. al., "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations". IMF Working Paper WP/20/254, 2020.

[60] A recent study demonstrated that among the 171 central banks of the IMF membership, 61% of jurisdictions limit the authority of issuance of currency to banknotes and coins, 23% allow directly for the issuance of currency in a digital format and 16% are unclear as to whether they authorise the issuance of a digital version of central bank currencies (Id., ibid., p. 21).

of regimes, a few consequences may be drawn: (i) to some extent, there should be an exchange of information between financial institutions and central banks for purposes of properly assessing customers' risk profiles and historic of transactions; (ii) distributions of tasks should avoid, where possible, the overlapping of responsibilities; and (iii) systems developed by stakeholders should be interoperable, not only within a certain jurisdiction but also (in certain cases) for cross-border purposes.

To understand how the different models delineated in the foregoing section affect the nature of the ensuing legal reforms, it is necessary to dive further into certain legal and institutional aspects entailed in the design of the CBDC architectures.

Legal implications of different CBDC designs

When it comes to CBDCs, several issues should be considered from the perspective of financial integrity supervision. The first aspect is the definition of the features of the CBDC design to be put in place: will it lead to complete disintermediation? Will it concentrate tasks in the hands of public stakeholders, either partially or entirely? Once these questions are addressed, a second step involves the understanding of how different AML/CFT procedures shall be allocated between the relevant stakeholders, pertaining both to the private and public sectors, as the case may be. From a public standpoint, it is necessary to understand if the central bank will be responsible for performing specific routines or if these will be entrusted exclusively or partially to FIUs or other competent authorities. Moreover, it will be important to set the governance structure for those responsible for running AML/CFT supervision, in relation to those developing software solutions, the market participants (when applicable), other public agencies directly or indirectly involved in supervision (as data privacy authorities and the financial supervisors of intermediaries), as well as sensible sectors of the government. Finally, in a third step, the accountability of central banks, FIUs and the enforcement measures against participant institutions shall be discussed as a delicate but inevitable part of regulating CBDC's integrity framework. This also encompasses understanding the intersections among the CBDC architecture with digital privacy and data processing regulation, including the interplay with data authorities.

From a financial integrity perspective, the simplest way forward would be for financial intermediaries to remain the main authority in charge of centralising the receipt of disclosures filed by reporting entities, assessing their risks and disseminating the resulting analyses to the competent bodies. In a CBDC-led economy, financial intelligence units (FIUs) could assume a privileged position of mediating the relationship between the central bank, private players and enforcement authorities, while also acting as a counterweight to the central bank's AML/CFT-related tasks. Under such a model, the central bank would play a role equivalent to that of a reporting entity, without assuming supervisory powers of its own. Regulatory competences would be exercised exclusively by the FIU, which would be responsible for establishing the standards and procedures applicable to retail CBDC transactions. On the other hand, the central bank would undertake to run the infrastructure and execute operational functions related to CDD and transaction monitoring. This could be beneficial for three objective reasons: (i) first, the model distributes attributions without detracting institutions from their core-mandates (i.e. primarily monetary functions for central banks and financial integrity tasks for FIUs); (ii) second, it avoids over-concentration of powers in the hands of a single authority, facilitating the creation of checks-and-balances mechanisms for ensuring accountability and review; and (iii) third, from a legal standpoint, it simplifies the legislative procedure to amend existing laws and specific competences, rather than requiring a comprehensive reformation of mandates.

Alternative model: central banks as co-regulators

The fact that central banks may resort to RegTech and SupTech solutions[61] when implementing retail CBDCs—and even embedded protocols for supervision—should not substantively alter the governance structure delineated above.[62]

[61] Regtech is the label given to the use of information technology in compliance, supervision and regulation. See, *ex multis*, T. Butler, "Towards a Standards-Based Technology Architecture for RegTech", 2017, 45 Journal of Financial Transformation, 49. See also EBA, "Analysis of RegTech in the EU Financial Sector", EBA/REP/2021/17, 2021. A concept related to RegTech is that of "SupTech", which is used to refer to the use of technology by financial regulators to conduct their supervisory and oversight activities.

[62] Different levels of supervision and enforcement may be achieved by RegTech solutions and will depend on the capacities and intentions of each public stakeholder. This requires understanding the new roles to be played, which generally encompass: (i) acting as developers/users of RegTech products; (ii) as buyers/users of software developed by third parties; (iii) as facilitators/coordinators of market developments; and/or (iv) as supervisors to RegTech firms (See Luca Enriques, "Financial Supervisors and Regtech: Four Roles and Four Challenges", Revue Trimestrielle de Droit Financier 53 (2017)). While these are not mutually exclusive activities, they each bear specific practical consequences. For supervisors to act as developers of RegTech solutions, they must be able to draw and retain people with the required skillset among its ranks. Regulators are generally under-resourced in terms of human capital and budgets and developing high-end technology capable of ensuring the soundness of a country or region-wide retail CBDC system which is also resilient to cyber-attacks is a complex and expensive task. In addition, competition with the private sector may be difficult to sustain, particularly in jurisdictions that struggle with economic difficulties. Acting as buyers, supervisors may either purchase standard products, standard prod-

Also, in a scenario where the central bank assumes greater prominence in adopting measures for prevention of ML/TF risks, the FIU could keep its role of centralising financial intelligence data and distributing alerts to the competent authorities. To that extent, it should always maintain its autonomy and act as an advisory and tutelage body of the central bank's retail CBDC activities, while the central bank undertakes to collect raw data, monitor transactions and generate suspicious transaction reports. From a legal perspective, the main difference implied in a model marked by a greater regulatory/supervisory activity by the central bank consists of the need to have these regulatory powers properly foreseen under the applicable laws. As opposed to the first model, in this alternative case the central bank would assume specific regulatory functions and would act as a co-regulator of the structure, asides from acting as its operational coordinator. This would entail a more profound reform of its legal mandate, bearing the legislative implications mentioned above.

Performance of operational tasks by central banks

Proposing central banks to act essentially as reporting entities should naturally come with a few carve-outs and clarifications. Central banks should not be equated to traditional reporting entities since the nature of their activities is fundamentally different from those of financial intermediaries: they do not carry out business activities, but rather exercise public duties. When engaging in financial or payment transactions, central banks will not pursue interests of their own, nor will they seek for profits or commercial relationships. Even when operating direct CBDC designs, assuming responsibility for customer interface and due diligence measures, central banks are expected to act in accordance with a pre-existing public mandate.

The difference is essential since it entails that central banks are not directly driven by market forces and should be subject to a public law regime, rather than a private law one. In most jurisdictions, this means that the central bank will act in the quality of a body of the public administration, with the privileges and immunities it entails (such as the presumption of legality and validity of its acts). In this sense, it should evidently not be subject to any kind of sanctions for non-compliance with mandatory AML/CFT standards and could also not be strictly considered a regulated or supervised entity by the FIU.

Nonetheless, there are ways to structure a public governance whereby the FIU undertakes the role being a second-tier administrative body, responsible for evaluating the central bank's performance of financial integrity duties and assisting with the identification of possible deficiencies in its internal controls and risk management systems, proposing periodical enhancements and ensuring that it complies with the required standards of AML/CFTs in the operation of retail CBDCs. Without prejudice to this administrative oversight, acts practised by the central bank and the FIU should be generally passive of being scrutinised by judicial review.

An additional point to be considered in a direct model foreseeing the performance of operating tasks by the central bank or, in any case, its involvement in the retail level consists of the reputational risks arising therefrom. Specifically, once the central bank becomes responsible for ensuring the technical requirements for the direct operation of retail transactions, including complying with AML/CFT obligations, and maintaining an interface with customers, its role is significantly shifted from purely monetary and/or supervisory tasks, as currently set out in most mandates. In the eyes of the public, the quality of the tasks and services sustained by the central bank in the context of retail CBDCs might affect their perception of the institution. Although this could bring consequences to the overall reputation of the central bank, including with regard to its traditional roles, we believe this risk should not impact on the CBDC's design, as it does not bring per se, decisive consequences. Rather, the reputational impact is most likely to be linked to the actual functioning of the system: if the CBDC is, indeed, presenting failures and vulnerabilities, the fundamental issue to be tackled is not the reputational risk, but the failures themselves. On the contrary, it does not seem likely that a fully functioning retail CBDC would bring about significant reputational damages to a central bank. In any case, this risk is duly mitigated in indirect CBDC models, as the Digital Euro (see below): for these CBDCs, the lack of an indirect interface with end users and the presence of intermediaries should minimise these risks significantly.

Outsourcing and delegation of powers

Similarly to reporting entities, central banks could also have the faculty of outsourcing some of their tasks, in a third-party reliance scheme. The delegation of tasks to third parties is another point to be explicitly covered by the legal foundations of retail CBDCs, in respect to the principle of legality. Jurisdictions may vary in the flexibility conferred

Footnote 62 (continued)

ucts with certain tailored specificities or fully tailored products. In all three cases, there is a risk that developers may exploit information asymmetries, considering that supervisors will ultimately be treated as customers, in direct or indirect conflict of interests with other market participants. Also ensuring a balanced and effective contractual governance of the relationship with the developers may pose hardships for weak jurisdictions. Moreover, entrusting the development of critical software to be used by several countries to a given number of developers may be risky for the over-empowerment of certain players it entails. More specifically, Big Firms that are also likely to simultaneously act as service providers for a wide range of financial and non-financial services may concentrate systemic and operational risks.

to public entities for the delegation of powers and outsourcing, with additional divergence arising from the contractual regime applicable to such activities. Public contracts and procurements may be part of the outsourcing process, requiring, in some cases, specific legislative treatment. In any case, third parties should be regulated, supervised and monitored and hold a contractual relationship with the public sector. The performance of specific tasks on behalf of the central bank should always be subject to the latter's control over the execution. Regulators should pay close attention to central bank reliance on third parties, given the systemic and integrity risks inherent to retail CBDCs. While the implementation of an internal compliance structure by central banks involves high investments and maintenance costs for public administrations, outsourcing gives rise to third-party risks of different natures (e.g. competition issues and conflict of interests for BigTechs, over-concentration of data processing and operational vulnerabilities).

Centralisation and public abuse

Understanding where governments may unlawfully make use of the powerful surveillance tools enabled by CBDCs is crucial for identifying red flags and developing mechanisms to mitigate such risks. It is also necessary for tailoring governance structures to prevent abuses from ever happening and for building paths to accountability. There are two main dimensions to public abuse: (i) an internal dimension, whereby public agents may seek to somehow benefit or profit from an irregular use of CBDC and its ancillary services or functions (which may be generally referred to as corruption), and (ii) an external dimension, whereby public agents or bodies may use information collected by CDBC infrastructures to unlawfully monitor citizens' activities, invading their private lives and either attempting to influence their behaviour or disposing of their personal and financial data in an abusive way.

Discussing corruption in CBDC may be premature, given the overall initial stages of the initiatives. Without any ambition for developing a comprehensive catalogue of potential corruption acts in CBDC architectures, we may highlight certain practices: (i) the political use of CBDC surveillance structures, by a public agent, against his/her political adversary (e.g. collecting and disclosing personal data); (ii) the interference in CBDC monitoring systems to tamper a suspicious transaction report, PEP-related alert or underlying investigations, as to prevent enforcement from successfully moving forward in the benefit of the agent itself or of an interested third-party (in exchange for political favours or bribes); (iii) the forgery of false data or false alerts, also for a political use; or even (iv) public agents may retrieve personal data collected by CBDC pertaining to a single user or group of users and sell them to an interested party, in exchange for benefits or bribes. In all of these cases, public agents somehow distort an impersonal and technical functioning of supervisory apparatus, gaining access to the systems and using them for their personal intentions. The risks may even bear diplomatic consequences, in case sensible information pertaining from national or foreign politicians is leaked to other countries. These are issues more easily susceptible to occur in designs that confer broad supervisory powers to central banks, FIUs or other public bodies and are especially delicate in countries with weak anti-corruption standards in place. The practices are no novelty in themselves, but may become even more perilous insofar as CBDCs gain importance in national economies.

The external dimension to public abuse in CBDC, discussed in Section "One or many: a physiognomy of CBDCs", relating more directly to data protection and privacy, offers a more dystopian vision: governments using technological surveillance systems to monitor day-to-day activities of citizens and interfering with their private sphere of action.

In order to prevent both internal and external forms of public abuse, jurisdictions should have robust anti-corruption measures in place, with strict assurance of the rule of law. Moreover, CBDC designs should have a minimum degree of privacy protection, technically impeding authorities to gain access to personal data and sensible consumer habits by data crossing. This should be a mandatory requirement for any design, as an imperative of fundamental rights. As mentioned, data processing laws and data processing authorities will play an important role in this regard, countering other authorities in tentative abuses. Most importantly, central banks, FIUs and competent authorities must have autonomy and retain independence from political groups, so that their structures are not easily manipulated from within. Proper governance and accountability are essential for segregating information and tasks, punishing deviations practised by public agents and ensuring that public bodies strictly observe their mandates, acting solely within the limits of the law. Finally, the legal framework for a CBDC should be legitimised by a far-reaching public dialogue, so that stakeholders may be presented with the chance to be heard and balance for themselves the benefits and risks of each CBDC design. Citizens may then decide how much privacy they are willing to sacrifice in detriment of the integrity of the financial system and the prevention of crimes.

Preliminary remarks: understanding the complexity of legislative reforms

In view of the above, it is clear that the implementation of CBDCs will require the underlying legislative reforms to also encompass the supervisory, governance and operational apparatus for financial integrity. In principle, there would not

be a need for governments to necessarily introduce a new AML/CFT law. Alternatively, the required reforms to monetary and central banking laws for enabling a sound adoption of retail CBDCs could contain specific provisions to address these new powers and amend existing laws in order to ensure alignment between different frameworks.

For ease of clarity, reforms should envisage the following topics: (i) the central bank's mandate should explicitly encompass either regulating or operating financial integrity aspects of CBDCs; (ii) such mandate should also discipline the possibility of delegation of specific competences and outsourcing of tasks to third parties, where permitted; (iii) the AML/CFT law should regulate the regime for retail CBDC, setting forth the conditions, standards and obligations for the relevant stakeholders; and (iv) interplay with other authorities (in particular, data protection authorities) and FIUs should be set forth under the applicable statutes, including for purposes of defining responsibilities and accountability. Granular rules for exchange of information, internal governance structures and technical standards could be set forth by secondary laws, administrative regulations and MoUs, depending on the particularities of each given jurisdiction's legal system.

Understanding the architectural shift of CBDCs

Before we embark in our analysis of the Digital Euro there is one last piece, we need to add to our overarching analysis of CBDCs. To understand how and why Central Bank Digital Currencies are expected to tilt the pre-existing *status quo*, we need to explore their impact on the architecture of financial monitoring. These reflections are largely applicable to traditional and distributed infrastructures as, in both systems, the introduction of CBDCs would mean the Central Bank would have full and direct access to a logically centralised ledger.[63]

There are two elements that are key in understanding this shift and its impact on financial monitoring.

First, a CBDC would reunite all the, currently fragmented, ledgers into a single currency-wide ledger. This is a momentous shift as it would push the architectural boundaries of financial monitoring even further. Eminently, the digitalisation of financial transactions is already seen by some as the holy grail of monitoring.[64] The transition from cash (token-based and peer to peer[65]) to digital transactions (account-based and necessarily intermediated) makes any transaction routed through such networks traceable and the connected metadata available to the private and public eye.[66] The key issue, in terms of privacy, is that digital value exchange systems require, by-design, the presence of an intermediary. This intermediary is the "man in the middle" who creates the possibility of control.[67]

However, legacy transaction systems are rooted in centralised ledgers, privately held by each intermediary. In its ledger the intermediary only records the transactions carried out by its customers and their account balance. The transaction trail is, hence, fragmented. Each intermediary has a limited understanding of the transaction trail as it only sees what its customer does. This fragmentation also means that an investigator, to pierce together a transaction trail, will have to reconcile the data contained in multiple ledgers. In contrast, a CBDC—whether rooted in a centralised or decentralised infrastructure—would generate a single, currency-wide ledger. This would significantly augment the monitoring potential enabled by financial ledgers. Eminently, such an architecture would eliminate the need to reconcile ledgers so providing the monitor with a complete picture of all transactions carried out with the currency.

Together with the archiving architecture there is a second element that makes CBDCs more transparent: its accessibility.

Currently, financial records are, almost entirely, controlled by the private sector. The ledgers are held by financial institutions that have exclusive control over their access. This means that State monitoring is always indirect. In the

[63] The same does not apply to so-called synthetic CBDCs—where the CB only manages the issuance of the currency to financial institutions with the management of accounts and funds entirely left to these entities—which are out of the purview of the present article, for an analysis synthetic CBDCs, see Bank of International Settlements et. al., *Central bank digital currencies: foundational principles and core feature*, 2020,4.

[64] Already in 1970 Stanford professor Paul Armer underlined how the (then) upcoming introduction of Electronic Funds Transfer Systems (EFTS) had the potential to create the best non-intrusive means for individual and collective control P. Armer, *Computer Technology and surveillance,* University of Stanford—Center for Advanced Study in the Behavioral Sciences, 1975, 11–12, "*The point here is that it's not enough just to have the option of using cash, the cash option must be used frequently or it becomes useless as a means for privacy (…) an EFTS (Electronic funds transfer system) system (…) was the best surveillance system we could imagine within the constraint that it not be obtrusive*".

[65] M. Klein—J. Gross—P. Sandner, *The digital euro and the role of DLT for central bank digital currencies,* cit., 17.

[66] F. Tronnier—D. Harborth—P. Hamm, *Investigating privacy concerns and trust in the digital Euro in Germany,* cit., 1, "*All new and digital currencies or payment methods create and leave electronic records, which could be tracked and monitored to counteract money laundering or other illegal activities*"; N. Bilotta, *CBDCs and Stablecoins: The Scramble for (Controllable) Anonymity,* cit., 168.

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

financial field, the State must either delegate to financial institutions—as it happens with AML checks—or cooperate with them—as in financial investigations—to access the relevant information. Either way, the State does not have direct access to the ledger. In this system, financial institutions play a role of filter guaranteeing, at least theoretically, that the State can only access information when legal. The flip side of the coin being, obviously, that a ledger fully in the hands of the private sector allows for extensive corporate monitoring and profiling.

In contrast, the CBDC's ledger would be managed and stored by the Central Bank. CBDCs disintermediate the relation between the State and the financial ledger allowing for direct control and eliminating the previous gatekeeper.

In sum, CBDCs deeply impact the architecture of financial control. Through the centralisation of all the transactions carried out with a certain currency in one ledger and the reallocation of the ledger to a public authority they sensibly expand the potential for State control.[68] The legal space of freedom remains the same, however, the architecture changes creating the potential for pervasive control. As underlined by the White House's Report on a U.S. CBDC[69] "*even if policies exist to prevent this harm at this time, enabling this capacity could allow a future Administration to use the CBDC system to surveil the population in close detail*".

As it is obvious, appraising this modification in the architecture of control is a political exercise.[70] Certain societies may view enhanced financial monitoring as a positive development allowing better control of corruption, tax evasion, etc.[71] Other political systems may be more cautious regarding the cost of control in terms of freedom. In European democracies, the unchecked expansion of State monitoring capabilities is certainly a primary concern.[72] This was confirmed by the public consultation on the Digital Euro carried out by the European Central Bank in 2021.[73] Respondents identified privacy as, by far, their primary concern. With 43 per cent of the respondents identifying privacy as the Digital Euro's most important feature, followed by security with only 18 per cent of the preferences.

A case study: the Digital Euro

The Digital Euro project: an introduction

With many central banks globally exploring, testing and launching CBDCs, the European Central Bank (ECB) had adopted, at least initially, a more cautious approach. Even though the ECB had been exploring the issuance of a digital version of the Euro for some years, with the first analysis already published in 2019,[74] it is only in the last couple of years that this work has gained significant traction with the launch of the "Digital Euro project".

The foundation of this project can be retraced to the first report on the Digital Euro published in October 2020.[75] The report sketches the fundamental framework of the future currency and underlines the key challenges towards its realisation. Furthermore, the report serves as a compass for regulators as it details fourteen key requirements that a European CBDC should abide by. These are high level principles that spell out the functions, characteristics and standards for the implementation of an EU digital currency. The report was followed by an experimentation phase aimed at testing the technical feasibility of the design choices identified by the Report.[76]

Following this initial "pilot" phase, the ECB embarked on a second, more structured, stage. The ECB's strategy was formalised in July 2021 when a twenty-four months

[68] N. Bilotta, *CBDCs and Stablecoins: The Scramble for (Controllable) Anonymity*, cit., 172.

[69] The White House, *Technical evaluation for a U.S. Central Bank Digital Currency system,* September 2022, 20.

[70] As recognised by then Deputy Governor of the Bank of Italy (now ECB's Board Member), "*just who should decide on the degree of anonymity associated with the use of a CBDC? Clearly, this is more than just a technical issue, and as such, the choice does not belong to central banks alone but also to the political sphere",* in P. Panetta, *Crypto-assets or virtual currencies as they were called before it was realised that they cannot perform the functions of money* in *SUERF Policy Notes*, 40 2018, https://suerf.org/policynotes/3251/21st-century-cash-central-banking-technological-innovation-and-digital-currencies.

N. Bilotta, *CBDCs and Stablecoins: The Scramble for (Controllable) Anonymity*, cit., 168. For an analysis of how different areas of the world perceive the regulation of the internet and digital technologies see, K. O'Hara—W. Hall, *Four Internets: the Geopolitics of Digital Governance,* in *CIG Papers no. 206*, 2018.

[71] K. O'Hara—W. Hall, *Four Internets: the Geopolitics of Digital Governance,* cit., 4, on the trade-off.

[72] See the results of F. Tronnier—D. Harborth—P. Hamm, *Investigating privacy concerns and trust in the digital Euro in Germany*, cit., 9.

[73] https://www.ecb.europa.eu//press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

[74] European Central Bank, *Exploring anonymity in Central Bank Digital Currencies,* December 2019. Already in 2016, the ECB launched, together with the Central Bank of Japan, the Stella Project. This, while not CBDC specific, is one of the first DLT experimentation by the ECB aimed at exploring new ways DLTs could innovate financial infrastructures and cross-border transactions, see European Central Bank—Bank of Japan, *STELLA—Synchronised cross-border payments*, June 2019, 1.

[75] European Central Bank, *Report on a digital Euro*, cit.; for more information on the project and all the relevant publications see https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html

[76] European Central Bank, *Digital Euro experimentation scope and key learnings,* 2021, 1.

investigation phase was launched by the Governing Council[77] and a (tentative) timeline was drawn.[78] According to this timeline, we might be just a few months away from the launch of the realisation phase—as the decision of the Governing Council is currently scheduled for the autumn of 2023.

In parallel with this technical effort by the ECB, the Commission has been working on the legislative groundwork needed to enable the launch of a European CBDC. Eminently, as underlined by the EuroGroup, "*the introduction of a digital euro as well as its main features and design choices requires political decisions that should be discussed and taken at the political leve*l".[79] To this end, the Commission is expected to adopt, in the second quarter of 2023, a proposal for a Digital Euro Regulation.[80] The Regulation, rooted in Article 133 TFEU, shall delineate the essential aspects and key design features of the currency and will provide to the ECB a political mandate for the issuance of the coin.[81]

We may, hence, be at the eve of the Digital Euro's launch. Once the political and the technical dimensions align, there will be virtually nothing in the way of its launch.

The recent European acceleration can be mainly connected to the arising public and private competition. The main driver of the ECB being that, in an increasingly cashless society, private (stablecoins) or public (foreign CBDCs) digital coins may significantly displace or even replace the Euro and European financial institutions.[82] As epitomised by the Lybra project, global tech companies could exploit their user base and network to substitute financial institutions and central banks. The same goes (even though, at least in the short term, to a lesser extent) for foreign CBDCs, with China in an advanced phase in the development and launch of its e-renminbi.

This scenario would have both economic and political effects. In the former sense, it would displace European companies in favour of global ones. Further, it would confer the control (and monetisation) of European financial data to global, foreign companies further expanding the, already existing, knowledge gap. In the latter sense, the widespread use of a private or foreign currency would affect European monetary sovereignty by significantly limiting the ability of the ECB to influence the money market. The Digital Euro therefore is conceived as a market-response to counter this trend so as to preserve monetary sovereignty and competitiveness.[83] At the same time, a CBDC is also seen as a means to further expand the strategic importance of the Euro in global markets.[84]

Even though several choices as to the design and features of the Digital Euro still have to be made, certain fundamental elements seem to be firm, at least so far.

First, the Digital Euro will be a liability of the Central Bank directly distributed to the general public to be used for retail transactions.[85] Second, the Digital Euro will rely on supervised intermediaries for user-facing activities including coin distribution. The ECB will solely retain control over the issuance and settlement of the currency with all other activities entrusted to private intermediaries.[86] Third, the Digital Euro is expected to be accessible also outside of the Euro area, even though certain restrictions will be imposed.[87]

According to our previous categorisation, the Digital Euro, as currently outlined, would then be a retail, non-synthetic, indirect and indifferent to geographical location CBDC.

[77] European Central Bank, *Eurosystem launches digital euro project*, July 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

[78] European Central Bank, *Digital Euro Project Timeline*, 2021, https://www.ecb.europa.eu/paym/digital_euro/shared/pdf/Digital_euro_project_timeline.en.pdf

[79] Eurogroup, *statement on the digital euro project*, 16 January 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/01/16/eurogroup-statement-on-the-digital-euro-project-16-january-2023/

[80] See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13392-A-digital-euro-for-the-EU_en

[81] See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13392-A-digital-euro-for-the-EU_en.

[82] See the continuous reference by European Institutions to strategic autonomy as the rationale for the introduction of the Digital Euro, see *ex multis* Eurogroup, *statement on the digital euro project*, cit.

[83] This strategy is paired with a more traditional policy response A clear example being the recently approved Market in Crypto-asset Regulation (MiCA) that provides for limitations to the possibility for private companies to issue stablecoins and even a veto power when such coins menace monetary sovereignty.

[84] As stated by European Central Bank, *Report on the Digital Euro,* cit., 9, "*A digital euro could be issued (i) to support the digitalisation of the European economy and the strategic independence of the European Union; (ii) in response to a significant decline in the role of cash as a means of payment, (iii) if there is significant potential for foreign CBDCs or private digital payments to become widely used in the euro area, (iii) as a new monetary policy transmission channel, (iv)) to mitigate risks to the normal provision of payment services, (v) to foster the international role of the euro, and (vi) to support improvements in the overall costs and ecological footprint of the monetary and payment systems*".

[85] European Central Bank, *Report on a digital Euro*, cit., 6.

[86] European Central Bank, *Progress on the investigation phase of a digital euro,* cit., 1-2, "*The Eurosystem has always made it clear that the digital euro should be available through supervised intermediaries"*; this same two-tiered approach had already been adopted in the first report on the matter see European Central Bank, *Exploring anonymity in Central Bank Digital Currencies,* 4, 2019, 4.

[87] See Requirement n. 6 of European Central Bank, *Report on a digital Euro*, cit., 14, "*The digital euro should be potentially accessible outside the euro area in a way that is consistent with the objectives of the Eurosystem and convenient to non-euro area residents"*.

The trade-off between privacy and traceability: the Digital Euro approach

With the realisation phase rapidly approaching, the next months will be crucial to understand how the privacy/transparency equilibrium will be struck. Privacy considerations should be at the core of the Digital Euro's architectural design, reflecting observance to fundamental rights enshrined by the EU Charter.[88] Nonetheless, the CBDC's technical features shall determine in what measure privacy shall be counter-weighted with control. The key decisions regarding monitoring will (and should) be made during the design phase of the Digital Euro. Eminently, for CBDCs monitoring is first and foremost an architectural problem. Once the potential for control is created through a certain architecture, *ex post* legislative limitations can only offer partial resort.

Perhaps the main privacy question currently faced by legislators, when considering CBDCs, is the degree of expansion of the State's monitoring potential irrespective of the legal framework. As underlined by the aforementioned White House Report, once the potential is created, nothing impedes future governments to exploit it. If and to what extent this possibility should be created is, hence, a matter of design much more than implementation. In this sense, unifying in a single ledger, entrusted to a public authority, most (and, potentially, in the future, all) financial transactions carried out in the Euro area are an architectural choice that requires strong guarantees and careful consideration.

The ECB has made, since its first steps in the field, privacy overtly a key topic in the Digital Euro's research. One of the fundamental requirements (R2) the Digital Euro should abide to—according to the first Report on the Digital Euro—is that it should have cash like features. This means "*a digital euro aiming to tackle a decline in the acceptance of cash should permit offline payments. Moreover, a digital euro should be easy for vulnerable groups to use, free of charge for basic use by payers and should protect privacy. It should have a strong European branding*".[89]

As an instrument that aims at becoming the digital doppelganger of cash, the question is how similar should the Digital Euro be to cash in terms of anonymity. This is also taking into account the differences between the two instruments in terms of AML risk profile. While anonymous, cash is always constrained by its physical dimension. To pay or stash, especially large sums, cash has to be transported and concealed. In contrast, the Digital Euro has the same characteristics of immateriality, volatility and globality of EFTS making the second (if equal anonymity was to be provided) much riskier than the first.

The ECB is quite clear in stating that the full anonymity guaranteed by cash will not be a viable option for a CBDC.[90] This is not only due to its potential for illicit use, but also as the lack of users identification requirements would prevent the ECB from imposing any limitations in the use of the coin.

The ECB seems to have lived a partial evolution in its approach to the topic. In its first paper, published in 2019, well before the Digital Euro project, the ECB had indeed explored the possibility for (at least nominally) anonymous payments. The paper, titled "Exploring anonymity in Central Bank Digital Currencies", proposed to create a voucher system that would give to each user a certain amount of anonymity voucher.[91] The vouchers would be time limited, non-transferable and would be issued, free of charge, at regular intervals. If the user wished to carry out an anonymous transaction, they had to attach the voucher to the transaction (one voucher for one coin) this way subtracting the specific transaction from the control of the AML Authority. Namely, it was the same paper that envisioned the introduction of an AML authority. The authority would have the duty to filter each and every transaction (except the anonymous one) with the power to either approve or reject them.

This first proposal seemed to be far from a satisfactory solution to the privacy problem. Namely, giving to a public authority the power to filter all financial transactions and to reject them generated (apart from feasibility doubts) a general *ex ante* control system. At the same time, the anonymity voucher system seemed far from anonymous. When a user spends an anonymity voucher, the only effect is that it circumvents the AML authority's filter. This, however, means the transactions are still registered (permitting *ex post* investigation and traceability) and visible to the intermediaries. Basically, the paper creates a previously non-existent control (*ex ante* filtering and approval by a public AML Authority) and then gives users a limited number of times they can circumvent it.

After this first more "creative" solution, the ECB seems to have gone back to the traditional model—where monitoring duties are completely entrusted to private intermediaries. This was clearly stated in the 2022 Digital Euro progress

[88] See, in particular, Articles 7 and 8 of the Charter.

[89] European Central Bank, *Report on the Digital Euro,* cit., 11.

[90] This was already stated by the European Central Bank, *Report on the Digital Euro,* cit., 21, and has been reiterated in European Central Bank, *Progress on the investigation phase of a digital euro*, cit, 7: "*full anonymity is not considered a viable option from a public policy perspective. It would raise concerns about the digital euro potentially being used for illicit purposes (e.g. money laundering and the financing of terrorism). In addition, it would make it virtually impossible to limit the use of the digital euro as a form of investment—a limitation that is essential from a financial stability perspectiv*e".

[91] European Central Bank, *Exploring anonymity in Central Bank Digital Currencies,* cit., 6.

report[92] "*in a baseline scenario, compatible with the current regulatory framework, a digital euro would provide a level of privacy equal to that of current private sector digital solutions. Users would need to identify themselves when they start using the digital euro, and intermediaries would perform customer checks during onboarding. Personal and transaction data would only be accessible to intermediaries for the purpose of ensuring compliance with anti-money laundering and combating the financing of terrorism (AML / CFT) requirements and relevant provisions under EU law*".

Notwithstanding the Bank's statements, the system would hardly correspond to the current architecture, wherein intermediaries perform AML checks and are the essentially the only entities having access to the ledger. The Digital Euro adds a new, overarching player: the central bank. As the latter would manage issuance and transactions, the ECB would necessarily need to have a certain level of control over the CBDC's ledger. Even though the identifying information would be stored by intermediaries, this does not change the fact that the Digital Euro's ledger would be much more intelligible (as would unify all transactions in a single ledger) and that the ECB would still have access to all transactions, even if in a pseudonymous fashion. While it is true that the ECB promises to design the Digital Euro "i*n a way that aims to minimise the Eurosystem's involvement in the processing of users' data*[93]" this does not change the fact that the infrastructure is there, the potential is created.

Probably conscious of this element, the ECB further states that "*the Eurosystem has no interest in exploiting individual payment data for any purpose. This stands in contrast to the monetisation of individual payment data by private companies*[94]*"*. This seems to represent a partial take on the problem of privacy. While it is true that central banks have no commercial interest in users' data, this does not mean they do not have any type of interest. Commercial interest is certainly not one of the primary concerns (or at least not the only) when dealing with monitoring. Immigration, politics, crime control, tax revenue are just some of the reasons why the public authority would want to access the Digital Euro's ledger. Some of the oldest and fundamental rules protecting private spaces safeguard the individual against intrusions of the State for reasons far from commercial. In this sense, stating that, since the Bank has no commercial interest in consumer data, the Digital Euro would guarantee a higher level of privacy, seems like a misrepresentation.

In this sense, the ECB needs to better clarify how it will guarantee that—if the legacy intermediary-centred model to financial monitoring is implemented—the Bank does not become a second monitoring layer built on top. At the same time, the ECB, if this model was to be implemented, should be clear in its public statements that, at least from a financial monitoring perspective, the Digital Euro is not digital cash, rather it is an EFTS system rooted in a public infrastructure. A clear communication of the risk profile associated with the Digital Euro is crucial to guarantee individuals can make informed decisions regarding their willingness to switch from cash to CBDC.

If intermediary-based transactions are the main transaction system, the ECB also envisions a second possibility: offline transactions.[95] Such transactions would be a complementary option envisioned for low value transactions. Their introduction is explicitly deemed further away in time so, probably, to be introduced after the launch of the Digital Euro. One of the reasons for its launch being the necessity to provide for a more private form of CBDC. An offline solution, as sketched in the reports, would probably work through a device funded by users. Once funded, the users would exchange the CBDC through close proximity exchange technology (which would limit the globality risk). This system would guarantee a higher level of privacy as the transactions would be peer-to-peer and the ledger would be stored individually by each device. To further limit the AML risk, quantitative limitations similar to the ones already in place for cash could be designed in the device both in terms of maximum holding and transaction.

This second offline solution would certainly represent a far better option in terms of privacy and, if paired with online transactions, could mimic the current equilibrium among cash and EFTS. At the same time, if correctly designed, an offline CBDC could guarantee higher compliance than cash in terms of quantitative limits as restrictions could be implemented by-design.

[92] European Central Bank, *Report on the Digital Euro,* cit., 21, and has been reiterated in European Central Bank, *Progress on the investigation phase of a digital euro,* cit., 7 and European Central Bank, *Progress on the investigation phase of a digital euro—second report*, 21 December 2022, 2.

[93] European Central Bank, *Progress on the investigation phase of a digital euro,* cit., 8.

[94] This same approach is reiterated in other statements of the ECB see F. Panetta, *A Digital Euro for the Digital Era*, Introductory Statement at the ECON Committee of the European Parliament, Frankfurt am Main, 12 October 2020, "*A digital euro would increase privacy in digital payments thanks to the involvement of the central bank, which—unlike private suppliers of payment services—has no commercial interests related to consumer data*".

digital euro would increase privacy in digital payments thanks to the involvement of the central bank, which—unlike private suppliers of payment services—has no commercial interests related to consumer data.

[95] European Central Bank, *Report on a digital Euro*, cit., 31; European Central Bank, *Progress on the investigation phase of a digital euro,* cit., 8; European Central Bank, *Progress on the investigation phase of a digital euro—second report*, cit., 9.

Institutional mandates and legal boundaries

With reference to the foundational principles of the Union, Article 128(1) TFEU has been correctly identified as one of the main legal sources for the issuance of CBDCs, since it establishes the competence for the Eurosystem to issue banknotes, without, however, circumscribing limitations as to its formal or operational characteristics. As pointed out by specialised literature, it stems from Article 128(1) TFEU that Euronotes could, in fact, be tangible or digital in format,[96] which entails that no major legal obstacle exists for the implementation of a digital EU currency. Such rules are complemented by the aforementioned Article 133 TFEU, which lays down the powers of the ECB, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, to establish the measures necessary for the use of the euro as the single currency.

As the choice of the indirect model for the Digital Euro seems solidified by now,[97] a two-tiered structure will allow intermediaries to continue being responsible for bearing the responsibilities in connection with providing interface solutions for end users (e.g. technology choice, data management, customer onboarding, screening and monitoring, etc.). This, naturally, implicates that ensuring regulatory compliance with AML/CFT obligations[98] should remain in the hands of the existing stakeholders, without major shifts in roles. Nonetheless, given that the scenario now expands to a digital environment, with a higher number of players and products, it is important to ensure that an alignment exists as to the obligations and responsibilities applicable to intermediaries of different categories that choose to transact Digital Euro or to provide services in connection with such transactions.

The Digital Euro Regulation should, in this sense, be able to establish a bridge not only between the Union's CBDC and the discipline of payment services under the PSD2[99] and the EMD2,[100] but also with the new digital finance legislation. Regarding the latter, while it is true that the MiCA Regulation carves out CBDCs from its scope of application,[101] the interrelationship between the governance of crypto-assets and that applicable to the Digital Euro, particularly from a financial integrity standpoint, but also from a licensing and conduct of business perspective, is still to be clarified. For example, the rules applicable to asset-referenced tokens (ARTs) as to supervision and enforcement of AML/CFT matters should be expected to be at least consistent with those applicable to the Digital Euro. The eventual case of interoperability—still largely unknown if at all feasible—between ARTs and the Digital Euro adds even further complexity to the matter and raises the bar with respect to the need for a comprehensive set of rules that is capable of ensuring a common ground for digital finance.

Most importantly, if EU legislators ultimately opt to allow for embedded features in the Digital Euro as to enable automated processes for AML/CFT routines, the limits and conditions to such exercises should be carefully set out. It is unclear which obligations are to remain in the hands of intermediaries and which will be—partially or entirely—automatised through RegTech and/or SupTech solutions: customer due diligence, suspicious transaction reporting and record-keeping and among the typical AML/CFT procedures that may be entrusted to automatisation, also to the benefit of end users.[102]

Finally, an institutional governance that strikes a balance between efficiency and accountability should also be a crucial point to be further delineated in the Digital Euro's design. As it stands, at least three major EU supervisors will have some level of competence over CBDC transactions, depending on the aspect to be covered: (i) concerning data protection, the EU Data Protection Supervisor (EDPS); (ii) for financial integrity, the new Anti-Money Laundering

[96] For a comprehensive analysis on the legal feasibility of the Digital Euro, see Grunewald, S., Zellweger-Gutknecht, C. and Geva, B., "Digital Euro and ECB Powers" (March 19, 2021). Common Market Law Review, Vol. 58(4), August 2021, 1029-1056. See also Zellweger-Gutknecht, C., Geva, B., Grünewald, S., "Digital Euro, Monetary Objects and Price Stability", 7 Journal of Financial Regulation 284, 2021; Nabilou, H., Central Bank Digital Currencies: Preliminary Legal Observations. Journal of Banking Regulation, 2019; Phoebus L. Athanassiou, Digital Innovation in Financial Services: Legal Challenges and Regulatory Policy Issues (Alphen aan den Rijn: Kluwer Law International B.V., 2018), Chapter 7.

[97] See ECB, "Progress on the investigation phase of a digital euro—second report", available at https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221221_Progress.en.pdf?f91e0b8ff8cbd6654d7e6b071a8f7071 (accessed 14 February 2023).

[98] See Bechtel, A. et al., "The Future of Payments in a DLT-based European Economy: A Roadmap", December 2020. See also ECB, "Roles of the Eurosystem and intermediaries in the digital euro ecosystem", 8 October 2022, available at https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov221003_businessmodels.en.pdf?fb8a6368c3206393ab66fd63e75bb3a6 (accessed 14 February 2023).

[99] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337 23.12.2015, p. 35).

[100] 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 (OJ L 267 10.10.2009, p. 7).

[101] See Article 2(2)(c) MiCA.

[102] See Mahari, R., Hardjono, T. and Pentland, A., "AML by design: designing a central bank digital currency to stifle money laundering", Mit Science Policy Review, 2022, available at: https://sciencepolicyreview.org/wp-content/uploads/securepdfs/2022/08/MITSPR-v3-191618003020.pdf

Authority (AMLA); and (iii) finally, the European Central Bank (ECB), as the monetary authority responsible for the issuance of the Digital Euro. To this structure, also the European Banking Authority (EBA) should have a role, given its mandate as a regulator of payment services and electronic money but also as a direct supervisor in the context of markets in crypto-assets. In addition, national authorities—either national data protection authorities, financial supervisors or FIUs—also bear responsibility for less significant institutions and national transactions, respectively.

This rather vast array of public authorities interested in the subjects or transactions involving the Digital Euro should have their mandates and roles made clear by the Digital Euro framework, in order to avoid an overlap of functions or an excessive burden to supervised entities. Moreover, ensuring their accountability, especially concerning digital privacy and data protection, is a major challenge to be addressed by the forthcoming Regulation.

The Digital Euro and the EU AML/CFT framework

On 20 July 2021, the European Commission presented a legislative package aimed at strengthening the EU's AML/CFT framework, comprising the following: (i) a proposal for a regulation establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)[103]; (ii) a proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing[104]; (iii) the VI Directive on AML/CFT, which is set to replace the existing Directive (EU) 2015/849[105]; and (iv) an amendment of the Regulation 2015/847 on the information accompanying the transfers of funds.[106]

Now that the package reaches its final legislative *iter* and is expected to come into force by the end of 2025, stakeholders are preparing to adapt to the new legislation. Among other changes, the new legislation foresees the inclusion of decentralised autonomous organisations (DAOs), non-financial tokens (NFTs) and DeFi platforms in the scope of "obliged entities", therefore being required to comply with AML/CFT rules, as long as they are controlled (directly or indirectly) by identifiable natural or legal persons; enhanced due diligence measures when enabling crypto-transactions worth more than 1000 EUR; cap payments in cash and crypto-assets, where the customer cannot be identified; and prohibition of anonymous crypto- and bank accounts.

According to the "Provisional Agreement Resulting from Interinstitutional Negotiations" of 5 October 2022 (2021/0241 (COD)), the co-legislators intended to extend the scope of the new EU Regulation on AML/CFT to transfers of crypto-assets. It also amends Directive (EU) 2015/849 to subject crypto-asset service providers (CASPs) to the same AML/CFT requirements and AML/CFT supervision as credit and financial institutions. These amendments automatically extend the scope of the existing Risk-Based Supervision Guidelines currently applicable to credit and financial institutions under that Directive. Following the imminent publication of the new package, the European Banking Authority (EBA) has launched a Consultation Paper on amending its Guidelines on the Risk-Based Supervision under Article 48(10) of Directive (EU) 20,157,849 (EBA/CP/2023/05), in order to include AML/CFT supervision of CASPs.

The link between AML/CFT and banking supervision is deeply rooted in the development of both silos of regulation. Ensuring proper AML/CFT safeguards relies upon an effective monitoring of suspicious financial transactions, which ultimately depends on building and maintaining solid governance structures, internal control systems and calibrated risk management procedures—elements essentially pertaining to prudential supervision.

While the task to investigate breaches on AML/CFT procedures and to carry out sanctioning procedures fall in the hands of FIUs, the ECB shall also act upon AML/CFT issues that may impact on the soundness of the intermediaries' internal structures. Breaches of AML/CFT provisions can, therefore, justify the withdrawal of a credit institution's banking license. Not by chance, the proposal for a regulation establishing the AMLA foresees that it will "*be entrusted to develop guidelines in coordination with the ECB, the European Supervisory Authorities (…) in cooperation between all competent authorities*".

It also states in Recital (59) that "*To improve cross-sectoral supervision and a better cooperation between prudential and AML/CFT supervisors the Authority should also establish cooperative relations with the authorities competent for prudential supervision of financial sector obliged entities, including the European Central Bank with regard to matters relating to the tasks conferred on it by Council Regulation (EU) No 1024/2013* (…)".

Such juxtaposition of competences and collaborative efforts naturally poses issues to the proper demarcation of powers and responsibilities of such EU Institutions and Agencies. Theoretically, central banks (such as the ECB and NCBs), depending on their relations with end users in the Digital Euro's design, could be bound to the same legislation applicable to other market participants with respect to AML.

[103] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0421.

[104] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420.

[105] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420.

[106] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422.

This would create a responsibility to these public institutions regarding AML/CFT compliance, authentication, fraud prevention, etc. Even though theoretically possible, it seems unlikely that this type of burden will be imposed on public EU institutions, as the Digital Euro's design is indirect and decentralised and will probably keep such obligations in the hands of intermediaries. Nonetheless, the role and accountability of the ECB and NCBs for financial integrity and data protection purposes, especially in coordination with other public stakeholders and private players, shall be carefully designed.

The ECB has already expressed that the Digital Euro would comply with AML requirements applicable to the financial system, even though central bank liabilities would not be subject to regulation and oversight.[107] A precise understanding of how current AML/CFT legislation will apply to the Digital Euro, however, requires a concrete analysis of the proposed Digital Euro Regulation *vis-à-vis* the new EU AML/CFT package and other pieces of existing laws and regulations, including the MiCA Regulation, as to ensure a coherent and consistent framework throughout EU legislation applicable to digital finance.

Conclusions

CBDCs represent the next step in the evolution of the currency. In a pervasively digitised financial environment, it was just a matter of time before analogical *fiat* currencies were substituted, or at least complemented, by a digital *fiat* currency. Given the telluric reach of such an innovation, the introduction of a CBDC raises various fundamental concerns spanning from financial stability to bank runs.

The present paper has focused on one of such concerns: the trade-off between financial integrity and monitoring, which touches upon the delicate balance between increasing security and preserving freedom. The digitalisation and unification of a currency's financial ledger would deeply impact such a trade-off. A CBDC would provide an unprecedented data source for the monitoring of retail transactions, hence extending the architectural potential for monitoring. Furthermore, the direct connection such a digital currency would create between central banks and the source of the information (i.e. the financial ledger) would disintermediate the relation between State authorities and financial flows. While public monitoring would still be limited by legal constraints, such an architectural modification creates a new potential for monitoring that should be explicitly acknowledged and addressed by the regulator, including for the purposes of identifying and structuring accountability mechanisms for public actors.

In such a context, the design phase of CBDCs is of particular importance, as it allows jurisdictions to broadly discuss how to best structure this new means of payment in view of the principles and values safeguarded by their legal system. The concrete impact of a CBDC on the financial integrity infrastructure will be, thus, ultimately linked to the specific design choices adopted by each jurisdiction.

In this sense, the ECB's proposals on the Digital Euro seem to lack the necessary awareness regarding the monitoring effects connected with the introduction of an EU CBDC. While privacy is clearly on the highest concerns of European stakeholders, the latest proposals by the ECB do not clearly acknowledge the negative effects that enhanced monitoring a Digital Euro would allow and do not offer convincing solutions as to the balancing of holding limits, anonymity and AML/CFT concerns.[108] In contrast, the ECB seems to have embraced a rhetoric that a Digital Euro would be good for privacy as it would transfer the control over data from corporations to the central bank. Given the telluric shift a CBDC would cause, this does not seem enough. On a legislative sphere, it is still worrying unclear how the Digital Euro Regulation will intersect with existing laws and regulations governing digital finance and AML/CFT in the Union. Finally, on an institutional level, the overlapping of a myriad of different public authorities and mandates which could, at least potentially, be involved in the Digital Euro initiative, raises significant doubts as to the roles, duties and responsibilities pertaining to each stakeholder. It is now up to the co-legislators, as part of the negotiations regarding a CBDC's Regulation, to understand how and where to draw the lines.

Funding Open access funding provided by Luiss University within the CRUI-CARE Agreement.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

[107] ECB, *Report on a digital Euro*, cit., Requirement 10.

[108] On the specific issue surrounding holding limits, see M. Warren, "Let the Digital Euro Circulate: Introducing a Retail C.B.D.C. in the Eurozone With Unlimited Holdings by Users", *University of Bologna Law Review,* Vol. 8, Issue 1, 2023.