THE AML/CFT IMPLICATIONS OF CENTRAL BANK DIGITAL CURRENCY AND THE DIGITAL EURO

FINANCIAL INTELLIGENCE UNIT OF LATVIA

Financial Intelligence Unit

AMLIH

1. Executive Summary

Central bank digital currency (CBDC) offers the next step in the evolution of finance. Generally understood as a central bank liability delivered in digital form, CBDC is envisioned to be used alongside existing cash notes and electronic payments. Programmable currency, retail bank accounts at central banks, and discreetly traceable digital money are just some of the ways CBDC can fundamentally redefine the existing banking and payment paradigm. These changes have important implications for financial integrity and economic crime resilience, creating both opportunities and challenges.

This study examines the impact of CBDC on anti-money laundering (AML) and other financial integrity and economic resilience outcomes, focusing on the digital euro project. To interface with AML, the study establishes a taxonomy of CBDC. Different operating models are considered based on the account or token-based form of CBDC, wholesale or retail access, remuneration mechanics, distribution, and utility with other payment systems. Design features like privacy and level of programmability are also explored.

The taxonomy is referenced against the indicated expressed preferences of various stakeholders to create the characteristics of the digital euro. The study analyzes a variant of the digital euro that is intermediated by commercial banks, focused on retail consumers, and has cross-border utility. This variant would also allow a level of money programmability.

The study finds that depending on the design choices of the digital euro, AML systems may be significantly strengthened, but may also encounter new technologically sophisticated risks. The digital euro may accelerate access to and retention of identity and transaction information, especially if the information is centralized at a central bank. However, as a new financial product, the digital euro may create new risks, or exacerbate existing delivery channel, product and service, customer, and geographical risks.

Several design choices are particularly important to ensuring better AML outcomes, while securing the benefits offered by CBDC. Programmability and privacy choices are examples of options that may provide important mitigating measures to new AML risks, by ensuring authorities have access to proper and timely data.

The study concludes by emphasizing the need to involve all stakeholders in the review of legal, technical, and institutional preconditions of the digital euro. It is especially important that all relevant AML authorities, including financial intelligence units law enforcement are included in ongoing discussions to ensure that AML and other similar policy goals are not jeopardized, but empowered.

Table of Contents

2. Introduction

CBDC are what many in the financial services sector view as the next innovation in money. Generally understood as a central bank liability delivered in digital form, CBDCs have a number of benefits that complement the existing cash note and wholesale central bank reserves. These include promoting the digitalization of economies, advancing monetary and fiscal policies, and expanding financial inclusion.[1] Several central banks are already testing a CBDC, and at least 87 countries—representing over 90% of global GDP—are exploring a CBDC solution.[2] Among these groups, is the European Central Bank (ECB), which has launched the investigatory phase of its CBDC, the digital euro project, and expects to complete it in 2023.[3]

While not finalized, several functional preferences are evident for the digital euro. From the outset, the digital euro seeks to be a retail currency, thus expanding the availability of CBDC beyond its wholesale use.[4] It aims to be programmable, to allow intermediaries to offer their services based on the digital euro.[5] It needs to consider offline usability to support financial inclusion, ensure the highest standard of privacy for users, and be maximally integrated with existing financial and payment systems in the Euro area.[6]

However, the digital euro is at the intersection of many different policy priorities. It is linked to the objectives generally attributed to central banks: price stability and financial stability.[7] It affects questions of data governance, like privacy and localization. Most pertinently, it also directly interacts with financial integrity objectives, including anti-money laundering, counter-terrorism financing, proliferation financing, and sanctions evasion prevention (AML/CFT/CFP).[8]

This study focuses on the financial integrity and economic crime resilience aspects of CBDC, and the digital euro. Like any new technology, CBDCs bring risks and opportunities. Distributing a digital euro could provide a seemingly "golden source" for identifying the origin and use of funds across a broad range of retail transactions. The potential of collecting additional data attributes on transactions in a controlled and safe manner, promotes improved effectiveness of AML obliged entities, financial intelligence units (FIUs), and law enforcement agencies (LEAs) to detect, identify, prevent, and ultimately combat tax evasion, money laundering (ML), terrorist financing (TF), and sanctions evasion.

---

[1] Raphael Auer, Jon Frost, et al., "Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier," November 4, 2021, https://www.bis.org/publ/work976.htm

[2] In fact, scholars note that "central banks collectively representing a fifth of the world's population are likely to launch retail CBDCs in the next three years." See Codruta Boar and Andreas Wehrli, "Ready, Steady, Go? - Results of the Third BIS Survey on Central Bank Digital Currency," BIS Paper (Bank for International Settlements, January 2021), https://econpapers.repec.org/bookchap/bisbisbps/114.htm

3 Christine Lagarde and Fabio Panetta, "Key Objectives of the digital euro," July 13, 2022, https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html

4 Lagarde and Panetta

5 Lagarde and Panetta

6 Lagarde and Panetta

7 Charles M. Kahn, Manmohan Singh, and Jihad Alwazir, "Digital Money and Central Bank Operations," International Monetary Fund, May 6, 2022, https://www.imf.org/en/Publications/WP/Issues/2022/05/06/Digital-Money-and-Central-Bank-Operations-517534

8 For the sake of brevity, this paper will refer to the different forms of money laundering and financial and economic crimes as "AML," unless otherwise specified.

However, the digital euro and CBDC may create unintended consequences. These may be new opportunities for exploitation by nefarious actors. The coexistence of the digital euro with other payment methods may lead criminals to revert to utilizing cash instead of digital banking. The range of programmability of the digital euro may lead to exploitation of the CBDC's digital customizability. Different data analytics capacities, cross-border data exchange agreements, and even domestic inter-institutional data access levels can lead to divergent supervisory outcomes. Each of these considerations is directly applicable to effective financial intelligence and law enforcement.

The structure of this paper is as follows: First, an introduction will elaborate on the taxonomy of CBDC, situating it among other forms of digital money. Second, the main CBDC model options will be examined. Third, the prevalent CBDC design choices will be explored. Fourth, the indicated preferences of the digital euro will be outlined. Fifth, the AML/CFT/CFP considerations of the digital euro will be assessed, followed by a discussion on the way forward.

3. Methodology

This report draws on a variety of literature from academic and institutional sources to develop a taxonomy and conceptual framework of CBDC. The works published by the main stakeholders, like the Financial Action Task Force (FATF), ECB, Federal Reserve, BIS, and IMF are particularly important in this regard. The preferences for the digital euro are drawn from sources like the ECB and its Governing Council members. The findings of this preliminary study draw on proposals that are subject to change. The examined operation models and features will develop as the digital euro project progresses and may have to be re-examined.

4. CBDC Taxonomy

CBDC is one of several newly proposed innovations that involve the electronic storage and use of monetary value. Though CBDC shares a space with other digital financial payment technologies and services like electronic money (e-money)[9] and stablecoins),[10] it is a distinct novelty.[11] Defined by the Bank for International Settlements as "a digital payment instrument, denominated in the national unit of account, that is direct liability of the central bank," CBDCs are the next generation of public money.[12]

The exact contours of CBDC will differ based on the central bank issuer. Generally, however, retail CBDC coexists with existing payment solutions – similarly to retail current accounts at a commercial bank, they are easily accessible and hold value. It is different, because the CBDC electronic account is, directly or through an intermediary, backed by a central bank liability and has legal tender status. While virtual assets like cryptocurrency and CBDC are both tokens, in the sense that they represent stored value (similar to cash), a CBDC does not necessarily need to utilize distributed ledger technology, such as blockchain, as a means of verification.[13]

---

[9] E-money refers to debt-like instruments that an entity issues on receipt of funds for the purpose of facilitating payment transactions. It is generally an electronic store of monetary value on a prepaid card, electronic device - often a mobile phone - that may be widely used for making payments. It is a fixed value claim on the balance sheet of the entity issuing it and is not considered legal tender. From a risk perspective, the guarantee of redeemability at face value is backed only by the e-money issuer to e-money holders, and is thus prone to credit risk, liquidity risk, and market risk. E-money is used as an attractive means of payment because of its convenience, but because it is supported only by the E-money service provider and the network of users supporting this e-money, it needs to be purchased with some form of value (like cash or deposits). These are services generally offered by non-banks, and examples include the M-PESA in Kenya, or web-based services like PayPal. For a deeper exploration of e-money, see Johannes Ehrentraud et al., "Fintech and Payments: Regulating Digital Payment Services and e-Money," July 5, 2021, https://www.bis.org/fsi/publ/insights33.htm; ECB, "Electronic Money," ECB, November 16, 2016, https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html; José Garrido and Jan Nolte, "Making Electronic Money Safer in the Digital Age," *IMF Blog* (blog), accessed August 22, 2022, https://blogs.imf.org/2021/12/14/making-electronic-money-safer-in-the-digital-age/

[10] Virtual assets are digital representations of value that can be digitally traded, transferred or used for payment. They do not include the digital representation of fiat currencies. Stablecoins are virtual assets that "purport to maintain a stable value relative to some reference asset or assets" and the term is not a distinct or regulatory classification. See Financial Action Task Force, "Virtual Assets: What, When, How?," EASY GUIDE TO FATF STANDARDS AND METHODOLOGY, 2020, https://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf; Financial Action Task Force, "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins," June 2020, 20, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf

[11] Board of Governors of the Federal Reserve System, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," January 2022, https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

[12] There are a variety of definitions of CBDC, and the definition will likely be different depending on the design choices made. The FATF, for example, has defined CBDC as "a digital form of central bank money that is different from balances in traditional reserve or settlement accounts." The US Federal Reserve has defined them as "digital liabilities of the central bank that are widely available to the general public," The Committee on Payments and Market Infrastructures define a CBDC as a "digital form of central bank money that is different from balances in traditional reserve or settlement accounts." The ECB has defined it as a "central bank liability that is made available to individual citizens in digital form." See Financial Action Task Force, "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins"; Board of Governors of the Federal Reserve System, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation"; Central bank digital currencies, "Central Bank Digital Currencies," March 12, 2018, https://www.bis.org/cpmi/publ/d174.htm; Fabio Panetta, "Central Bank Digital Currencies: Defining the Problems, Designing the Solutions," https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220218_1~938e881b13.en.html

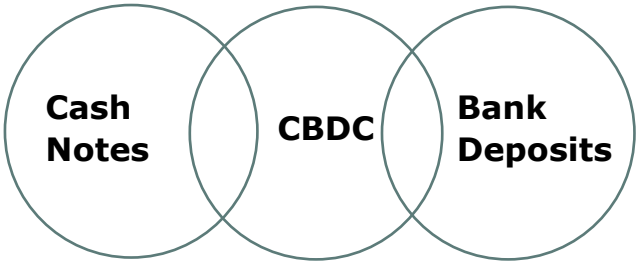
[13] An important distinction between token- and account-based money is the form of verification needed when it is used. Token-based money depends on the ability of the money itself to be validated, such as cash banknotes not being counterfeit, or an electronic coin being genuine, and noting whether it has already been spent. Account-based systems depend on the ability to verify the owner of the account, this is how general retail accounts at banks work. See Benoît Cœuré and Jacqueline Loh, "Central Bank Digital Currencies," n.d., 34

Unlike CBDC, cryptocurrency does not provide claims against a central bank, but against an entity (or its cash, flows, assets, residual value, etc.).[14]

CBDC aims to change the payment paradigm. For many decades, central banks have provided the monetary base through two channels: (1) cash for individuals, and (2) central bank reserves for financial institutions, generally referred to as public money. The private sector has offered its own payment solutions based on commercial bank money (also known as private money), such as deposits, or bank liabilities, which are typically not legal tender. Monetary policy and, at times, fiscal stability are contingent on the backing of private money by public money. It is thus the third form of money alongside central bank cash and "book money," created by commercial banks.

Most of the money circulating in the economy is private money belonging to commercial banks, and to a lesser degree, non-bank money.[15] For instance, having money in a commercial bank functions as a claim against the bank. The majority of transactions made today via payment service providers (like PayPal), debit and credit card payments, and bank wire transfers constitute obligations of one party to another. Though merchants, banks, and payment processing companies accept these digital payments at the point of sale, there is a separate process that settles obligations and balances the accounts represented in transactions.[16] As the claim of a money owner is not against the central bank, but against the commercial bank, they are subject to a variety of liquidity and credit risks from that money being fractionally backed, or backed only in part, by central bank assets and lender-of-last resort facilities.[17]

Figure 1. CBDC as a Mix of Cash and Bank Deposits



Source: Author

Unlike the private money of commercial banks, CBDC is a direct claim on the central bank. Central bank money can be issued as needed, carries neither credit nor liquidity risk, and is thus considered the safest form of money. By bringing CBDC directly to the public, the dependence on private money supply chains can be

[14] Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion.," Website (Publications Office of the European Union, September 6, 2018), http://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1

[15] Commercial bank money is the digital form of money generally used by the public and retail consumers. Commercial bank money is held in accounts at commercial banks. Non-bank money is digital money held as balances at nonbank financial services providers. These firms typically conduct balance transfers on their own books using a range of technologies, including mobile apps. See Board of Governors of the Federal Reserve System, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation"

[16] This is why electronic fund transfers can take multiple days to deposit into bank accounts. These crediting, debiting, and settling processes involving digital payments are also the source of fees charged by payment processors and banks. See Yaya Fanusie, "Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them" (A Lawfare Paper Series, November 2020), https://s3.documentcloud.org/documents/20423765/fanusie-dsc-final-2.pdf

[17] Kahn, Singh, and Alwazir, "Digital Money and Central Bank Operations"

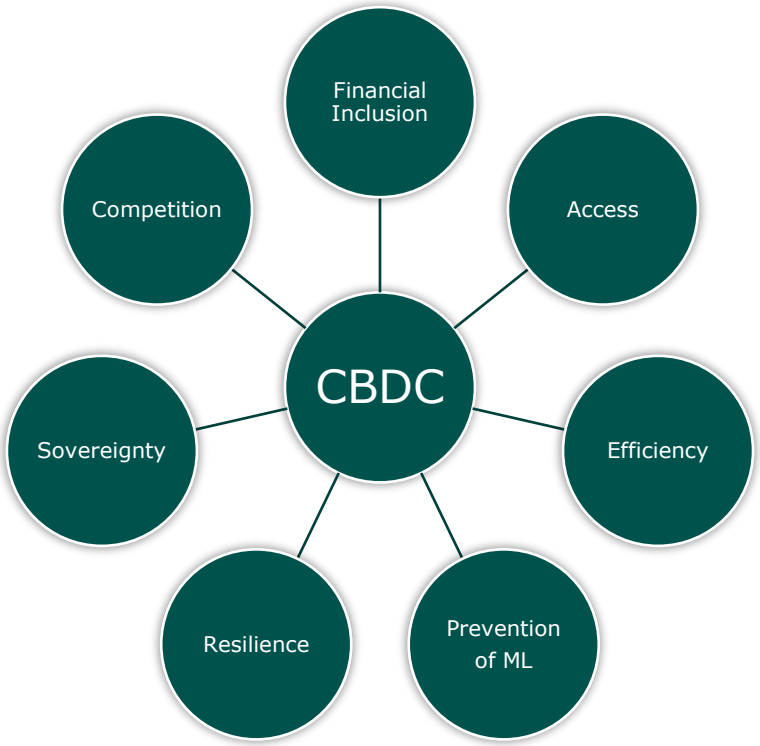
circumvented to reach a variety of policy goals. Monetary policy decisions such as interest rate changes, for example, can immediately reach the public, instead of having to pass through commercial banks.

There are a variety of rationales for developing a CBDC. A study of several jurisdictions that have launched CBDC projects finds a common denominator among seven overarching policy goals.[18] The most common goal is increasing payment efficiency. Especially in countries where the use of cash and checks is high, the operational costs of digital payments are elevated and at times cost prohibitive. CBDCs may be a way to increase the diversity of payment systems by providing a common means of transferring money between systems.

Efficiency intersects with other goals aimed at internal market development. Access to financial payments is limited in cash-heavy sectors, and financial inclusion concerns ensuring financial services to the unbanked. Competition would be increased, for example, by CBDC competing with existing forms of payment, or by being designed as a platform open to private payment service providers with a low barrier of entry.

The last set of goals aim to provide systematic protection to payments. The resiliency of payment infrastructure is a concern in highly digitalized jurisdictions and where payments are concentrated among a few large operators. Monetary sovereignty would also be a protection mechanism against the risks associated with adopting foreign digital currencies or global stablecoins. This also includes the aim to reduce the illicit use of money, especially cash, which is inherently anonymous and lacks audit trails.

Figure 2. Core features of CBDC



Source: Author adapting The Bank of Canada et al.[19]

[18] The Bank of Canada et al., "Central Bank Digital Currencies: Foundational Principles and Core Features," October 9, 2020, https://www.bis.org/publ/othp33.htm

[19] The Bank of Canada et al.

Depending on the policy goals of the CBDC, it can potentially bring a range of benefits.[20] Among others, it can provide households and businesses with safe and convenient electronic central bank money, thus supporting faster and cheaper payments and increasing financial inclusion. CBDC can enhance payment system competition, efficiency, and resilience in the face of increasing concentration among a few large companies.[21] CBDC provides new monetary and fiscal levers for governments and central banks. The adoption of CBDC could be used by central authorities to advance fiscal policy and enhance macroeconomic projections by using the granular payment flow data associated with its digital nature. Through programmability, it is also a way to generate more functional data from the use of money, while also ensuring a high-level of data protection by siloing data at central banks.[22]

However, CBDC also poses risks. The transmission of monetary policy could be affected in unpredictable ways, as CBDC would change the demand for base money and its composition, as well as the sensitivity to interest rates. It could also affect financial stability and banking intermediation if it competes with commercial bank deposits. Banks may also increase their reliance on wholesale funding, affecting funding costs, stability, and market discipline. CBDC issuances may also change central bank balance sheets depending on conversion modality, disintermediating commercial banks.[23] It also creates new sources of data that need to be protected from both cybersecurity intrusions and unauthorized access to personal information.[24]

[20] John Kiff et al., "A Survey of Research on Retail Central Bank Digital Currency," IMF, June 26, 2020, https://www.imf.org/en/Publications/WP/Issues/2020/06/26/A-Survey-of-Research-on-Retail-Central-Bank-Digital-Currency-49517

[21] Board of Governors of the Federal Reserve System, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation"

[22] Toni Ahnert, Peter Hoffmann, and Cyril Monnet, "The Digital Economy, Privacy, and CBDC," *Working Paper Series*, Working Paper Series (ECB, May 2022), https://ideas.repec.org/p/ecb/ecbwps/20222662.html

[23] Ramón Adalid et al., "Central Bank Digital Currency and Bank Intermediation," SSRN Scholarly Paper (Rochester, NY, May 1, 2022), https://doi.org/10.2139/ssrn.4108346

[24] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no. 2 (June 2016): 442–92, https://doi.org/10.1257/jel.54.2.442

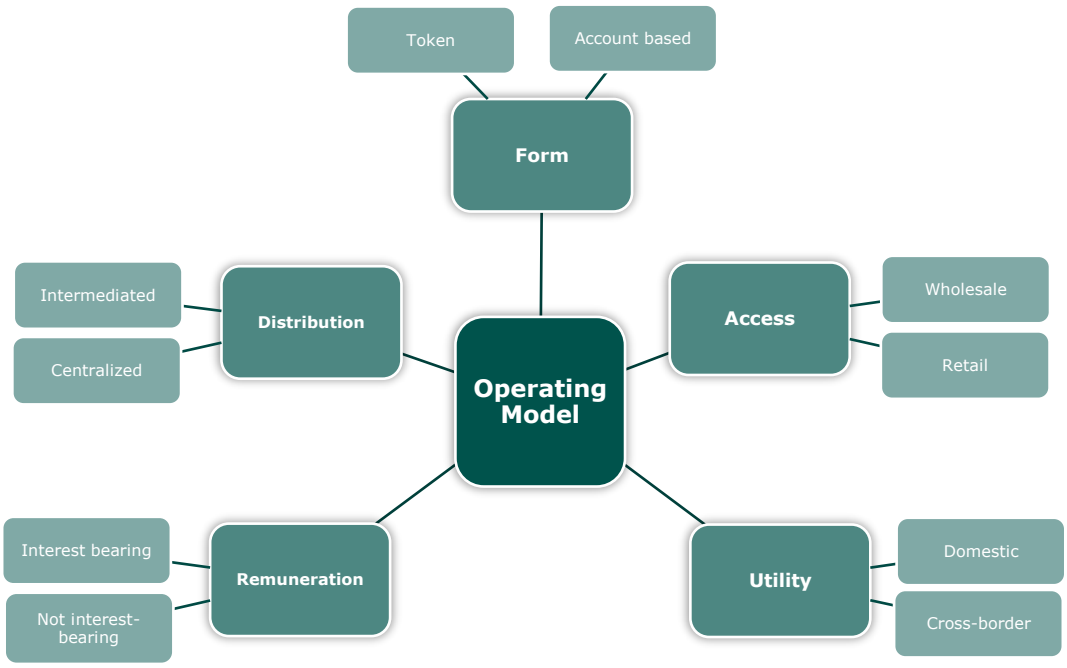
5. CBDC Models

Differences in policy objectives have resulted in broad variety of CBDC projects. They subsequently envision many different contours for operating models and design decisions. However, the Group of Seven Central Banks proposes three foundational principles for CBDC:[25]

1. **Do no harm to wider policy objectives.** CBDC should continue supporting the fulfillment of public policy objectives and not interfere with the ability to carry out mandates.
2. **Ensure the coexistence and complementarity of public and private forms of money.** CBDC should ensure that they do not interrupt the broader money and payment ecosystem.
3. **Promote innovation and efficiency.** CBDC should aim to foster innovation and competition for both public and private agents.

These principles generally guide the overall development of CBDC in the many jurisdictions, including the Eurosystem, where it is still under development. However, five main considerations have emerged regarding the broader operating models of CBDC: (1) form, (2) remuneration, (3) access, (4) utility, and (5) distribution.

Figure 3. Key Modelling Decisions in CBDC



Source: Author adapting Popescu[26]

[25] More information on the Core features can also be found here: see The Bank of Canada et al., "Central Bank Digital Currencies"

[26] Adina Popescu, "Cross-Border Central Bank Digital Currencies, Bank Runs and Capital Flows Volatility," IMF, May 6, 2022, https://www.imf.org/en/Publications/WP/Issues/2022/05/06/Cross-Border-Central-Bank-Digital-Currencies-Bank-Runs-and-Capital-Flows-Volatility-517625

Form

The first set of considerations is whether a CBDC should be account or token-based. Token-based CBDCs function similarly to currency, with the exception that they take the form of cash cards or electronic wallets that may enable peer-to-peer (P2P) payments. Account-based CBDCs are deposits envisioned to be held in a central bank account. Account-based CBDCs also enable the verification of users identities in the payment system. The decision on form can also determine the level of programmability that the CBDC carries, as token-based electronic money is innately created using programming languages, unlike centralized ledger-based balances in purely account-based CBDC. A hybrid of both is also available, whereby a bank account would function as account-based with the added functionality of token-based CBDC.

Access

The second consideration concerns access to CBDC. Access to the wholesale market, meaning financial institutions or operators of payment systems, would limit users to a set of predefined user groups, typically banks and other members of the national payment systems.[27] The other option is to allow the broader public, known as retail consumers, to access money.

Remuneration

The third consideration regards remuneration. Designing account-based CBDCs that pay interest rates in line with current monetary policy objectives would enable the central bank to directly influence price stability or otherwise stabilize the business cycle. A remunerative CBDC could provide a channel for implementing negative rates or "helicopter money." It also warrants a discussion about a tiered remuneration system, where the potential structural and cyclical bank disintermediation that might take place when introducing a CBDC can be addressed by differentiating remuneration according to the amount held, bringing remuneration to zero for holdings of CBDCs above a certain threshold.[28]

Utility

The fourth consideration is the utility of CBDC. Authorities must decide the extent to which their CBDCs are interoperable with payment systems available in other jurisdictions. Such arrangements can be a useful method to ease the burdens of making cross-border payments by reducing transaction fees and the need for correspondent-banking relationships, increasing the speed of transactions, and creating direct traceability of payments.[29] There are three conceptual models of a "multi-CBDC" (mCBDC) arrangement. The first model enhances the compatibility between multiple systems by ensuring compatible technical, regulatory, and coordinated identification schemes. The second paradigm is the interlinking of shared technological interfaces, with mutually accepted identification standards. The third model is the integration of various CBDCs into a single platform, where identification schemes are mutually recognized. But because mCBDC projects are so complicated, the first step might also be a domestic restriction.

Distribution

The last consideration is the distribution model. The distribution model determines how CBDC is issued and distributed to running user models. There are three

[27] Kiff et al., "A Survey of Research on Retail Central Bank Digital Currency"
[28] Ulrich Bindseil, "Tiered CBDC and the Financial System," Working Paper Series (ECB, January 2020), https://ideas.repec.org/p/ecb/ecbwps/20202351.html
[29] Raphael Auer, Holti Banka, et al., "Central Bank Digital Currencies: A New Tool in the Financial Inclusion Toolkit?," April 12, 2022, https://www.bis.org/fsi/publ/insights41.htm

conceptual distribution models determining the main interlinkages between central banks, commercial banks, and retail end users.[30] In a unilateral model, the central bank issues CBDC and performs all functions, including directly interacting with end users. In this model, the central bank functions independently of commercial banks, potentially sharing payment initiation services with non-central bank institutions.

The second model is intermediated, and in this model the central bank issues money but delegates functions to other intermediaries, like commercial banks, who interact with end users. This model resembles the traditional division of competences where intermediaries like commercial banks can aid in the distribution of CBDC to retail end users, while also overseeing payment and customer identification. The third model is synthetic CBDC, whereby non-central bank actors can issue money that is backed by central bank assets that they require from the central bank. This variant may be useful to run a token-based CBDC if the goal is an elevated level of privacy, where no party has full oversight over the movement of the token.

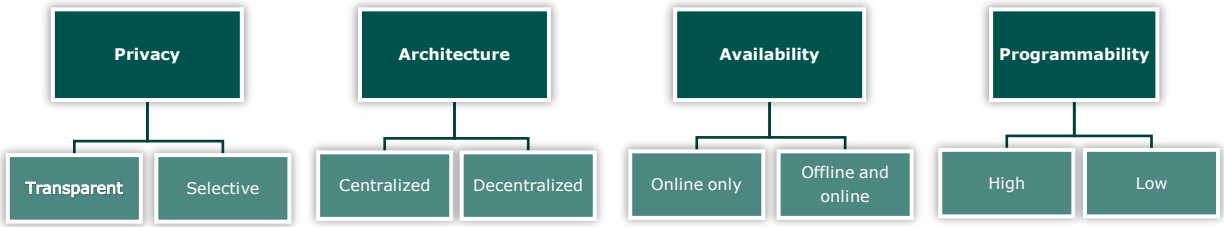
[30] Auer, Banka, et al.

6. CBDC Design Features

Alongside the core properties, there are other design features that determine the scope of utility the CBDC provides.[31] There are also secondary design choices on controls, technical design, and the technological toolkit used.[32] These design decisions are not exhaustive, and other aspects can also dynamically become important depending on jurisdictional priorities and the operating model and design feature mix.

Four key dimensions are particularly important to the functionality of CBDC. They are also capable of significantly mitigating or exacerbating existing and emergent ML/TF and sanctions evasion threats. Record-keeping architecture, privacy features, and other design choices directly impact the ability of financial intelligence units and broader law enforcement, and other stakeholders to trace and audit transactions and uncover illicit financial flows.

Figure 4. Key Dimensions in CBDC Design



Source: Author adapting Popescu

Privacy

The design feature of privacy regards a spectrum of options for how and what information on CBDC transactions and other exogenous factors are collected and used.[33] On one end is the choice of full transparency, which follows the current banking paradigm with e-money. Commercial banks have access to a broad range of information regarding information on transactions, balances, loans, and personal information.[34] Various metadata, like the IP address of received payments, may also be available in a transparent privacy mode.

Selective privacy can require that commercial and central banks managing the accounts and transactions do not have access, or even allow the collection of, a variety of data. Such an option may apply to low-value payments, with required customer checks performed during onboarding. Still, a higher degree of privacy, or even anonymity, could be ensured for low-value and low-risk payments. This decision would aim to emulate the near anonymity offered by cash in CBDC. Depending on the technology utilized, users may be able to select the extent to which they are willing to share their data with counterparties, the central or non-central banks.[35]

[31] Cœuré and Loh, "Central Bank Digital Currencies"
[32] The Bank of Canada et al., "Central Bank Digital Currencies"
[33] The Bank of Canada et al.
[34] Ahnert, Hoffmann, and Monnet, "The Digital Economy, Privacy, and CBDC"
[35] Ahnert, Hoffmann, and Monnet

Architecture

The control of accounts, verification of identities and access to data are the subjects of CBDC architecture.[36] Central banks do not traditionally maintain accounts for natural or legal persons in the retail market, and the task is generally delegated to commercial banks.[37] This would exemplify an intermediated format, whereby central banks would delegate account management to a commercial bank, which would also conduct AML/CFT/CPF functions and identity verification. In this model, the central bank still has accounts with retail individuals, but through commercial banks. In a centralized system, identification verification and account management would be handled by the central bank.

Similarly, there are three types of systems that can be utilized for transaction data storage.[38] In the current hybrid system, commercial banks keep their own records of customers and transactions. Transfers between central bank reserve accounts are used to settle cross-bank transactions. The central authority, which might be the central bank or another authority, would verify and update the single record of all the transactions that have taken place in a fully centralized format. On the other hand, in a fully decentralized variant, every financial institution has its own record of the entire chain of all transactions, which are cross-verified and updated through a distributed process. This decentralized storage variant can usefully utilize distributed ledger technology, like the blockchain.

Availability

Availability refers to the ability to utilize CBDC online, connected to a ledger on the internet, or offline. It is technically possible to verify the availability of funds and validate transactions without the need to interact with the online ledger, as has been done with non-internet-driven mobile phones or a prepaid card, which are funded in advance. The online variant of CBDC represents the existing mainstream use of e-money, whereby transactions are processed through an online process, in which transaction data is transferred via a payment gateway to the merchant's payment processor, which transfers info to the card or issuing bank, and reverses the information flow after assessing whether the transaction is legitimate and funds are available.

Along with the traditional online use of e-money, users could also choose to pay offline. To ensure financial integrity goals are met, offline devices should carry on-device analytics or undergo periodic synchronization with trusted verification services (like turning on a smartphone and interacting with the online bank), to control for transaction limits or other factors.[39]

Programmable Money

A CBDC can decide to allow for different levels of money programmability. Programmable money is understood as a digital form of money that users can program to follow an inherent logic for a predefined purpose, using the attributes of the digital money.[40] Programming allows payments to be managed algorithmically by smart contracts. Smart contracts are computer programs

[36] Sarah Allen, Srdjan Capkun, and Ittun Eyal, "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," July 2020, https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf
[37] Allen, Capkun, and Eyal
[38] Allen, Capkun, and Eyal
[39] Kiff, "Taking Digital Currencies Offline," IMF, accessed August 22, 2022, https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline
[40] Deutsche Bundesbank, "Money in Programmable Applications Cross-Sector Perspectives from the German Economy," December 2020, https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf

intended to automatically execute actions according to the terms of a contract defined in digital form, using a specific programming language. Programmability thus changes the nature of digital money from accessible entries in a digital database, to a mechanism guaranteeing an inseparable storage and utilization mechanism.

Programmability can also directly affect the nature and value of the monetary unit itself. Central banks may, for example, attach expiration dates to money or ensure that it is used for specific products or services. Governments can thus ensure that certain money is put toward a specific utility, to maximize the impact of stimulus or support a certain group of people or sector of the economy.[41]

The level of programmability refers to the extent to which the functions and conditions of the CBDC are open to programmability. They can remain as low-programmable static account-based balances, or coded to allow for micropayments or feedback functions with many chains of counterparties.[42]

Programmable Payments

Programmable money would be supplemented by programmable payments, which are transfers of money for which the time, payment amount, or measurable pre-requisite events can be set in advance.[43] These can, for example, be the arrival of products at a destination, the provision of services, or the expiration of a period of performance. Applied to transaction issues, they can reduce the need to assign excess liquidity buffers during treasury downtime, allowing fully real-time payment. Thus, they can transform legacy systems like next-day-processing, manual monitoring, and forecasting models in favor of live events.

Programming can be directly integrated into the CBDC. The programming can also be done via the wallets holding the money, to make payments contingent on the occurrence of certain events, and ensure fully automated settlements between different devices, with and without human interaction.

[41] Markus Brunnermeier and Jean-Pierre Landau, "The digital euro: Policy Implications and Perspectives," Study, January 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703337/IPOL_STU(2022)703337_EN.pdf

[42] Deutsche Bundesbank, "Money in Programmable Applications Cross-Sector Perspectives from the German Economy"

[43] Deutsche Bundesbank

Box 1. Programmable Money Use Cases[44]

Machine-to-Machine (M2M). M2M payments enable fully automated settlement between different devices without the participation of the end customer.

- An electric car can pay for the charging station at the car park or parking fees independently through "car to car" or "car to charging station" payment processes.

Internet of Things (IoT). Payments in the IoT between different devices connected to the Internet or another proprietary network initiated by the interaction of the end customer.

- A person pays their neighbors for the shared use of energy received from the neighbor's solar panels, or for the partial consumption of energy from a network.

Pay-per-Use. Direct payment is measured based on the amount of consumption or use.

- A leased machine charges a price measured in units of use and processes payments independently.

Bidirectional clearing. Settlement of many mutual claims and/or liabilities between counterparties.

- Two businesses settle their trades with each other in real time. As part of the payment process, invoices are sent out and accounting done automatically.

Cross-border payments. The cash leg settlement of cross-border business made more efficient through a reduced number of intermediaries, improved standardization, and greater transparency.

- Digitalized letters of credit required for export handling allow smart contracts to manage payment when conditions set out in the letters are met.

24/7 payments. Payments made outside the availability periods or amount limits of conventional systems.

- Redemption of a security with a maturity date that falls on a Saturday morning.

Payments as an information function. Integration of payment and information systems, designing the payments to contribute to processes and data integration across enterprises.

- Extending the use of digital money by attaching usage attributes or other metadata to the payment, which enable ML checks via whitelisting or blacklisting directly at the act of payment as the sender of the payment is identifiable in the payment itself.

Offline payments. Technical bridging of disruptions to internet access as well as integration of non-internet-enabled devices in payments.

- Integrating a system of payments without an internet connection, like paying with a smartphone at the grocery store when the internet connection is disrupted.

[44] Deutsche Bundesbank

7. The Digital Euro

The investigation phase of the digital euro project was launched in October 2021, and is expected to conclude in late 2023. During this phase, the operational model, features, and distribution channels will be assessed, alongside impact assessments on the market. Once the phase is over, the development and implementation of the digital euro may begin based on a decision of the Governing Council of the ECB.[45]

This section aggregates a variety of sources to denote a possible preference for the operating model and design features of the digital euro.

Box 2. Digital euro Operating Model Indicated Preferences

Operating Model	Indicated ECB Preferences[46]
Form	Intermediated
Access	Retail
Remuneration	Not-interest bearing
Utility	Cross-border

Source: Author

Form

It is likely that the digital euro will be a hybrid between token- and account-based systems. For intermediary commercial banks to manage customer onboarding and AML/ 'know your customer' (KYC) duties, retail customers would require account-based relationships with the banks. In turn, a direct line to the central bank account presents the path of least resistance, ensuring that the ECB does not have to reconstruct existing account management infrastructure. It would allow the ECB to have oversight over the number of digital euros in circulation, set holding limits per balance, transaction, and provide for a remuneration channel.

The token-based status would allow for integrating token characteristics into the digital euro. Programmability would be necessary to add a variety of features, including the higher privacy standards characteristic of the European Union, or allow for other innovations based on smart contracts in the payments sector.[47]

Access

The stated goal of the ECB is to create a CBDC primarily for retail payments. The goal is to provide a variety of efficiency increases in payments, monetary policy transmission, and financial stability, among other goals, to individuals and businesses in the Eurosystem.[48] The digital euro would complement other safeguards like banking regulation and supervision, deposit insurance, and the monitoring function of capital markets.[49]

The goal is to bring a form of CBDC to retail that a commercial bank can already access via the Trans-European Automated Real-time Gross Settlement Express Transfer services. These services ensure the free flow of cash, securities, and

[45] Christine Lagarde, "A digital euro," July 13, 2022, https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
[46] Preferences are drawn from an aggregation of sources, including speeches, presentation, reports, and other documents specified in this document.
[47] Emanuele Urbinati, Alessia Belsito, and Daniele Cani, "A digital euro: A Contribution to the Discussion on Technical Design Choices," July 2021, https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/deexp/ecb.deexp211011.en.pdf
[48] Fabio Panetta, "Designing a digital euro for the Retail Payments Landscape of Tomorrow" (Brussels, November 18, 2021), https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211118~b36013b7c5.en.html
[49] Panetta

collateral across Europe and ensure that transactions are settled in central bank money. The aim is also to increase competition in the payment market and unlock new business opportunities targeting retail customers.[50]

Remuneration

A two-tiered remuneration system is proposed with fixed or soft upper limits.[51] This system would provide the flexibility needed to meet the demand for the digital euro. In the introductory period, the system would place fixed upper limits on individual deposits to prevent disruptions in the financial system. An automatic system to channel surplus digital euro balances into a commercial account is under consideration. For enterprises and merchants accepting large scale payments, the tiered remuneration system would provide higher limits.

Utility

The initial goal is to make the digital euro function in the euro area. The digital euro could become a cross-border instrument in the medium term.[52] This would be achieved through system interoperability. In preparation for such an eventuality, new settlement infrastructure is under consideration to ensure interoperability from the outset. Two approaches have been proposed. The first is a unilateral approach, which would allow for the use of the digital euro based on compliance with the systems and rules of the digital euro; this could, however, bring risks of informal currency substitution and appreciate the euro from growth in demand.[53] The second, multilateral approach would involve cooperation between central banks to make their CBDCs directly exchangeable in individual currency areas. With such an approach, large quantities of digital money could not be held in foreign currency.

For the multilateral approach to work, there would have to be common technical standards, at least compatible message formats and programming interfaces, and the CBDCs would have to be integrated as much as possible into a single system.

Box 3. Digital euro Operating Model Indicated Preferences

Design Features	Indicated ECB Preferences
Architecture	Intermediated
Availability	Offline and online
Privacy	Selective
Programmability	Medium

Source: Author

Architecture

The architecture of the digital euro would be intermediated. To avoid disruption to the market and disintermediation from commercial banking, the private sector could offer accounts or digital wallets that would facilitate the management of digital euro holdings. These would have a direct line to accounts at the ECB. The intermediated model would also allot customer verification and AML/KYC functions to banks, meaning that the existing infrastructure and rules would remain in place.

Availability

The preferred goal is to make the digital euro function online and offline.[54] In the online system, a third party should be able to process payments, and while offline, P2P payments should be possible. The goal would be to ensure that it could be

[50] Panetta
[51] Joachim Nagel, "Joachim Nagel: Digital Euro - Opportunities and Risks," https://www.bis.org/review/r220810a.htm
[52] Nagel
[53] Nagel
[54] Nagel

exchanged for cash at any time and vice versa.[55] These possibilities should be supported by the standard offerings of commercial banks and payment service providers, and these functions should be interoperable, utilizing mobile technology like smartphones.

Privacy

The digital euro should have a high level of selective privacy, with stratified privacy levels based upon the type and sum of a payment. The possibility of anonymous payments should also be provided. Anonymity could be possible when paying via electronic wallet without an internet connection. With P2P payments, an issuer could ask the payment service provider to exempt payments in smaller amounts from AML/KYC obligations. Also, privacy should be ensured by being able to exchange CBDC for cash anywhere. However, privacy should be considered in line with AML/CFT objectives.[56]

Programmability

The digital euro prefers at least a medium level of programmability. It would be at the core of the new services that the digital euro would serve as a platform for developing.[57] Programmability would also help integrate privacy options directly into the digital euro itself, rather than depending on commercial banks not collecting data.[58] Programmability could also ensure that macro-level data are collected from the digital euro to allow for better oversight without having to intrude on personal data.

[55] Nagel

[56] Eurogroup, "Digital Euro Privacy Options," https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220404_privacy.en.pdf?39c27f3bda85972b8070c318bb4e3578

[57] Panetta, "Designing a digital euro for the Retail Payments Landscape of Tomorrow;" Burkhard Balz, "The digital euro for Tomorrow's Payment Systems" (Deutsche Bundesbank, 18.05.2022), https://www.bundesbank.de/en/press/speeches/the-digital-euro-for-tomorrow-s-payment-systems-891262

[58] Urbinati, Belsito, and Cani, "A digital euro: A Contribution to the Discussion on Technical Design Choices"

8. AML/CFT/CFP and Sanctions Evasion Considerations of the Digital Euro

The digital euro is likely to have both positive and negative impacts on combating financial and economic crime. It would constitute a new form of payment, which presents a variety of new challenges. When other payment instruments like credit cards or online payments first arrived, they also added new complexities to ML prevention, and the digital euro can be expected to do the same.[59] However, just as these now-old payment methods brought challenges, they also brought new opportunities to collect financial intelligence.[60] The few CBDC that have already been deployed present evidence that CBDCs may facilitate ML and other financial integrity risks, similarly to cryptocurrencies.[61] Focusing on threats, they depend on the features chosen, and how they are implemented in the current AML/CFT/CFP framework.

If not carefully considered and adapted, each design feature of the digital euro can create new AML/CFT/CFP vulnerabilities. These threats may arise indirectly at multiple levels of the system harnessing the digital euro, particularly given that the CBDC should be usable across the jurisdictions in the eurozone system. Criminals may thus exploit arbitrage opportunities in legal frameworks or take advantage of differences in enforcement capacity. The digital euro may require changes in the governing, accounting, and financial reporting standards to recognize its unique functionality, as well as the broader technical infrastructural systems underpinning it. The digital euro may similarly affect the interoperability of multiple public agencies that depend on the existing frameworks to fulfill their financial integrity objectives. FIUs, LEAs, prosecutors, tax, and capital market authorities are among the affected stakeholders, especially in relation to cyber-resilience.

The dominant view of how CBDC should be approached is to ensure that the balance between priorities remains similar to current levels. This is understood to mean that, for example, AML/CFT/CFP policy objectives should be balanced with others (such as privacy, or payment efficiency) in a way that does not make using CBDC riskier than using physical cash from an AML/CFT/CFP perspective, but also does not make it less risky by encroaching on other priorities.[62] The baseline for discussion during the investigatory phase of the digital euro should consequently be that the balance of risk does not skew away from the current proportion.

It follows, that the design considerations of the digital euro must take into consideration a broad range of AML/CFT/CFP objectives in the EU. These objectives are put in place by an extensive set of laws, rules, and regulations adopted by jurisdictions to mitigate the use of the financial system to conduct financial and economic crime, finance terrorism, or evade sanctions. The EU adopted six consecutive AML Directives between 1991-2020 to harmonize AML/CFT/CFP

[59] Financial Action Task Force, "Money Laundering Using New Payment Methods," 2010, https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf

[60] Online payments, for example, are now the core of financial intelligence investigation.

[61] China's eYuan has been used to launder overseas fraud proceeds and conduct other crimes, while the IMF has highlighted Nigeria's eNaira as a potential illicit financing channel. See Bloomberg, "Chinese Police Makes Arrest Over Digital Yuan Scam - Bloomberg," November 17, 2021, https://www.bloomberg.com/news/articles/2021-11-17/chinese-police-makes-arrest-over-digital-yuan-scam; International Monetary Fund, "Nigeria: 2021 Article IV Consultation-Press Release; Staff Report; Staff Statement, and Statement by the Executive Director for Nigeria," IMF, February 9, 2022, https://www.imf.org/en/Publications/CR/Issues/2022/02/09/Nigeria-2021-Article-IV-Consultation-Press-Release-Staff-Report-Staff-Statement-and-512944

[62] European Data Protection Board, "Response of the EDPB to the European Commission's Targeted Consultation on a Digital Euro," June 14, 2022, https://edpb.europa.eu/system/files/2022-06/edpb_responseconsultation_20220614_digitaleuro_en.pdf

approaches.[63] These have been further globalized by the evolving recommendations of the FATF,[64] which have noted that CBDCs will be treated as fiat currencies.[65] Therefore, the activities of financial institutions, designated non-financial businesses and professions, and VASPs using CBDCs would be obligated entities as if they were using cash or electronic payments.[66] On this basis, a high-level risk assessment of digital euro design features follows in the next section.

[63] European Commission, "EU Context of Anti-Money Laundering and Countering the Financing of Terrorism," accessed August 22, 2022, https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en

[64] FATF is an inter-governmental policymaking body whose purpose is to establish international standards, and to develop and promote policies, both at national and international levels, to combat money laundering and the financing of terrorism.

[65] Financial Action Task Force, "FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins"

[66] Financial Action Task Force

9. Digital Euro Design Feature Risk Considerations

Most "direct" criminal use of the digital euro will be stopped (at least online), since sending and receiving online digital wallets and transactions will require the collection and retention of identity documents, and their retention. This data provides FIUs and LEAs an auditable digital paper trail that can be checked, similarly to the current framework. However, as the digital euro becomes more widely accepted by merchants, its novel technical features—interoperability and cross-border payments—may provide new ways to launder criminal proceeds by establishing new complex schemes, as well as potentially reviving old ones.

The design features of the digital euro are assessed below for their risks. The scope of the assessment considers some of the core functions of AML/CFT/CFP rules, highlighting how these functions may be impacted by the design choices. This includes the level of access to intelligence, the exchange of information, and the capacity to perform financial intelligence for FIUs, LEAs and their partner institutions. It also includes impact on dependencies in financial intermediaries that act as gatekeepers, including recordkeeping and reporting requirements, customer identification and KYC requirements, the travel rule, and suspicious activity and transaction report rules. Each threat area is provided with a risk level.[67] The assessment follows a shorthand for evaluating a combination of threats and vulnerabilities, and risk levels for obliged entities. Three approximate risk levels are provided:

Box 4. Risk Level Legend

Risk Level	Description
Low	The possibility of a threat occurrence is low. There is little data indicating that criminals intend to use the associated attribute for transactions in relation to ML/TF/PF or sanctions evasion. Using this feature for illicit activity may require more complex planning, knowledge, and technical competence than other features.
Medium	The possibility of a threat occurrence is medium. Criminals may utilize the feature to conduct ML/TF/PF. It is considered a moderately available and generally safe channel for committing criminal activity and requires some strategic planning or technical knowledge.
High	The possibility of a threat occurrence is high. This feature broadly enables ML/TF/PF activity and use thereof at comparatively low risk and cost for criminals. The feature allows executing ML/TF/PF activity relatively easily without much planning or technical understanding. Resulting threats can be considered significant.

[67] The risk level grading follows the approach of the National Risk Assessments of the Republic of Latvia, available at: https://www.fid.gov.lv/uploads/files/2021/NRA_2017_2019_Executive_Summary%20%28002%29.pdf

Design Feature	Risk Level
Architecture	**Low**

An intermediated architecture does not present a systematically significant shift from the status quo. If financial institutions and other private sector AML obligated entities hold accounts or wallets, they also remain the main vehicle for onboarding clients and performing identification. This is especially the case if payment access and processes for retail take place through financial institutions—the traditional vehicle.

Careful preparation would have to be undertaken to evaluate the trends in shifts from the use of cash, especially if the digital euro is introduced alongside a slowdown in the issuance of cash by the ECB. Organized crime and professional ML networks may begin to hoard cash to build up reserves or de-bank if the digital euro comes with more stringent transaction monitoring capacity.

The preference for the intermediated infrastructure is a hybrid of account-based and token-based digital euro. It is prudent to understand how tokenization leads to changes in available data, considering the level of privacy and programmability, which may be high. As the goal of the payments is for them to take place in real time, commercial banks may need to prepare capacity to assess much higher rates of payment. If central banks will also share responsibility for assessing transaction trails, a data exchange system with FIUs, LEAs, and other public authorities should be arranged. For example, at the moment, efficiently tracing cryptocurrencies remains a challenge, and by placing similar tokens and a possibly exchangeable digital euro that can perform many nearly simultaneous transactions at real time, one creates the equivalent of virtual asset tumblers.[68]

On a larger scale, the intermediation of the digital euro calls for a reassessment of how stolen funds should be seized and returned. With new multi-factor authentication measures like biometrics, private keys, or cold storage, accessing and securing custody over funds is more difficult. Exacerbating such issues is the high potential for comingling funds from different wallets at a rapid pace. A tokenized digital euro may provide the non-fungibility to separate from other money, but if the digital euro can be converted to cash at will, it is unclear how the chain of transactions works.

[68] One investigation of a single virtual asset tumbler required years of investigation and the active coordination of seven public agencies. See Financial Crimes Enforcement Network, "First Bitcoin 'Mixer' Penalized by FinCEN for Violating Anti-Money Laundering Laws," October 19, 2020, https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws

Design Feature	Risk Level
Availability	**Medium**

There is a preference to make the digital euro usable for both online and offline payments. The risks are covered in the architecture section, and online payments are the status quo. Offline availability, however, potentially creates significant ML/TF risks. These risks are based on three presumptions: (1) users can switch between online and offline payments at will, (2) offline payments support P2P, and (3) offline payments are unrecorded or are recorded with reduced due diligence by intermediaries.

First, allowing for the interchangeability of online and offline payments at will creates an information gap in the access to payment records, changing the digital forensics necessary to trace financial flows.[69] If these payments are unrecorded, the limits on total amount of transactable digital euro, and the number of wallets that can be transmitted to require severe limitations.

Second, depending on the size of these limits, offline payments may make moving monetary value across borders easier. There are no regulatory requirements for reporting digital euros held within smartphone digital wallets, or other related cold storage methods. Considering the preference for being able to exchange digital euro for cash at will, there may be a variety of ways to exploit the fungibility of cash and digital euro.

Third, it remains unclear how financial intelligence should use gaps in the audit trail based on anonymous offline transactions. Frequent near-threshold payments, cash deposits, or withdrawals are indicative of individuals trying to avoid reporting requirements. These are important signifiers that can lead analysts and investigators to investigate these individuals against criminal typologies. Since the offline mode of payments for the digital euro would be enabled with the specific purpose of allowing untraceability as a corollary of cash, it is unclear how intermediaries performing examinations or public authorities conducting investigations should account for the utilized sums.[70]

[69] Raphael Auer and Rainer Böhme, "The Technology of Retail Central Bank Digital Currency," SSRN Scholarly Paper (Rochester, NY, March 1, 2020), https://papers.ssrn.com/abstract=3561198

[70] One could contend that digitally anonymized payments offer greater privacy than cash, which can be marked or inspected for its serial number. From this perspective, anonymized offline payments create a greater audit gap than cash.

Design Feature	Risk Level
Privacy	**High**

A core principle in the development of the digital euro is a prominent level of privacy protection. The indicated preferences involve at the very least a degree of choice for retail users in how data is shared, as well as being in favor of offline payments that offer a high level of, if not complete, anonymity.

A high level of anonymity in an offline wallet increases the inherent risks of the digital euro. The European Banking Authority (EBA) has previously identified anonymity from the use of cash and stored value instruments and the anonymity allowed from transactions below a defined threshold as risks in the European Union's financial sector.[71] For example, while prepaid cards are often of low value, the risks increase when products offered by e-money institutions allow high-value or unlimited payments, loading or redemption, and cash withdrawal. The EBA noted the lack of traceability for money thresholds for such prepaid e-money services in third countries as problematic.[72]

The preference for cash-like features in a digital form is in tension with several regulatory trajectories. In line with FATF standards, the AML/CFT/CFP package proposed by the European Commission in July 2021 extended the ban on anonymous accounts and wallets[73]

Another privacy-related risk stems from the fact that the digital euro could have both account-base and token-based features. A token-based digital euro enables the use of cryptographic and institutional arrangements to enable a higher level of user privacy. Users may be able to select the extent to which data is shared with different entities at the digital wallet level, which may not be accessible to financial intermediaries banking the client.[74] Through this functionality, the goal of the Eurosystem is to decrease the amount of data collected from users to the minimum necessary to perform their functions, such as accessing information for settlement functions, or performing supervisory or oversight tasks. However, it raises concerns about who has access to this data and the ability of the financial sector to perform compliance functions and access the full transaction history of their clients, as well as the secondary access of FIUs, LEAs, and other authorities to this data.

Utilizing innovative techniques to enhance user forensics and financial intelligence could mitigate some of these concerns. Novel data analytics tools, like black boxes, indirect analyses, and artificial intelligence (AI), may help mitigate the lack of access to certain information that is currently available. However, these possibilities need to be managed carefully against other regulatory limitations. The AI regulation, for example, requires careful assessment before engaging in any profiling of individuals. Profiling may be an especially useful tool given the ability to decrease retail user access to certain personal information in banking and the ability to rapidly move the digital euro across many wallets via smart contracts.

[71] European Banking Authority, "Opinion of the European Banking Authority on the Risks of Money Laundering and Terrorist Financing Affecting the European Union's Financial Sector," March 3, 2021, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf
[72] European Banking Authority
[73] European Banking Authority
[74] The Bank of Canada et al., "Central Bank Digital Currencies"

Design Feature	Risk Level
Programmability	**High**

A digital euro will necessarily employ a level of programmability, which gives rise to a variety of new ML threats. Programmability may foster a new system of intermediaries that utilize the allowance creation of new types of financial services. However, unfettered programmability may lead to a variety of new ML typologies and exploitation schemes. Programmability will be enabled through smart contract functionality, allowing for payment interface providers to build software services that interact directly with the digital wallet of the retail customer. With a real-time payment system, programmability can be made to perform currency swaps instantaneously, automatically, and via micropayments.[75]

These are likely to be an increasingly elaborate new generation of ML schemes.[76] Such schemes would be exploited for layering stage activities, which involve concealing the criminal origin of proceeds by creating a "clean" digital paper trail for money that has traveled through many digital euro wallets. Next, the integration of those digital funds creates the appearance of a legal origin for criminal proceeds. Those criminal proceeds are used for personal benefit by converting the digital euros to cash, using them for direct consumption, or purchasing other investments.

For instance, physical cash and private or commercial virtual assets may be traded for the digital euro through underground networks like noncompliant Dark Net crypto exchanges.[77] Similarly, the money-mule system that exists currently with traditional virtual assets to launder fiat currency could also be possible with the digital euro, with wallets and programs replacing the currency-mule. Criminal entities can tumble money through many wallets automatically, distancing themselves from the illicit source of funds. Retail merchants that agree to be fronts can also be utilized to move funds through the digital euro ecosystem by comingling funds through a high volume of business transactions to conceal illicit proceeds. Through smart contracts, trade-based laundering can be committed by falsifying invoices for virtual services and creating a system of money mules with fictitious clients and supply chains that interact instantly across the web.

Programmability may also contribute to the growth of informal economies. By utilizing the hawala principle,[78] schemes to move money internationally through ledger-based systems that lock the digital euro into a certain contract without the digital euro visibly changing location in an account. The transaction would then take place through bargaining with services, goods, or cash assets outside of the digital network, allowing cross-border informal transfer of value without the transfer of actual funds. The true function of such enabling smart contracts would be technically difficult to extract and near impossible to interlock with a ML network without having access to an insider.

A hike in cyber-fraud as predicate crimes with the intent of ML can also be expected with the initial release of a token-based digital euro. This can include counterfeiting hacks or exploits that could potentially 'double spend' by digitally creating money

[75] Lee Reiners, "CBDC – How Dangerous Is Programmability?," *The FinReg Blog* (blog), September 21, 2021, https://sites.duke.edu/thefinregblog/2021/09/21/cbdc-how-dangerous-is-programmability/

[76] Fanusie, "Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them"

[77] Fanusie

78 Hawala is a system of using informal methods to transfer money without any physical cash being transferred. It uses proxy systems to settle accounts between transaction parties, hiding the participation of the real ultimate beneficiaries of the money being exchanged.

without legal authorization.[79] Hackers can create self-executing smart contracts that exchange the digital euro automatically, which is a commonly observed fraud in virtual assets.[80]

Next, it is not clear how AML/CFT/CFP compliance duties and financial intelligence would be done for parties that use programmability features. Depending on the extent of programmability permitted, financial crime schemes can be created with thousands of participant wallets, supported by automated smart contracts that perform a vast variety of services. An equivalent compliance system must enable banks to analyze these networks to perform their AML/KYC roles.[81] If a bank is dealing with a hosted wallet, it should be able to analyze transactions in real-time to ensure payments only travel through other trusted wallets.[82]

Similar difficulties may be encountered by FIUs, LEAs, and other authorities. How they access the data associated with programmable money flows is unclear. The architecture of programmable money should be refined to ensure authorities have a level of centralized access to payment data across wallets, regardless of their geographic and jurisdictional domicile. The current framework of information exchange between FIUs in the European Union, for example, requires that an FIU formally request data on a specific legal or natural person from another member state FIU. This system of data exchange will be severely insufficient if the amount of transaction flow chains continues to increase.

The risks increase even further if the digital euro can—through a variety of currency exchange functions—transcend borders outside of the European Union.[83] A system of data exchange adapted in the European Union may not be in effect outside of its borders, where different AML/CFT/CFP regulations, supervision, and enforcement standards are in effect. The challenge would be particularly noteworthy if digital euro transaction chains required data from offshore or non-cooperative jurisdictions.[84]

[79] GaoBingyu et al., "Tracking Counterfeit Cryptocurrency End-to-End," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, November 30, 2020, https://doi.org/10.1145/3428335
[80] Chainalysis, "The 2022 Crypto Crime Report: Original Data and Research into Cryptocurrency-Based Crime," February 2022, https://assets.bitcast.site/other-files/Crypto-Crime-Report-2022.pdf
[81] Cœuré and Loh, "Central Bank Digital Currencies"
[82] Henry Balani, "What Faster Payments Means for Anti-Money Laundering Compliance," *Journal of Financial Compliance* 1, no. 3 (2017): 245–54
[83] Cœuré and Loh
[84] U.S. Department of Treasury, "Fact Sheet: Framework for International Engagement on Digital Assets," July 7, 2022, https://home.treasury.gov/news/press-releases/jy0854

10. Digital Euro Product Risk Assessment

Though the digital euro is a new product, it is entering an existing AML/CFT/CFP domain. The digital euro will be part of an existing risk framework, whereby its introduction will interact with the weights of other inherent risks in the risk-based approach of obliged entities in different jurisdictions and sectors. These entities, together with the ECB and perhaps eurozone central banks and commercial banks, will have to adapt their internal control systems to the presence of the digital euro, taking into account the change it brings to the risk environment.

This section builds on the previous risk features to outline the preliminary considerations of the digital euro in a risk-based approach framework.

Product Delivery Channel Risk

Depending on the attributes of digital euro, its delivery channel can extend several significant AML/TF risks. First, the delivery of the digital euro to end users will be done by central banks or using the status quo of commercial banks or service providers; both variants provide different prima facie risks of money laundering. If the delivery of digital euro is through central bank digital wallets, then central banks may have to create a novel KYC system, which will be dependent on the variety of idiosyncratic digital identity schemes in the European Union. These systems, if not harmonized across the eurozone, will create vulnerabilities through varying levels of access to customer due diligence or interpretation of the risk-based approach framework. By extension, if the management of the digital euro is through digital wallets in commercial banks, then the vulnerability arises through the differing risk-based approaches of each bank. The vulnerabilities to money laundering would continue throughout the banking relationship with each wallet holder.

Product and Service Risk

The level of programmability of the digital euro may create a proportional level of product or service risks. A high-level intermediation of the digital euro is a key benefit of CBDC, but it is also a central vulnerability. Free interconnectedness with other digital products and services may result in the creation of a variety of new ML schemes that utilize high-frequency micro-transactions across many digital actors. With a real-time payment system and the ability to create complex multi-layered payment schemes, the services and products that utilize these schemes may be exploited for ML purposes. The vulnerability of these products and services will be extended without a way to trace transactions across jurisdictions and if they are allowed to enter third-countries.

Customer Risk

The breadth of clients for the digital euro should include all banked eurozone citizens and residents. Without additional monitoring of customers by central banks or financial services or a segmented roll-out of the digital euro, the vulnerabilities of the digital euro may emulate those of digital payments or even cash. Depending on the level of anonymity and other factors, the digital euro may be utilized for a variety of predicate crimes. Under a risk-based approach, the obliged entities under the digital euro will have to assess the economic and personal activities of the person, as well as their participation in legal structures and the beneficial ownership of the respective funds therein.

Geographical Risk

The initial distribution of the digital euro may be limited to eurozone jurisdictions. Each country has a unique risk profile, and if they are not sufficiently managed at a subsidiary level, geographical risks may create legal, enforcement, or monitoring arbitrage opportunities for criminals. Differential supervisory capacity and legal harmonization among countries using the digital euro are thus capable of amplifying localized risk profiles and potentially creating new synergies in the apparent legalization of illicit funds. Vulnerabilities may arise from geographical locations with a lot of trade with third countries, where trade-based money laundering can be utilized as an on- and off-ramp for the exchange of third-country currency or goods into the digital euro. The geographical risk can also create further vulnerabilities to the evasion of sanctions regimes, especially if the extent of due diligence in the utilization of the digital euro extends to a single or few jurisdictions. A lack of harmonization of digital euro approaches toward third countries can significantly increase the vulnerabilities to money laundering and terrorist financing.

11. Meeting New Challenges

Issuing the digital euro is a complex project that will involve multiple stakeholders beyond its traditional central bank counterparts. The interest in and impact of the digital euro extends also to the legal framework, technological infrastructure, and institutional capacities. The issuance of the digital euro thus requires carefully reviewing the legal, technical, and institutional preconditions to ensure that it does not jeopardize policy goals like AML/CFT/CFP and sanctions evasion.

This study finds a variety of risk areas where certain indicated preferences alter the AML/CFT/CFP risk framework. There are a range of new institutional interactions that require in-depth analysis and discussion before the introduction of CBDC. Multiple public agencies, such as FIUs, tax agencies, capital market, and statistical agencies, plus supervisors, consumer protection agencies and private sector stakeholders, including merchants and users are directly impacted by the changes brought by the digital euro.

Each of the design features of the digital euro presents an opportunity and a need for discussion. It is important to demarcate the lines of privacy, programmability, architecture, and availability afforded by the digital euro. Each presents individual domain challenges, but also creates cascading interdependencies. It is likely that fundamental changes will be made to the AML/CFT/CFP framework, commercial bank compliance functions, FIU and LEA duties, and other governance frameworks.

These discussions need to take place alongside a comprehensive review of key domains. The AML/CFT/CFP framework in the European Union is adapting to virtual assets and account-based banking systems, but token-based banking that combines the features of virtual assets and traditional banking is not yet covered. Similarly, suspicious transaction report dissemination, information requests, and other cross-border information exchange mechanisms are at the crux of monitoring the digital euro. Mechanisms ensuring a useful level of monitoring capacity by public authorities will have to be in place prior to the launch of the digital euro.

Many of these domains are growing increasingly interdependent; the financial integrity, cyber-security, and privacy domains are already closely connected. Key issues like the mitigation of financial integrity and cyber-security risks are drivers of architecture design decisions. The effective implementation of financial integrity measures is important in all cases. This entails ensuring compliance with the FATF and other standards and taking effective action to mitigate ML and TF risks. Cyber-

security across different product layers forms the basis for a reliable and resilient digital euro payment system that is resistant to fraud and cyber-attacks. Incorporating flexibility into the architecture can support future-proofing the digital to account for changing user needs, regulations, and technology.

Lastly, the digital euro must take into account a variety of systemic challenges. The creation of new dynamics for international payments outside the dominant SWIFT and SEPA payment networks may create significant divergences in payment functionality across jurisdictions.[85] Data storage and governance rules are also important, to ensure that the movement of digital euro across jurisdictions remains traceable. Access to data and ensuring the capacity to share data in a similar format, provided the volume of data grows, is important, as is having a way to isolate and react to non-cooperative jurisdictions that provide communication platforms, servers, computers, or other relevant financial technology services in the jurisdiction. The design of the digital euro system should be adaptable to changes in these systematic challenges.

Stakeholder Engagement

The digital euro is still in the early stages of development, and much can still change. These morphing design features can materially impact the ability to collect and analyze financial intelligence by both public and private sector entities. To develop a mutual understanding of these impacts and help anticipate the consequences of a digital euro, it is important to engage these stakeholders throughout the design process with a clear understanding of their roles.

There is a possible spectrum of roles that stakeholders can play in the development of the digital euro. These roles fall under three archetypes: (1) followers; (2) consultants; and (3) advocates. Each role demarcates the extent of influence the entity has on the design of the digital euro and how it adapts its own internal policy to this process.

Followers will monitor the developments of the digital euro without involving themselves in the design. They may provide technical input reactively in response to requests, but they will focus on adapting policy to the final proposal and assisting in its implementation.

Consultants will engage in digital euro design discussions as experts on how illicit actors may exploit different features. They do not take a position on a preferred design and focus on ensuring the quality of technical input in response to stakeholder requests.

Advocates will engage in discussions about digital euro design with preferences for features that may best support reaching their objectives and the public good. They will actively promote a position on designs through available interagency forums.

Each role may be more fitting at different points in the design cycle. The ECB and the respective domestic representatives at member state central banks should ensure that different domestic institutions and agencies are looped into the design cycle, with clearly defined expectations. Coordination with FIUs, LEAs, national security agencies, prosecution offices, and the judiciary may be light initially but should increase as design preferences take shape and solidify.

Central banks may consider establishing national consultative committees of stakeholders to facilitate communication among these stakeholders, via surveys and focus groups. Clear mandates and effective collaboration can help prioritize

[85] For example, China's alternative network CIPS, could grow in use.

tasks, scope the development of the digital euro, and maximize resource efficiency.[86]

[86] Kiff et al., "A Survey of Research on Retail Central Bank Digital Currency"