The Digital Euro:
An Analysis of the Commission's Proposed Legislation

Mikolai Gütschow, Dresden University of Technology (TUD), Germany
Bernd Lucke[1], University of Hamburg (UHH), Germany

May 2025 (rev. July 2025)

Abstract

We analyse the Commission's draft regulation for the establishment of the digital euro (DE). Key findings include: a) The offline version of the DE, designed for proximity payments, has no clear advantage over cash and is inferior in terms of security, convenience, inclusiveness and scope. b) The online version is superior to commercial bank money only in terms of lower issuer risk. In most other respects it greatly resembles commercial bank money without discernible benefits for customers. Privacy is similar, but concerns remain about illegal user re-identification at central level. c) The DE distorts competition between banks and non-banks and is unlikely to foster innovation in payments markets. d) DE issuance and basic services are unprofitable for payment service providers. e) Banks may find it profitable to issue a DE based stablecoin that would be superior to the DE in all regards. f) Such a stablecoin might replace the DE and undermine the ECB's efforts to preserve control of monetary policy in digitalized payments markets.

Keywords: Digital Euro, payments technologies, regulation, privacy, tamper-resistant design

CCS-Concepts:

- Social and professional topics -> Computing / technology policy -> Government technology policy
- Security and privacy -> Security in hardware -> Tamper-proof and tamper-resistant designs
- Information systems -> World Wide Web -> Web applications -> Electronic commerce

JEL: E42, E58, E52

[1] Corresponding author: Prof. Dr. Bernd Lucke, von Melle Park 5, 20146 Hamburg. Tel. +49-40-42838-3996. Email: bernd.lucke@uni-hamburg.de, ORCID 0000-0002-4883-8756.

1. Introduction

In recent years, new technologies and the digitalization of the economy made private digital means of payment gain significant traction. But only central bank money has legal tender status. This type of money is accessible for the general public only in the form of physical money, i. e. banknotes and coins, henceforth referred to as cash. As with increasing digitalization the usage of cash is likely to diminish while payment habits shift towards the use of private digital payment solutions, it is unclear what quantitative role central bank money (banknotes and commercial bank reserves at the central bank) will play in the future. And, from a policy perspective: It is unclear how effective monetary policy can be if we are approaching a cashless economy.

While cash is used by the general public, transactions between commercial banks use reserves – a different form of central bank money that is exchanged digitally. Monetary policy may still be effective if reserves retain their current function in the payment system even in a nearly cashless society. But will they? Reserves are liabilities of the central bank that commercial banks are entitled to convert to cash at any moment. What value would reserves have if the demand for cash approaches zero?

If the demand for reserves decreases along with the demand for cash, central banks might loose their ability to conduct monetary policy the way they used to since the rise of fiat money. A related concern is about financial stability and the role of the commercial banking sector: The diminishing use of cash could undermine trust in (private) commercial bank money, as this trust relies on the ability to convert demand deposits at par into cash (i. e. central bank money) any time . Would this trust prevail if central bank money comes out of use in the non-bank private sector? Currently, cash probably serves as a monetary anchor of our monetary system. What impact on financial stability would it have and would we still trust banks the way we do now if a monetary anchor in the form of central bank money ceases to exist? Clearly, such scenarios are food for thought for central banks around the globe. The simplest solution would be to offer private agents a digital form of central bank money either as a replacement for (physical) cash or as a complementary means of payment. If the general public uses a central bank digital currency (CBDC) for day-to-day transactions, there will still be demand for central bank money, even if cash comes out of use. Hence, the central bank can implement its monetary policy via this demand. Moreover, commercial banks (and possibly other payment service providers (PSPs)) could back customer deposits by a promise to pay any claims in digital central bank money and thus maintain the current level of trust in the fiat money system.

In recent years, many central banks began studying the viability of CBDCs. In a 2023 survey of the Bank for International Settlements (BIS), 94% of responding central banks were studying or implementing CBDCs (Di Iorio et al. (2024)). In line with this, the Atlantic Council reports that currently 134 central banks explore CBDCs, up from 35 in 2020. According to these figures, 66 countries or currency unions are in an advanced phase, i. e. in development, pilot or launch.

Notable initiatives include China’s digital yuan project. Extensive research and development took place since 2014, making the People’s Bank of China one of the most advanced central banks in CBDC exploration. The project is currently in a large-scale pilot phase, with trials taking place in multiple cities, including Shenzhen, Suzhou, Chengdu, and Xiongan. The government has distributed millions of digital yuan to citizens via a lottery system and through partnerships with commercial banks, allowing for real-world testing and adoption.

Pilot projects are also undertaken by other large countries, e. g. Brazil and India. Smaller countries like The Bahamas, Nigeria, and Jamaica have already launched their digital currencies, but adoption remains gradual and requires continuous adjustments. (IMF (2023)). International organizations are also playing a key role, with the BIS Innovation Hub conducting technical experiments on CBDC payment solutions, such as offline transactions and cross-border payments.

However, not all central banks are moving forward with CBDCs. For instance, Uruguay scaled back its CBDC efforts after an initial pilot, and Kenya has postponed further exploration, citing no immediate need.

In the Eurozone, the development of the digital euro has reached an advanced stage. The European Central Bank (ECB) began exploring the feasibility of a digital euro (DE) through several reports and a public consultation in 2020 and 2021. The ECB proposed a two-tier system for a general-purpose digital currency and launched a two-year investigation phase in July 2021 to address key design and distribution challenges. This phase involved focus groups, prototyping, and conceptual work. By November 2023, the ECB began a "preparation phase" which focuses on finalizing a digital euro rulebook, selecting providers for platform development, and conducting testing.

In June 2023 the European Commission (COM) initiated the first legal steps to introduce the DE in the Eurozone. To this end, it submitted a draft regulation to the European Parliament and the Council, COM (2023a), that envisions the DE as a retail CBDC – i. e. as a form of digital central bank money directly accessible to the general public and endowed with legal tender status. Simultaneously, the Commission invited the ECB to comment on this proposal in the form of a legal opinion. The ECB presented its opinion in October 2023, cf. ECB (2023a).

The COM proposal is still under the scrutiny of the co-legislators. In this paper, we aim to aid lawmakers by analyzing and evaluating the draft regulation as proposed by the Commission, taking into account the ECB's legal opinion and previous documents issued by the ECB on this matter, e. g. the 2020 "Report on a Digital Euro", ECB (2020). To do so, Section 2 starts with outlining some legal and functional distinctions, Next, Section 3 analyzes the explicit and implicit goals of the digital euro's introduction, as well as potential unintended side effects. Section 4 examines the proposed regulation's capacity to achieve these goals while mitigating undesired outcomes. The paper concludes with a summary of findings and reflections on the broader implications of the digital euro for the EU's monetary and financial ecosystem.

2. Some distinctions

2.1 Legal delineations

The legal basis for an EU regulation on a digital euro is Article 133 of the Treaty on the Functioning of the European Union (TFEU). This article stipulates that the co-legislators (i. e. European Parliament and the Council) "shall lay down the measures necessary for the use of the euro as the single currency" and that they shall do so "without prejudice to the powers of the European Central Bank".

This legal delineation between co-legislators and ECB has important implications: Legislation such as the proposed regulation can only target the *use* of the DE. The *issuance* of the DE,

however, is a matter distinct from its use and is, hence, not a competence of the co-legislators. While neither primary law (e. g. the TFEU) nor secondary EU law (e. g. a regulation) currently contains express wording on the competence to issue digital euros, Article 128 TFEU assigns the "exclusive right to authorize the issue of euro banknotes" to the ECB. From this, it seems clear that the ECB would also have the exclusive right to authorize the issue of euros in *non-physical* forms – as emphasized in the ECB (2023a) legal opinion.

To give an example: Legislation may regulate who and under which circumstances has to accept the DE as legal tender – this concerns the *use* of the DE. But security properties of the DE are – as are security properties of banknotes – a matter related to the *issuance* of euros. DE security is therefore a competence of the ECB and co-legislators must not interfere with it.

In the case of banknotes, security is basically the protection of money holders against fraud by forging banknotes. In the case of digital euros, security issues under ECB competence cover much more: They not only involve the protection against fraud (e. g. digital copying and multiple usage of a single unit of DE), but also privacy (protection of transaction data) and protection against theft or loss. The risk of theft or loss is a completely private concern for the holder of banknotes, while it is a public concern in the case of digital euros due to the Commission's design choice that holding DEs requires an ECB-secured environment.

It may seem problematic that important issues like privacy or property protection depend on technical measures that are, by virtue of the treaties, beyond the reach of a body with direct democratic legitimization, i. e. not under the scrutiny of elected parlamentarians. On the other hand, transaction data are inherently related to the *use* of DEs and, hence, both co-legislators are free to legislate which type of (personal) information the ECB shall or must have access to, what kind of anonymization shall be applied and how long personal transaction data may be stored in the DE official payment infrastructure.

Similarly, holding DEs is a form of DE use, thus the co-legislator may specify ceilings for private holdings (or authorize the ECB to do so), thereby imposing upper limits to the risk of theft or loss. Thus, the co-legislators may - and possibly should – argue that there are certain aspects of a digital currency where no strict separation of powers applies. Here, it seems reasonable to agree on a concept of shared competence.

Along the same line, note that Article 127 TFEU also assigns to the European System of Central Banks (ESCB) the task "to promote the smooth operation of payment systems". This implies that the technical features of the DE payment infrastructure, insofar as they fall under public authority, are within the competence of the ECB, rather than that of Parliament and the Council. It is less clear whether *design* features of this infrastructure and its interfaces (both user interfaces (UI) and application programming interfaces (API) of private payment services providers (PSPs)) are also an exclusive competence of the ESCB due to their role in "the smooth operation of payment systems". Since infrastructure design and interfaces have clear implications for the *use* of the DE it seems easy to argue that also in this regard there exists a "shared competence" that justifies scrutiny of and legislation by the co-legislators.

2.2 Functional distinctions

Besides the important legal distinction between competences based on either use or issuance of the DE, there is the important economic (or functional) distinction between the DE as a means of payment and the DE payment infrastructure. As Bofinger and Haas (2020) point out, a new payment object (e. g. the DE) could be used either with a new payment system of with an existing one. Conversely, it would be conceivable to establish a new (digital) payment system for the use of an existing digital currency (e. g. private commercial bank money, a stablecoin, a cryptocurrency or even a foreign CBDC). It would even be possible to establish an existing digital currency (foreign or private) in an existing payment system (public or private) as legal tender.

Under this perspective, the title of the COM proposal "Regulation of the European Parliament and the Council on the establishment of the digital euro" is misleading. While the regulation would indeed establish the digital euro in Article 3, major parts of the regulation are actually dealing with how the DE payment infrastructure shall be shaped (i. a. Articles 13, 14, 18, 19, 23-25) and how the costs for the private part of this infrastructure shall be recovered (Article 17).

The misleading title is a minor issue, but it possibly hints at a more serious deficiency of the COM proposal: Has the Commission, in drafting the proposed regulation, given due consideration to alternative design choices for the payment object and the payment infrastructure? As proposed, the regulation would establish the DE as a new payment object and an infrastructure that is partially relying on existing private infrastructure of PSPs and partially on new public infrastructure (particularly for settlement) under the control of the ECB. This is one of several possible configurations and perhaps a good one. But have alternative options been studied?

There is strong evidence that this was not done. Along with the draft regulation, the Commission published an impact assessment (IA) outlining in detail how the Commission's thinking developed, COM (2023b). Chapter 5 is devoted to available policy options. In terms of fundamental choices for payment object and payment infrastructure, no mention is made of combinatorial possibilities similar to those outlined by Bofinger and Haas (2020). The IA considers different levels of payment privacy with respect to intermediaries and the ECB, but it misses out on alternative designs such as asymmetric anonymity as proposed by Chaum (1988) and Dold (2019), combining identifiable payees with guaranteed payer privacy. In essence, only two options are discussed in the IA: Either do nothing or introduce the DE under a set of key design choices previously made by the ECB.

These key design choices include creating the DE as a new payment object both in online and offline form and for retail use only. DE distribution shall mainly rely on existing private PSP infrastructure, partially complemented by new public infrastructure for people without payment account. DE issuance and settlement shall be central and under the control of the ECB, using a newly set up account-based infrastructure specifically designed for a high volume of payments with instant clearance[2].

[2] An earlier paper (ECB (2021)) described experiments aimed at scaling the Eurosystem's existing Target Instant Payment Settlement (TIPS) infrastructure to fit the needs of retail P2P payments in digital euros. While quite positive results were reported, in more recent documents the ECB seems to have abandoned the idea of using

Why have alternative design choices not been studied in the IA? The fact that the ECB favors a particular design does not relieve Commission and lawmakers of their responsibility to check if the ECB's preferred option is optimal for society at large. For instance, digital payments are widely used and function smoothly in the EU on the basis of commercial bank money. Introducing a new means of payment may be disruptive. Assuming that change is indeed imperative, the ECB's opinion that a new payment object is required should be double-checked with existing options which may be less disruptive and possibly equally effective.

In fact, what are the merits of the ECB's opinion that we need both a new payment object and a new payment infrastructure for settlement relative to the alternative design of no change in the payment object, but less reliance on private and in particular foreign-owned infrastructure for distribution and settlement? Or relative to a design where the infrastructure would remain unchanged, but the payment object, while still commercial bank money, would be more tightly tied to ownership of central bank money in the form of reserves?

Many such questions could be raised. Essentially, their answer depends on what exactly the EU wants to achieve by establishing the DE in its proposed form. Does the EU primarily aim at reducing the market power of US-owned private PSPs? Does it want to achieve higher resilience against adverse external events and, ultimately, strategic autonomy, in its payments system? Or is the main concern a better monetary anchor to improve the effectiveness of the ECB's monetary policy when the importance of cash is fading? The desirability of a particular design choice and the appropriateness of measures chosen to implement it greatly depends on the explicit and implicit objectives that guide the establishment of a DE and its infrastructure. To these objectives, summarized in Table 1, we now turn.

3. Objectives

3.1 Explicit objectives

As explicit objectives we define goals that the Commission explicitly mentions in its legislative proposal COM (2023a). As such, goals associated with the introduction of the DE and its infrastructure are:

G1: Provide a catalyst for innovation in payments, finance and commerce.

G2: Reduce the fragmentation of the EU retail payments market.

G3: Enhance efficiency of payment systems.

G4: Enhance resilience of payment systems.

Cf. COM (2023a, Recital 1).

G5: Preserve functioning of monetary and financial systems (by providing a monetary anchor that ensures consumer confidence in commercial bank money)

G6: Safeguard stability of monetary system in a digitalized economy.

---

existing infrastructure. For instance, ECB (2024A) describes "selecting providers that could potentially develop a digital euro platform and infrastructure" as one aim of the DE preparation phase 2023-2025.

Cf. COM (2023a, Recital 3)

G7: Ensure and enhance financial inclusion.

G8: Ensure wide acceptance of the DE.

Cf. COM (2023a, Recital 5). Note that the acceptance of the DE (G8) has two sides: acceptance by the payee as a valid discharge of a payment obligation and acceptance by the payer as a means of payment that is not inferior to cash or commercial bank money. We interpret the phrase "wide acceptance in payments" in Recital 5 as encompassing both aspects.

However, this is not entirely clear, as the draft resolution subsequently focuses almost exclusively on "mandatory acceptance," which may suggest that the Commission is more concerned with ensuring acceptance by payees than with promoting the widespread use of the DE by payers. Recitals 11, 16, 18–20, 42, and 81, as well as Articles 7, 11, 12, and 16, clearly address payee acceptance alone.

That said, it seems evident that the Commission also aims for broad acceptance of the DE by payers, as a legislative initiative imposing mandatory acceptance on payees would only be proportionate if the DE were actually widely used in household spending. Articles 37 and 41 may, but need not, be interpreted as reflecting the broader notion of "acceptance."

G9: Preserve the role of the euro in retail payments markets in the face of competition by currencies with advanced digital capabilities.

Cf. COM (2023a, Recital 7)

G10: Detect and prevent criminal activities, e. g. fraud, tax evasion, money-laundering and terrorist financing.

Cf. COM (2023a, Recitals 68 and 73)

G11: Ensure a high level of privacy and personal data protection.

Cf. COM (2023a, Recitals 70-72 and Section 1 of the Explanatory Memorandum)

Goals G1-G11 are listed here in the order in which they appear in the recitals of the draft regulation. It is unclear if this order is indicative of the relative importance the Commission assigns to each goal. But it is clearly the case that G1-G4 are indirect goals that target the quality of payment systems in general, while G5-G7are concerned with the functioning, the outreach and the stability of the monetary system and G8-G9 directly target the performance of the ECB's currency.

G1-G4 are concerned with allocative efficiency, G5-G7with necessary conditions for allocative efficiency, and G8-G9 are focused on the market power of the ECB. Hence, from the point of view of consumer welfare, it seems fair to say that, indeed, G1-G7 are more important than G8-G9, although, undisputedly, welfare may be well-guarded if a domestic public body rather than foreign or private agents determine monetary developments.

Be this as it may, note that goals G1-G9 may be in conflict with each other. For instance, if third-party digital currencies offer faster or securer or technically superior payment options, then G3 (efficiency of payments systems) and G9 (preserve importance of euro) clearly clash. Similarly, G3 (efficiency) and G4 (resilience) may be challenging to reconcile with G7

(financial inclusion), as individuals who struggle with managing digital currencies may be both costly to include and vulnerable points of entry for malicious actors.

Detection and prevention of criminal activities (G10) and privacy and personal data protection (G11) are explicitly listed as objectives of the regulation. However, in the Recitals, they are mentioned only much later than other desirable features of a digital currency, such as the efficiency and resilience of the payment system. This may reflect the fact that G10 and G11 are not optional goals to be balanced alongside others, but rather inviolable rights anchored in the EU Charter of Fundamental Rights or legally binding targets in secondary Union law (e. g. in the anti-money laundering (AML) and counter-terrorist financing (CFT) Directive (EU) 2015/849).

Specifically, Article 17 of the EU Charter of Fundamental Rights states that "no one may be deprived of his or her possessions," thereby affirming the protection of private property. While it does not explicitly require the detection or prevention of fraud, such measures can be understood as part of the broader duty of public institutions to safeguard property rights. Moreover, the Charter ensures the protection of privacy under Article 7 and of personal data under Article 8. It may therefore be more accurate to view G10 and G11 as constraints that the regulation must respect, rather than as objectives it seeks to achieve.

Indeed, G10 and G11 could also be interpreted as subordinate goals serving G8, or as instrumental in achieving G8 (wide acceptance). Nevertheless, we follow the Commission in treating G10 and G11 as goals in their own right, given the uncertain contours of the constitutional protection afforded to these rights, which leave significant scope for policy and design choices. In the case of privacy, this interpretation is also consistent with public concerns: according to the Commission's stakeholder consultation, "privacy was considered the most important feature of a digital euro by both citizens and professionals" (COM 2023a, p. 6).

3.2 Implicit objectives

In addition to G1-G11, a number of implicit goals may be identified. These are goals not explicitly mentioned in the proposed regulation, but more or less clearly articulated in supporting official text. The reason why these goals are not explicitly stated, is not always clear. For instance, Article 119 of the Treaty on the Functioning of the European Union (TFEU) commits to the principle of an open market economy with free competition – the fundamental principle upon which the Common Market is built. But no reference is made to Article 119 TFEU in the draft legislation and strengthening or, at least, preserving competition in payment services is not among the explicit goals mentioned in the proposed legal text.

On the other hand, the explanatory memorandum in the proposal COM (2023a), under the heading "reasons for and objectives of the proposal", mentions "supporting a stronger and more competitive, efficient and innovative European retail payments market and digital finance sector". This wording associates competitiveness with efficiency (G3) and innovativeness (G1), and while the concepts are certainly not the same, there is little doubt that competitiveness is conducive to achieving G3 and G1. Is this why the Commission did not make stronger competition an explicit goal? In any case – and since the Commission is bound by Article 119 TFEU – we assume that the establishment of the DE also pursues the implicit goal

IG1: Increase competition in payment services and the digital finance sector.

Another, fairly obvious, implicit goal is

IG2: Reduce dependence on non-EU financial infrastructure, enforce control of EU-based infrastructure.

To see this, note that the explanatory memorandum views the digital euro as supporting the "EU's open strategic autonomy". Pointing explicitly to the perceived threat, the ECB's (2020) report on the DE singles out foreign payment providers and states that a digital euro would contribute to "strategic autonomy by providing an alternative to foreign payment providers for fast and efficient payments in Europe and beyond." Clearly, the concern is not the currency, but the infrastructure owned by these foreign PSPs, e. g. "International Card Schemes (ICS) or large, often foreign-owned platforms offering digital wallets to cardholders. This … may have negative implications also for the EU's open strategic autonomy in payments," (COM (2023b, p. 20)). The ECB (2020, p. 12) concludes that by issuing the DE the Eurosystem could ensure that payments in the euro area "are conducted under its direct control". It remains open (and is probably of second-order importance) if direct control is to be achieved by regulatory oversight or by outright ownership.

A related implicit goal may be

IG3: Reduce market share of foreign-owned PSPs, support EU-based PSP's

This is not the same goal as IG2, as control of the payment infrastructure does not preclude the usage (and not even the extensive usage) of this infrastructure by non-EU PSPs. But the Commission notes that in 2016 "the share of transactions processed by international card schemes for payment cards issued in the EU was 67.5%". It further explains that only in nine EU member states "domestic schemes compete with ICS. […] These European domestic card schemes work, however, only within the borders of a single Member State, while the cross-border EU retail electronic payments in physical shops are largely served by ICS or large, often foreign-owned platforms", cf. COM (2023b, p. 20). The Commission concludes that central bank digital money may increase the choices people have both for point-of-sale (POS) and e-commerce payments.

The Commission explicitly aims to preserve the functioning of monetary and financial systems (G5). This functioning involves the ECB's monetary policy. But as Recital (37) and Article 15 (1) of the draft resolution acknowledge, DE holding limits imposed by the ECB may impact its monetary policy stance. This clearly is a concern for the Commission, one reason being that, by Article 127 TFEU, the ECB's monetary policy shall ensure price stability. Hence, another goal – for unclear reasons held implicit - is

IG4: Preserve or even enhance the ECB's ability to fulfill its mandate, i. e. ensure price stability.

Finally, it seems fairly clear that an implicit goal of introducing the DE is

IG5: Strengthen and extend the reach of the Euro beyond the borders of EU and Eurozone.

This can be deduced from the draft regulation where Recital (46) notes that "the distribution of the digital euro … outside the euro area would contribute to foster the international use of the euro". While this is merely a factual statement, ECB (2020) makes clear that such an outcome is indeed desired, cf. "Reasons to issue a digital euro: … (v) to foster the international role of

the euro" (p. 9) and "the Eurosystem might consider issuing a digital euro in part to support the international role of the euro, stimulating demand for the euro among foreign investors" (p. 14).

Moreover, in the draft regulation's explanatory memorandum the Commission reminds readers that "The digital euro has also been identified as an element of the Commission strategy to support the EU's open strategic autonomy," citing consistency with the Commission Communication "Towards a stronger international role of the euro" cf. COM (2018)[3]. But – and this may be the reason for keeping this goal rather low key –Recital (47) emphasizes that there is no intention to undermine monetary sovereignty or replace national currencies in non-Eurozone Member States or elsewhere in the World. Rather, the EU should provide for the "possibility" to conclude agreements with third countries "for the regular provision of digital euro payment services". In simple words: IG5 shall be reached by mutual consent.

Again, implicit goals may be in conflict with each other – or they may be in conflict with explicit goals. For instance, IG2 (enforce use and control of EU-based infrastructure) is bound to contradict IG1 (increase competition in payments services), since IG2 comes at the expense of competing non-EU based infrastructure. Also, IG2 very likely runs counter to G3 (efficiency of payment systems), G4 (resilience) and G1 (foster innovation), as the enforcement of a single piece of EU-controlled infrastructure would restrict technological possibilities and likely reduce profit opportunities.

Also, IG3 (reduce market share of foreign PSPs) may or may not be compatible with IG1 (increase competition) and the Treaty principle of an open market economy with free competition. It would be compatible with IG1 only if foreign PSPs currently enjoy dominant market positions to an extent detrimental to free competition. If that were the case, then rather than introducing a new form of the single currency, the appropriate response would be for the Commission's Directorate-General for Competition (DG COMP) to intervene immediately and enforce EU and national antitrust and anti-collusion laws.

Further, IG5 (extend the DE to third countries) may be in conflict with G1 (foster innovation) and G4 (resilience). For agreements with third countries on the use of the DE would also require consent in terms of regulating innovations in digital finance – and if the third country takes a more cautious approach in this respect, innovation could be hampered. On the other hand, extending DE infrastructure to third countries may give rise to security risks as new interfaces will be created that are beyond the reach of EU or Member State authorities.

While such conflicts between explicit and implicit goals exist, this is not unsual for a legislative proposal. Government objectives are often multidimensional and finding a balance between different objectives may be necessary. However, disagreement may exist over where the optimal balance is. This, basically, is a political decision. From a scientific perspective, the key question is whether one goal can be improved without compromising the others and whether certain designs aimed at specific objectives may have unintended negative effects in other areas.

[3] However, a digital euro is not mentioned in this Communication.

3.3 Non-goals

While quite a few objectives are either explicitly or implicitly specified in the legal text, there also are some non-objectives. By this we mean goals that some people may find reasonable in the context of introducing a digital currency, but the Commission apparently does not share this opinion and, hence, does not mention it – neither explicitly nor implicitly.

For instance, some proponents of alternative digital currencies find it desirable that private agents have freedom of choice with respect to hardware and software they use to manage their digital currency holdings. They argue that software should be open-source rather than proprietary to ensure that no abuse of private data can occur and that there should be no hardware requirements which possibly would result in dependence on only a few selected manufacturers. The Commission does not seem to share this objective or outwardly rejects it, as it is nowhere mentioned in the legal text. Therefore, we have the non-objective

NG1: Freedom of choice with respect to hardware and software.

Another noteworthy non-goal is NG2: Provide central bank money as a store of value for private non-banks.

The absence of this objective is somewhat surprising in light of the Commission's plausible assessment that the use of cash in payments will diminish as the economy digitalizes. At present, private non-banks may hold cash as a store of value and they may prefer cash to commercial bank money for this task since cash is free of issuer risk. If cash is gradually replaced by digital currencies, it could be desirable for the digital euro to inherit not only the transactional function of cash but also its store-of-value function. However, the Commission does not support this approach. On the contrary, its proposed regulation explicitly seeks to limit the store-of-value role of the digital euro (cf. Article 16).

Table 1

Goals and Non-Goals

G1	Provide a catalyst for innovation in payments, finance and commerce.
G2	Reduce the fragmentation of the EU retail payments market.
G3	Enhance efficiency of payment systems.
G4	Enhance resilience of payment systems.
G5	Preserve functioning of monetary and financial systems (by providing a monetary anchor that ensures consumer confidence in commercial bank money)
G6	Safeguard stability of monetary system in a digitalized economy.
G7	Ensure and enhance financial inclusion.
G8	Ensure wide acceptance of the DE.

G9	Preserve the role of the euro in retail payments markets in the face of competition by currencies with advanced digital capabilities.
G10	Detect and prevent criminal activities, e. g. fraud, tax evasion, money-laundering and terrorist financing.
G11	Ensure a high level of privacy and personal data protection.
IG1	Increase competition in payment services and the digital finance sector.
IG2	Reduce dependence on non-EU financial infrastructure, enforce control of EU-based infrastructure.
IG3	Reduce market share of foreign-owned PSPs, support EU-based PSP's
IG4	Preserve or even enhance the ECB's ability to fulfill its mandate, i. e. ensure price stability.
IG5	Strengthen and extend the reach of the Euro beyond the borders of EU and Eurozone.
NG1	Freedom of choice with respect to hardware and software.
NG2	Provide central bank money as a store of value for private non-banks.

4. Analyzing the proposed design of the digital euro

4.1 Scope

As drafted in COM (2023a), the DE shall be a retail currency, cf. Recital (1). Article 16 (1) empowers the ECB to impose holding limits. By virtue of G5 (preserve functioning of monetary system), these limits must be set low – otherwise, commercial banks could face destabilization due to a loss of deposits. For this reason, papers by ECB authors, e. g. Bindseil (2020), Meller and Soon (2023), have proposed holding limits of €3,000 euro for private agents and zero for companies. Such choices would limit the DE to essentially being just a retail currency.

Technically, DE amounts exceeding the holding limits can be transferred due to the so-called waterfall and reverse-waterfall features of DE payment accounts (see below). But if companies have zero holding limits, then DE business to business (B2B) transactions would essentially be transfers of commercial bank money via the DE infrastructure. In fact, companies would have little incentive to make payments in DE, as doing so would require converting commercial bank money into DEs and—given a zero holding limit—immediately passing the DEs on to the payee. It would be simpler and more practical to transfer the commercial bank money directly to the payee.

Hence, there is no compelling reason to initiate DE B2B payments or DE transactions from businesses to private agents unless the DE infrastructure is deemed significantly safer or less costly than existing alternatives. However, a cost advantage appears unlikely, as the ECB must maintain the competitiveness of the current TARGET/TIPS system if it intends to preserve it. Given that private payment infrastructure is generally regarded as secure and reliable, wholesale trade, financial investments, and wage payments are therefore likely to continue relying on commercial bank money rather than adopting the digital euro.

Due to holding limits, the DE falls short of one of the classical functions of money: serving as a store of value. As Bindseil (2020) notes, a holding limit of €3,000 per private agent would roughly correspond to the average monthly net income of euro area households, meaning it would primarily function as money held for transactional purposes. Consequently, the DE would have limited utility as a store of value, increasing the likelihood that customers will prefer commercial bank money as a (also digital) means of payment with broader functionality than the DE.

Holding limits pose a particular problem for the offline version of the DE. Note that Meller and Soons (2023) suggest a DE holding limit of zero for companies in the probably correct anticipation that a nonzero holding limit would allow natural persons to set up legal entities under their control to circumvent and undermine individual holding limits. But if companies have zero holding limits, this also applies to their offline holdings, cf. Article 16 (4). Hence, companies are able to receive offline DE payments only if this is done on a device connected to the internet, such that the offline DEs received are instantly converted into commercial bank money and credited to the company's non-DE payment account.

This, however, implies that usage of offline DEs in interaction with business enterprises requires internet connectivity and is therefore at odds with the contention that the offline DE is useful for payments "in rural or remote areas without a (stable) communication network (Recital 5)[4]. It is also at odds with the assertion in ECB (2024a), that the "offline functionality would enable payments to be made without an internet connection, for example … in locations with limited network coverage, and in the event of power cuts." It rather seems that, unlike cash, the DE is not very useful in such locations or situations.

Another limitation of the DE's functionality arises from its restricted geographic reach, cf. Articles 18 and 19. As proposed, the DE would function as an internal currency within the Eurozone. Unless non-Eurozone countries—whether EU Member States or third countries—sign an agreement with the EU ensuring that their national legislation aligns with all relevant EU laws governing the DE, Eurozone residents will generally not be able to make or receive payments in DE when transacting with non-Eurozone residents. This stands in stark contrast to euros in the form of commercial bank money or cash**,** which are widely accepted outside the Eurozone, particularly in countries with a high volume of Eurozone tourists.

---

[4] The ECB (2020) also highlights "extreme events" such as cyber incidents and attacks, recommending the establishment of "back-up systems" and "resilient channels that are separate from other payment services and can withstand extreme events." However, other forms of disruption—such as power outages or internet connectivity failures—would still prevent companies from receiving offline digital euro payments. This is because a zero-holding limit would require an active connection to the private payment infrastructure in order to convert received digital euros into commercial bank money, rendering offline functionality ineffective under such conditions.

The Explanatory Memorandum mentions the DE serving "future use cases in industry 4.0 and web3", and Recital 55 further elaborates on "payments between machines". However, both the prescribed account-based architecture with holding limits tied to legal entities, and the fact that DE is not programmable money (Art. 24(2)) contradict this statement. As such, the DE does not cover additional use-cases that would give it an advantage over cash or commercial bank money, or could make it a contender to innovative programmable means of payment.

Hence, in terms of scope, the DE has no advantage and three important limitations compared to cash or commercial bank money: It is primarily limited to retail payments, lacks a significant store-of-value function, and cannot be used while traveling in non-Eurozone countries unless a contractual agreement exists between the respective country and the EU. These constraints pose challenges to achieving goal G8 (wide acceptance of the DE) and implicit goal IG5 (extend reach of euro to non-euro countries). In terms of scope, commercial bank money and cash appear to be clearly superior. Whether the DE offers a competitive advantage over these traditional means of payment in other respects remains to be seen.

Takeaway 1:

The DE's scope is significantly narrower than the scope of cash and commercial bank money, as the DE is primarily limited to retail use, has holding limits that hinder its role as a store of value, and cannot be used outside the Eurozone without agreements. These constraints make commercial bank money and cash more functional and widely accepted, raising doubts about whether the DE will be widely accepted.

4.2 Risks

4.2.1 Insolvency risk and risks to financial stability

One reason why the DE might be preferred to commercial bank money (but not to cash) is the lack of insolvency risk for the issuer. By Article 4 (2), the DE shall be a direct liability of the Eurosystem, just like banknotes. In the case of a banking crisis or even an actual run on private credit institutions, DE holdings are free from insolvency risk of the bank where the DE user has a digital euro payment account (DEPA). In this respect, holding DE is just as good as holding cash.

For a private agent, the DE is free from insolvency risk, unlike commercial bank money. However, how would the DE impact the insolvency risk of banks? Beyond banknotes, the DE would introduce a second form of central bank money accessible to customers, providing an additional option for converting deposits during a banking crisis. Any conversion of commercial bank money into DE or cash would put pressure on bank reserves, potentially increasing the risk of insolvency.

Article 13(3) grants DE users the legal right to convert their commercial bank money into DEs "at any point in time, on a continuous basis"—a process known as "funding." ("Defunding" is the reverse operation.) This right is also endorsed by the ECB: "PSPs would have to make digital funding and defunding functionalities available to end users on a 24/7/365 basis" (ECB, 2023b, p. 22). Consequently, in times of banking crisis, customers can convert their deposits

into central bank money instantly and with minimal effort—subject, of course, to the DE holding limit.

By contrast, if banknotes are the only form of central bank money available to private agents, customers must physically visit an ATM or a local bank branch to convert deposits into cash. During a banking crisis, this may mean waiting in long lines, encountering closed branches, or finding ATMs depleted of banknotes[5]. The bank's loss of reserves would be significantly slower if customers lacked an instant, digital method to convert (portions of) their deposits into central bank money. In this regard, the DE—or more specifically, Article 13(3)(a)— conflicts with goal G6 (stability of the monetary system).

To address this issue, note that Article 13(3) is not fully coherent with Articles 8 and 12(1). Article 12(1) establishes that the DE and cash are always equal in value, and Article 8 designates both as legal tender. Yet, despite this formal equivalence, Article 13(3)(a) effectively grants customers a legally enforceable right to have their bank deposits[6] paid out in DE rather than in cash, up to the DE holding limit. In this case, banks cannot fulfill their obligation by offering cash as a substitute. If banks could opt to pay out deposits exclusively in cash, their inevitable loss of reserves during a crisis would not be further exacerbated by the ability of customers to instantly and effortlessly convert deposits into DE.

On top of DE funding by deposits, Article 13(3)(b) also obliges PSPs offering cash services to make available to customers the functionality of DE funding and defunding via euro banknotes and coins — but without the provision that this must be possible "at any point in time, on a continuous basis."

Lawmakers might consider amending Article 13(3) to allow banks—perhaps only under extreme circumstances and with ECB approval—to require that DE funding be conducted exclusively via cash. This would mean that banks are not always obliged to provide DE funding under Article 13(3)(a) but could, in emergencies, invoke Article 13(3)(b) instead, relieving them of the obligation to disburse central bank money instantly and on a 24/7/365 basis. While commercial banks' liabilities toward customers would, of course, remain unchanged, this modification could significantly slow reserve depletion in times of acute crisis.

A second, more economic remedy of the problem would consist in setting incentives for customers to always hold money on the DEPA (up to the holding limit) and use non-digital euro payment accounts only to the extent that their money holdings exceed the DE holding limit. In this case, DEPAs could hardly be used as an outflow option for deposits in the case of a banking crisis, but, of course, banks would have a permanently lower level of deposits also in normal

---

[5] If just a single bank is in trouble, customers do not necessarily need to line up for cash; they can also transfer their deposits online to other banks. However, this process would still be slower than moving deposits to their DE account, as the troubled bank may delay the transfer until the close of business. Additionally, the customer may need time to assess whether the receiving bank is truly a safe haven or if contagion could spread and affect it as well. And, of course, the customer must already have a payment account with the receiving bank—opening one would take additional time.

[6] A technical point: The wording of Article 13(3) (a) does not make it clear whether customers' right to fund the DE with deposits applies only to funds in the non-digital euro payment account linked to the DEPA (cf. Article 22 (4)) or to all payment accounts the customer holds with the same PSP. Since transferring commercial bank money between accounts at the same institution is not necessarily instantaneous, this distinction is significant and should be clarified by lawmakers

times. The obvious way to set such incentives would be a slightly higher interest rate on DEs (to be paid by the Eurosystem) than on commercial bank money.

However, Article 16(8) of the draft regulation explicitly rules this out: "The digital euro shall not bear interest." This provision clearly interferes with the ECB's independence, as interest rate policy falls within the domain of monetary policy. Consequently, the ECB's opinion on the draft regulation challenges Article 16(8) on principle, defending its "primary law competence to independently define and implement monetary policy" (cf. ECB 2023a, 10.7). At the same time, the ECB emphasizes that "it cannot be stated firmly enough that the ECB is not developing a remunerated digital euro." Hence, unless the ECB changes its stance, the second remedy will be infeasible. Nevertheless, it would be advisable to delete Article 16(8), as such a provision exceeds the co-legislators' competence.

Takeaway 2:

The digital euro, like cash, is free from issuer risk, as it is a direct liability of the Eurosystem, whereas commercial bank money carries the insolvency risk of the issuing bank. However, the DE's seamless convertibility from deposits slightly increases the risk that financially strained banks become illiquid, making it more likely that customers lose remaining deposits compared to the current monetary system.

4.2.2 Security risks and risks to privacy – offline version

Article 23 (1) requires that "the digital euro shall be available for both online and offline digital euro payment transactions". Offline DEs, intended for payments "in close physical proximity" (Recital 75), are to be stored on local storage devices, e. g. "smart phones, tablets, smart watches and wearables of all kind" (Article 2 (31)). We first discuss risks from offline usage of the DE:

Offline payments shall be settled instantly by updating the records of DE holdings on local storage devices, as referenced in Article 30 (1) and (3). For offline transactions, no personal data of the payer or payee is recorded, except when DEs are funded or defunded on the devices (Article 34 (1)). Consequently, the privacy level of offline DE transactions, as outlined in the draft regulation, is high and comparable to that of cash payments.

However, the Commission is empowered to impose holding and transaction limits on offline DEs through an implementing act (Article 37 (5)). Exercising this authority, the Commission could significantly restrict the scope of payments that benefit from cash-like privacy. First, it may set an offline DE holding limit significantly lower than the overall DE holding limit established by the ECB. Second, it can further impose transaction limits based on anti-money laundering (AML) measures and efforts to prevent terrorist financing.

Note that this would be carried out through an implementing act under Article 292 TFEU. Implementing acts do not require approval from Parliament or the Council, nor can they be revoked by the co-legislators. Instead, they are subject to a comitology procedure, in which experts appointed by national governments advise the Commission on how to shape the act.

We suggest that lawmakers consider replacing the implementing act with a delegated act, which would require approval by the co-legislators, or alternatively, eliminating Commission-imposed holding and transaction limits from the DE regulation altogether. If such powers are deemed

necessary, the Commission should be required to obtain them through ordinary AML legislation[7].

Needless to say, any holding or transaction limit on offline DE puts it at a disadvantage compared to cash. Even if similar limits were imposed on cash, they would be difficult to enforce and easily circumvented. Cash allows privacy for holdings and transactions precisely at amounts that are out of reach for offline DEs due to these limits. On the other hand, cash, like the DE, carries zero issuer risk. Hence, privacy concerns may weigh heavily against achieving the goal of wide acceptance (G8), as they create a strong incentive for individuals to prefer cash over offline DE.

The security of offline DEs depends on the tamper resistance of hardware. Article 35 (1)(c) assigns the responsibility for "safeguarding the security and integrity of … local storage devices" to the Eurosystem. It is not clear if the Eurosystem can live up to this responsibility. Grothoff and Dold (2021) argue that "hardware protections typically fail against well-equipped adversaries with ample time and expertise" and point out that vulnerabilities have eventually led to successful attacks on all major hardware security architectures, including those of Intel, Samsung, ARM, AMD, and SIM cards.

Once compromised, devices storing offline DEs could be exploited for multi-spending[8]. While counterfeit banknotes typically exhibit detectable deviations from genuine ones, unauthorized copies of DEs – as any digital copy – are truly identical and thus indistinguishable. Moreover, such copies could be produced and used in payments without limit, meaning the financial damage could be unbounded.

Whatever the reason, any event of multi-spending will remain undetected until the – potentially transitive – recipient tries to deposit the offline DE after reconnecting to the Internet. It is highly unclear how this aligns with the instant settlement of offline DE transactions laid out in Article 30 (1). Surprisingly, the draft regulation is entirely silent on the question of liability for such damage: Would responsibility fall on the user, the device manufacturer, or the Eurosystem? Under what circumstances would one of these actors be held liable?

If lawmakers wish to promote adoption of the offline DE, they should consider introducing explicit rules that limit or exclude user liability—except in cases of intent or gross negligence. Although such limitations may already follow from general principles of law, codifying them would reduce legal uncertainty and provide greater assurance to both DE users and device manufacturers as they evaluate potential financial risks. More fundamentally, imposing liability on offline DE users would presuppose the ability to trace individual transactions. Yet Article 34(1) explicitly prohibits the processing of personal data for offline DE transactions, except at the moments of funding and defunding. The promise of anonymity therefore implies a structural barrier to holding users accountable after the fact. In this light, a general exclusion of user liability appears not only reasonable but also a logical corollary of the regulation's own privacy commitments.

Since offline DE functions as a bearer-based payment instrument, neither a PSP nor the Eurosystem is involved in transactions or able to verify the authenticity of transferred DEs.

---

[7]. Article 16 (4) of the draft regulation states that „the holding limit for offline digital euro [is] set by digital euro users", but this limit must not exceed any limit imposed by the Commission on the basis of Article 37 (5).

[8] We prefer "multi-spending" to the more widely used "double-spending" since it seems a more accurate description of the problem.

Such checks are only possible when offline DEs are funded or defunded—that is, when the user connects his device to his PSP. Consequently, fraud can only be detected with a delay, undermining goal G10. If the offender owns the compromised device used for multi-spending, he might be able to indefinitely avoid reconnecting to a PSP. If, instead, the offender manipulated someone else's device and transferred the forfeited DEs from there, the anonymity of offline payments might make it impossible to trace the forfeited DEs back to their criminal originator. It is worth noting that Article 32 explicitly restricts fraud detection and prevention mechanisms to the online DE.

For this reason, Article 37(3) requires PSPs to provide funding and defunding data to Financial Intelligence Units (FIUs) and other competent authorities upon request[9]. Such data would likely include transaction amounts, account numbers, and device identifiers.

It remains unclear whether the personal identification of offline DE users—whether as victims or suspects of fraud—would be permitted under Article 37(2). Additionally, it is uncertain whether funding and defunding data alone, no matter how comprehensive, would suffice to detect and combat DE forgery[10]. The ECB (2024b) vaguely refers to a "minimum amount of data compatible with the need to detect forgery," leaving open the question of whether detecting fraudulent activity in offline DE would also, despite Article 34 (1), necessitate storing transaction data and, in in suspicious cases, disclosing it to competent authorities[11].

Tampering with offline DE devices—whether by foreign nation-state attackers or organized crime—could cause significantly greater financial damage than traditional banknote forgery. It may therefore be proportionate to impose lower privacy standards for offline DE than for cash. However, while this rationale may be valid, it does not change the likely perception among private actors that cash remains less susceptible to financial loss due to criminal activity—and consistently reliable in terms of privacy. This reinforces concerns that achieving goal G8 (wide acceptance) for offline DE may be difficult.

The risk of multi-spending and undue money creation resulting from successful attacks on hardware security is also underscored by a formal theorem in computer science, derived by Gilbert and Lynch (2002). Their work proves the impossibility of designing a distributed system (such as a web service) that simultaneously satisfies three desirable properties: consistency, availability, and partition tolerance (CAP).

Applied to DE, consistency requires that multi-spending and undue money creation are prevented, availability means that payments can be initiated and received at any time, and partition tolerance allows (parts of) the system to function even when (temporarily) offline.

---

[9] Competent authorities are those defined in Article 2(31) of the proposed Anti-Money Laundering Regulation (COM/2021/420 final), including financial supervisory authorities responsible for AML/CFT compliance. The ECB appears to fall within this definition, as it serves as a supervisor for significant credit institutions under the Single Supervisory Mechanism (SSM). While the ECB is not an AML/CFT authority in itself, ensuring compliance with AML/CFT regulations is an integral part of its prudential supervision within the SSM framework.

[10] This may be clearer with the following example: Person A funds his device with offline DE and pays B. B is a criminal who manipulated his device to double-spend the DEs, paying C and D. When C and D defund, one of them fails, but the defunding data would not reveal B.

[11] Note that Article 32 of the draft regulation envisions an ECB-operated "general fraud detection and prevention mechanism." This mechanism is intended as a service for PSPs and applies exclusively to online DE. It remains unclear why a similar ECB service for offline DE has not been proposed.

Consequently, the so-called CAP theorem implies that offline DE, by being partition tolerant, must necessarily compromise either consistency or availability (or both).

In simple terms: offline DE cannot be both duly protected against multi-spending and available to users at all times.

This is a fundamental issue for the concept of offline DE. Whether the Commission is unaware of the CAP theorem or has deliberately chosen to ignore it in the draft regulation remains unknown. However, the inherent incompatibility of the desirable CAP properties clearly makes cash a more reliable bearer-based payment instrument than offline DE, thereby undermining goal G8. Moreover, is is hard to see how goal G4 (enhance resilience of payments systems) can be achieved with a currency whose offline version is either sometimes not available or vulnerable to fraud (or both).

Lawmakers might conclude from this insight that consistency and availability should take precedence over partition tolerance. This would imply abandoning the offline DE entirely, thereby reducing the overall system complexity as only one DE (online) would remain, or limiting offline DE to a backup payment solution for emergency situations in which online DE or other forms of online payments are unavailable or insecure.

Finally, there is a substantial risk that the anonymity of offline DE transactions may open new avenues for criminal activity. Criminals could use well-known relay attacks (cf. Tu and Piramuthu 2020) to "simulate" proximity payments between devices over the Internet, effectively enabling offline DE transfers between devices that are not in physical proximity at all. Extortion and blackmail could be used to force victims to transfer offline DEs to the coercer's device. If anonymity holds, the perpetrator would be untraceable and, in any case, would face a significantly lower risk of being caught than when demanding cash payments or transfers of commercial bank money.

In this context, it should be noted that digital crime can be automated, affecting a large number of potential victims simultaneously. Hence, the fact that devices will have low holding limits for offline DE does not prevent criminals from appropriating substantial sums of money: each individual victim may contribute only a small amount, but scale effects make the effort worthwhile from a criminal perspective. Moreover, if blackmail involves information the victim is determined to keep undisclosed, a significant share of such criminal activity may go undetected - especially when the financial loss to the victim is relatively small.

Takeaway 3:

In terms of privacy, cash dominates offline DEs due to caps and geographical limits beyond which offline DE users can no longer benefit from its cash-like level of privacy. For the same reason, its store-of-value function is inferior to cash. Offline DEs, relying on hardware integrity, are less secure than cash and may carry higher liability risks for users and even pose a financial threat to the Eurosystem. Yet they have no superiority over cash in terms of issuer risk. Also, offline DEs cannot be both always available and immune to fraud, violating G4 and possibly G10. Taken together, users are likely to perceive cash as superior to offline DE. This is different for criminals, who may find digital anonymity attractive for conducting extortion and blackmail on a large scale.

4.2.3 Security risks and risks to privacy – online version

Turning to the online version of the DE, its distribution also relies almost entirely on PSPs. Under Article 13, PSPs are required to offer their customers the opportunity to open DEPAs and manage their DE payments using the PSP's payment services. Customers have the option to link their DEPAs to a non-DE payment account (NDEPA) at their PSP, such that any DE holdings exceeding the holding limit are automatically transferred to the linked NDEPAs (the so-called "waterfall" mechanism) and any DE payments surpassing the available DE balance are automatically covered by funds from the linked NDEPA (the so-called "reverse waterfall" mechanism). Since Article 13(6) stipulates that DE users will have no contractual relationship with the Eurosystem, PSPs serve as the only point of contact for DE users.

This design inherently leads to the security of online DE payments being equal to the security provided by the user's PSP for transactions involving commercial bank money. PSPs will integrate DE management into their existing systems and safeguard its integrity using the same mechanisms they employ to protect commercial bank money. Likewise, PSPs will connect to the Eurosystem's DE infrastructure in the same way they trade and manage their reserves.

As a result, security alone neither incentivizes nor discourages the use of online DE.

The situation is different, though, when it comes to privacy. For online DE transactions, PSPs must collect and store exactly the same data as they do for online transactions involving commercial bank money. These non-anonymized data are stored in a decentralized manner, distributed across PSPs.

However, unlike commercial bank money, the ECB's digital euro settlement infrastructure will also record all individual transactions centrally (cf. Article 30(2)). But transaction data communicated to the Eurosystem must not include personal information that could be used to "directly identify individual digital euro users" (cf. Articles 34(4) and 35(4)).

This design raises privacy concerns: Article 30(1) and (2) stipulate that online DE transactions must be settled instantaneously "at the moment of recording the transfer of the digital euros concerned from the payer to the payee." The fact that transfers are recorded from payer to payee (!) suggests that the ECB would not only have access to all transactions but also to the unique DEPA identifiers involved. As required by Article 34(4), PSPs must segregate account holders' names and other personal data from the unique DEPA identifiers, meaning the Eurosystem would not be able to directly identify individual DE users. But what about indirect identification on the basis of DEPA identifiers?

Scientific evidence suggests that pseudonymized payment data can be used for individual re-identification (cf. Lubarsky, 2017). Kikuchi (2021) highlights that the likelihood of successful re-identification increases with the number of records linked to a pseudonym. Such indirect identification would, in fact, be legally permissible, as the draft regulation prohibits only direct identification. Moreover, account switching in "exceptional circumstances" directly via the ECB's infrastructure circumventing the normally involved PSP as established in Article 31(2) suggests that the ECB will have access to personal information[12].

---

[12] This is also confirmed by Recital 76 of the proposed Regulation: "The European Central Bank and national central banks may process personal data in so far as it is necessary to fulfil tasks that are essential to the proper functioning of the digital euro. […] The European Central Bank and national central banks would process personal

While we have full confidence that the ECB has no intention of re-identifying DE users, some—perhaps many—DE users may be more skeptical. As ECB (2024) states: "The public consider privacy and data protection to be two of the most important design elements of a digital euro." The mere fact that re-identification is both legally and technically feasible could fuel, for instance, misperceptions about secret mass surveillance, ultimately undermining trust in the DE and harming the wide acceptance goal (G8)[13].

Such fears could be mitigated if lawmakers chose to prohibit any form of identification, including indirect identification, and implemented measures ensuring that the Eurosystem could not link transactions to fixed pseudonyms. For instance, it would suffice to inform the Eurosystem that a DE transaction, uniquely identified by a random identifier, is taking place between two PSPs acting on behalf of undisclosed customers. Simultaneously, DEPA account numbers linked to the random identifier would be transmitted directly between the PSPs, bypassing the Eurosystem. In fact, the system could be set up such that the receiving PSP is informed only about the amount and the account to be credited, but not about the account to be debited at the payer's PSP. Moreover, the ECB would not learn which individual accounts are involved in a DE transaction, but would merely be notified of a DE transfer between the payer's and the payee's PSPs, cf. Dold (2019).

Such an approach would closely resemble the handling of commercial bank money transfers, where the Eurosystem is involved only in the transfer of reserves between commercial banks, without access to information about the specific customer accounts associated with the transaction. It would even provide greater privacy as today, since, unlike today, the payer's identity would not be revealed to the payee's PSP.

Takeaway 4:

Online DE and commercial bank money offer equal security. They have similarly low privacy at the PSP level, but central storage of pseudonymized transaction data raises re-identification concerns unique to the DE, possibly undermining goal G11 (ensure protection of personal data).

4.2.4 Legal liability in case of security breaches

A striking omission in the Commission's proposal is its silence on the issue of liability in case of theft, security breaches, or malfunctions in the operation of the digital euro—be it in its online or offline version. Unlike commercial bank money, the DE is a direct liability of the ECB (Article 4(2)), not of the payment service provider (PSP) facilitating access to it. Thus, the liability regime laid down in the EU's Second Payment Services Directive (PSD2), which governs the responsibilities of PSPs in the event of unauthorised payments or fraud, cannot be straightforwardly applied to the DE.

---

data for these tasks using state-of-the-art security and privacy-preserving measures, such as pseudonymization or encryption, to ensure that data cannot be used to directly identify a specific digital euro user."

[13] Such concerns might be reinforced by the fact that Article 35(8) empowers the ECB to maintain a system of unique "user identifiers" that unambiguously distinguish DE users and to "establish a single access point of digital euro user identifiers and the related digital euro holding limits." This centralized access point is necessary for PSPs to enforce the overall DE holding limit for users with multiple DEPAs. However, there may be concern that user identifiers associated with specific DEPAs could facilitate re-identification.

This raises fundamental questions: If, for instance, a criminal hacks into a DE-enabled device or account, creates digital copies of the DE, and succeeds in spending them multiple times before detection, who would be liable for the financial damage? Would the user bear the risk, despite not having contributed negligently to the breach? Would the PSP be liable, even though it neither holds the DE on its balance sheet nor controls its issuance or verification? Or would the liability fall to the Eurosystem, which ultimately issued the compromised digital euro units?

Article 35(1)(c) makes the Eurosystem responsible for safeguarding the integrity of local storage devices in offline DE usage, but does not address the consequences if such integrity fails. Similarly, Article 13(6) rules out any contractual relationship between DE users and the ECB or national central banks, further obscuring the legal channels through which compensation claims might be raised.

European law defines PSP liability extensively under PSD2 (cf. Articles 73–92), but it contains virtually no provisions addressing the legal liability of the ECB vis-à-vis private agents. Article 340(3) TFEU establishes that the ECB is liable only "in accordance with the general principles common to the laws of the Member States" and only for damages "caused by its servants in the performance of their duties." This leaves significant uncertainty about ECB liability for system-wide flaws, institutional negligence, or even passive omission to prevent known vulnerabilities.

Lawmakers may therefore wish to consider inserting explicit provisions in the DE regulation that clarify the liability framework for both online and offline usage. Without such provisions, legal uncertainty may undermine the very trust in central bank money that the DE is intended to bolster.

Takeaway 5:

The introduction of the DE entails many open questions concerning liability rules in the event of theft, malfunction, or security breaches. As the DE constitutes a direct liability of the ECB rather than of the PSP, existing provisions under PSD2 may not be applicable, justified or proportional. The draft regulation remains silent on whether users, PSPs, or the Eurosystem would bear responsibility for financial loss in such cases. This legal ambiguity may severely undermine confidence in the DE, i. e. goal G8 (wide acceptance).

4.3 Costs

The costs associated with the introduction and use of the digital euro (DE) can be either direct or indirect. Direct costs can be divided into four categories: those borne by the Eurosystem, PSPs, merchants (retailers), and households (customers).

Regarding the latter, Recital 40 explicitly states that "natural persons …should not bear any direct fees for their basic access to and basic use of the digital euro." Basic DE usage is defined in Annex 2 of the draft regulation (COM (2023c)) and includes, among other features, waterfall and reverse waterfall functionalities as well as point-of-sale (POS) DE transactions.

Article 17(1), however, prohibits only PSPs from charging fees to natural persons. To align it with Recital 40, lawmakers should make clear that merchants, not just PSPs, are also barred from imposing such fees.. This prohibition is necessary because, under Article 7(2), the DE is designated as legal tender at full face value. As Recital 42 correctly highlights, any transaction

fee—whether imposed on the customer or the merchant—effectively reduces the face value of a payment, contradicting the principle established in Article 7(2).

One might argue that the legal tender status at full face value, as laid down in Article 7(1) and (2), implicitly precludes surcharges on digital euro payments. Still, greater legal clarity would be achieved by including an explicit ban on such fees in Article 17. Moreover, if the prohibition on fees is indeed implicit in Article 7, it would apply equally to natural and legal persons. It is therefore unclear why Recital 40 limits the fee prohibition to natural persons alone.

It is also difficult to understand why a merchant service charge—defined as "a fee paid by the payee to a payment service provider when acquiring a digital euro payment transaction"—is explicitly permitted under Article 17(2), while PSPs would be prohibited from charging natural persons for receiving or initiating digital euro payments. Within this legal framework, merchants may attempt to circumvent such charges by authorising natural persons to receive and initiate the company's digital euro transactions free of charge. Waterfall and reverse waterfall functionalities could then be used to convert digital euros into or from commercial bank money at no cost, with the actual financial settlement between the natural person and the company taking place exclusively in commercial bank money.

In any case, merchants and PSPs would pass on their uncovered DE costs by raising prices for goods and services, meaning that customers ultimately bear these costs indirectly[14]. Since most customers will likely be unaware of this, the perception of DE as cost-free would support—or at least not hinder—the goal of wide customer acceptance (cf. G8). Merchant acceptance, on the other hand, is enforced through Article 7(2) and (3), which makes DE acceptance mandatory, subject to exceptions for microenterprises and non-profit legal entities outlined in Article 9 and motivated in Recital 18.

Mandatory acceptance (Article 7(2)) requires all enterprises exceeding a certain size, as defined in Article 9(a), to implement and maintain the necessary technology for receiving DE payments and to bear any operational costs related to DE transactions. PSPs are explicitly allowed to charge merchants for DE services, up to a certain limit, cf. Article 17 (2) and (6). While other electronic payment systems (e.g., credit cards) also impose costs on businesses, accepting such payment technologies remains voluntary. Hence, to reduce expenses, companies may choose to replace non-mandatory payment systems with the required DE infrastructure, even if they consider existing technologies to be technically superior, more user-friendly, or more widely accepted.

In this respect, mandatory acceptance contributes to goals G2 (reduce fragmentation) and G8 (wide acceptance) but may undermine G3 (efficiency of payment systems) and G1 (promote innovations). Regarding implicit goals, mandatory acceptance supports IG2 (greater EU control over payment infrastructure) and IG3 (reducing the market share of foreign PSPs), but it likely conflicts with IG1 (increasing competition).

Like merchants, PSPs also incur additional—and potentially significant—costs in providing DE services to their customers. Article 14(1) obligates retail credit institutions to offer all basic DE

[14] There is no strong case for distributional concerns in this context. While the indirect costs passed on through higher prices are borne by all customers rather than solely by DE users, customers who pay with cash or commercial bank money also generate handling, transaction, or payment infrastructure costs for merchants. These costs are also reflected in prices, meaning that DE users pay for technologies they do not use, just as users of other means of payment do.

payment services upon customer request. Consequently, these institutions must integrate DE functionality into their software and security systems, ensure proper maintenance, provide customer support, and enforce compliance with AML/CFT regulations under Directive (EU) 2015/849, commonly referred to as Know-Your-Customer (KYC) requirements.

In fact, PSPs serve as the sole point of contact for DE users in all other matters related to DE usage, while the ECB and national central banks (NCBs), as the bearers of the DE liability, have no direct interaction with DE users. Yet by Article 13(1), PSPs must not charge the costs of basic DE services to natural persons. The draft legislation leaves open the question how PSPs may recover the costs they incur from handling a liability that is not theirs.

The natural solution would be for the Eurosystem to compensate PSPs for their costs. Since the draft regulation lacks such a provision, PSPs will need to offset their DE-related expenses by increasing fees for other services or reducing interest rates for depositors.

This could trigger a substitution effect: customers may favor the cost-free DEPA over NDEPAs or other deposit accounts if the latter become more expensive or provide lower returns than before the DE's introduction. By legally mandating free basic DE services, the draft regulation promotes wide acceptance (G8) but simultaneously makes traditional banking services less attractive to customers. DE holding limits (Article 16(1)) may be necessary to prevent serious risks to goal G6 (safeguarding the stability of the monetary system).

Since there are no direct costs for basic DE payment services, most DE users will perceive the DE as cost-free, and even those who do not use it may be unaware that they indirectly contribute to its financing through higher bank fees or lower interest rates.

Turning to the costs of the Eurosystem, Recital 41 states that the Eurosystem will not charge PSPs "for the costs it bears to support their provision of digital euro services to digital euro users." PSPs, however, may view this perspective as entirely inverted: DEs are neither an asset nor a liability on their balance sheets, PSPs have no commercial interest in offering basic DE payment services—since these are inherently unprofitable—and they do offer them solely to comply with a legal obligation. This, however, serves the interests of the Eurosystem rather than their own. In other words, PSPs may see the Eurosystem as outsourcing its own responsibilities, effectively compelling private financial institutions to manage core functions of a central bank digital currency—a task that, in their view, should fall to the Eurosystem itself.

It is peculiar that Recital 41 has no analogue in the legal text. Specifically, Article 17, which regulates fees for DE payment services, does not prohibit the ECB from charging PSPs fees. This is even more surprising as Recital 41, unconventional for a recital, is a factual statement rather than an explanation or justification of a legal stipulation. This seems to be a flaw in the draft regulation that lawmakers should correct.

Suppose the Eurosystem does indeed cover its own costs, such as those for DE development, central bank infrastructure, and central clearance. This would reduce the profits of national central banks and, in turn, their contributions to national budgets. Taxpayers would ultimately bear the shortfall. Thus, the DE is certainly no free lunch: it adds to the existing costs of payment systems, and these costs are ultimately borne by private agents—either through higher prices for goods and services or through reduced government resources.

However, it is also possible that the Eurosystem will offset its costs by drawing on PSPs. Recital 9 - once again, a recital not reflected in the regulation's Articles - suggests issuing DEs by

converting PSPs' central bank reserves into DE holdings. Since credit institutions hold nearly all their reserves in the ECB's deposit facility (where they are remunerated at the deposit facility rate (DFR)), this issuance method would lower the ECB's interest expenses—effectively cutting into a risk-free component of bank income[15].

For example, if the DFR is at 2% and the total volume of issued DEs amounts to €1 trillion, as assumed in a back-of-the-envelope calculation by Bindseil and Panetta (2020), this would generate €20 billion per year—far exceeding the Eurosystem's DE-related costs. Historically, however, European central banks have operated under regimes of reserve scarcity. Under such a system, the ECB would not be able to offset its costs simply by reducing reserve remuneration.

Takeaway 6:

Wide acceptance (G8) of the DE is legally enforced by obligating PSPs to charge no fees for basic DE payment services to end users and by requiring most commercial enterprises to accept DE payments. But who bears direct costs matters little, as all expenses are ultimately borne by private agents.

Takeaway 7:

While users are led to believe that the DE is cost-free, this is a misperception. Unless other payment technologies are greatly reduced in volume or entirely eliminated from the market, the DE imposes yet another layer of costs on private agents, adding to the overall burden of payment systems.

4.4 Convenience and inclusiveness

Convenience is a key factor in ensuring the wide acceptance of the DE (G8). There is little doubt that the online version of the DE will, in principle, be just as easy to use as commercial bank money. But this is true only for people with a reasonable degree of digital competences - and provided their DEPAs are linked to their NDEPAs via the waterfall and reverse waterfall mechanisms, enabling automatic funding and defunding of online DEs. However, if a customer chooses not to use the waterfall options, the DE holding limits make DE payments significantly less convenient than online transactions with commercial bank money, card payments, or other well-established private digital payment methods such as PayPal.

Moreover, people with limited digital skills or economic knowledge may find the distinctions between offline DE, online DE and online commercial bank money confusing and rules about holding limits offline and online across devices and accounts partially associated with waterfalls up and down difficult to grasp. The same applies to the as-of-yet unknown and increasingly demanding security and authentication requirements for either form of euro and (temporary)

[15] The remuneration of excess reserves currently provides Eurozone banks with substantial risk-free interest income on fully liquid assets. Lucke and Meyer (2024) argue that this income is undeserved and should be taxed away. Issuing DEs by converting reserves would represent a significant step in that direction, though commercial banks would still retain approximately two-thirds of this undeserved income.

dysfunctionalities that sometimes come along with software updates on private devices. Last but not least, consumers may, view the payments market as annoyingly fragmented when at checkout they are given the choice between many different payment methods, e. g. cash, credit card, giro card, online DE, offline DE, Paypal, Wero, Apple Pay, Google Pay etc. Such a perception would clearly contradict goal G2 (reduce the fragmentation of the payments market).

Payments with offline DE are likely far less convenient than those with its non-digital counterpart, cash. A proximity connection must be established between the payer's and payee's devices, yet devices may fail to detect each other—whether due to unknown technical issues or user handling errors. To initiate or receive a payment, users will likely need to authenticate themselves on their devices, presumably using high-security measures such as two-factor authentication (2FA). Additionally, holding limits on either device may prevent a transaction from being completed. By contrast, cash payments are unaffected by any of these issues, making them inherently more reliable and user-friendly in everyday transactions.

Since the offline DE is less user-friendly than cash, financial inclusion (G7) is at risk. Elderly individuals, as well as people with disabilities or functional limitations, often face difficulties with digital technologies. The concerns already mentioned for online DE usage carry over to offline use: Authentication procedures have grown increasingly complex and demanding over time, a trend that is likely to continue. Moreover, frequent changes in authentication requirements or the functional design of DE interfaces may pose additional challenges for individuals with limited digital skills. While this issue affects both online DE and commercial bank money, it may be particularly severe where it extends to offline DE. —whereas cash remains entirely unaffected.

Hence, while the draft regulation aims for inclusiveness (Recital 29 and Article 14), it is unlikely that this goal (G7) will be satisfactorily achieved for the offline DE. In fact, if cash usage declines as more people rely on digital payment methods—whether private or official—those who are digitally disadvantaged may ultimately be worse off than they are today, when cash remains a viable alternative.

To address a possible lack of inclusiveness, Article 14 (3) requires Member States (MS) to designate certain entities (e. g. regional authorities or postal offices) to provide digital inclusion support, "face-to-face in physical proximity to persons with disabilities, functional limitations or limited digital skills, and elderly people". The same obligation is imposed on a broad group of PSPs under Article 14 (4). Additionally, the entities designated by MS must also offer basic DE services to individuals without an NDEPA (cf. Article 14(3)).

Various issues arise in these specifications that warrant improvement by lawmakers:

First, Article 14 does not explicitly state that the specified services must be provided free of charge. While this is likely the intention—given that PSPs are prohibited from charging fees for basic DE services and that imposing costs on elderly or disadvantaged individuals for inclusiveness services would be widely seen as unfair—it should be explicitly clarified that these services will not incur costs for customers.

Second, it remains unclear whether asylum seekers, beneficiaries of international protection, third-country nationals without a residence permit whose expulsion is legally or practically impossible, and individuals without a fixed address are also entitled to the (free) services outlined in Article 14(3) and (4). Although this vulnerable group is explicitly mentioned in Article 14(5) in the context of AML/CFT legislation, it is not referenced in the earlier

paragraphs of Article 14. This is a broad and diverse group, many of whom are not elderly, and whose only potential "disability" may be limited proficiency in the domestic language. Lawmakers should clarify whether this qualifies them for inclusion under the provisions of paragraphs (3) and (4).

Third, if digital inclusiveness and basic DE payment services are provided free of charge, the financial burden will fall on designated public entities and PSPs. This burden may be substantial, as the intended beneficiaries are numerous, and each client may require considerable time and assistance. As a result, service providers may attempt to cut costs, leading to lower service quality, long waiting times, or accessibility barriers. This would be counterproductive to achieving the inclusiveness goal (G7).

Takeaway 8:

Offline DE is significantly less user-friendly and far less inclusive than cash. Free support for marginalized or vulnerable individuals will likely suffer from quality shortcomings, making full inclusiveness (G7) difficult to achieve.

4.5 Competition

4.5.1 Competition between DE and private payment solutions

The draft regulation's implicit objective IG1 (increasing competition in payment services) is compatible with the explicit goal G9 (preserving the role of the euro in retail payment markets) if the DE enjoys a competitive edge over private payment technologies or foreign currencies with advanced digital capabilities. However, it is unclear where this competitive edge would come from. In fact, a regulatory framework designed to foster competition and innovation (IG1 and G1) should largely remain neutral regarding the technology and infrastructure used by the DE or its competitors, as long as they enable high-quality payment services that are efficient and resilient (G3 and G4).

Yet, there are two major breaches of this neutrality principle.

First, the draft regulation mandates that the DE be distributed by PSPs (Article 13). The most cost-efficient way of doing this will be that PSPs process DEs through the same infrastructure they use for their own payment services. As a result, the DE infrastructure is – at any point in time -- inherently on equal footing with that of competing private payment technologies for euro-denominated transactions. This design prevents the DE from gaining a competitive edge in this regard, meaning that no competition will occur between the public DE and private solutions at the infrastructure level[16].

Second, Article 24(2) of the draft regulation prohibits the DE from being programmable money. While the ECB may develop techniques that allow conditional payments in DE (Article 24(1)), programmability of the DE beyond conditional payments would conflict with the DE being designed as legal tender that all but the smallest companies have to accept in payment. This

[16] Note that, under Article 13, the DE will use privately provided infrastructure, but the ECB will not compensate PSPs for an appropriate share of the infrastructure costs. In fact, it freerides on infrastructure investment, maintenance and innovations.

being so, it must be ensured that the DE is fully fungible and therefore, programmable features like time limits on DE usage or usage in payment only for specific goods and services must be ruled out.

While the prohibition of programmability beyond conditional payments is reasonable, it imposes a significant technological constraint on the DE. As Recital (7) emphasizes, demand for programmable money may emerge in the future, and it is not at all clear that this demand would be limited to conditional payments, as Recital (7) suggests. Even governments might find enhanced programmability features useful—for instance, to ensure that social assistance is spent only on specific goods and services that clearly benefit the recipient and only at "trusted" shops that would be permitted to convert programmable money into fully fungible euros.

In this perspective, the prohibition in Article 24(2) places the DE at a technological disadvantage compared to competing currencies that offer a broader range of programmable features or private payment solutions denominated in euro. While lawmakers could lift this prohibition at any time if greater flexibility in programmability proves warranted, competing payment solutions may by then have advanced to a degree that makes it difficult for the DE to catch up.

Hence, the legal framework prevents the DE from having superior infrastructure and partially restricts its ability to compete technologically by limiting programmability to conditional payments. Thus, in a competitive environment, the DE appears inherently disadvantaged in achieving goal G9 (preserving the role of the euro in retail payment markets). However, this disadvantage is offset—potentially more than fully—by the regulation granting the DE legal tender status (Article 8) and the advantage of mandatory acceptance (Article 7(2)).

This legal enforcement gives the DE a competitive edge over other payment solutions that customers might prefer if payment systems competed on a level playing field. There seems to be an implicit acknowledgement in the draft regulation that the DE might not be competitive and unable to achieve goal G9 unless competition is distorted in favor of the DE by elevating it to a superior position as the sole digital means of payment that has legal tender status and benefits from mandatory acceptance. The implication of this, however, may be that achieving goal G9 will not be due to the DE being inherently superior to competing payments solutions, but rather coerced by the legal settings.

This leaves us with the question of whether implicit goal IG1 (increasing competition in payment services) will be achieved by introducing the DE. While, trivially, the DE is a new competitor, the important question is whether it will lead to greater competition among non-state digital payment solutions and thereby enhance efficiency (G3) and innovation (G1).

It is hard to see why this should be the case. If a public payment solution—free for customers to use, granted legal privileges over competitors, and entitled to unlimited use of competitors' infrastructure at no cost—enters the market, why should this foster competition among private PSPs that have traditionally served this market? Their market share is likely to decline, and so are their profits. With lower profit potential, investment and innovation are more likely to decrease than increase.

Greatly harmful to innovation is the almost parasitic way in which the DE would utilize private infrastructure. PSPs will have to anticipate that any infrastructure investment or innovation they consider funding will, by law, be made available for DE usage. As a result, such expenditures provide them with no competitive advantage over the DE, making competition based on

technology or quality of service virtually impossible. However, competition along a price or cost dimension is equally unfeasible, as DE usage is free of charge (for basic services), and central banks face neither legal nor economic requirements to operate the DE in a profit-oriented manner.

Takeaway 9:

Infrastructure constraints and limits on programmability put the DE at a structural disadvantage compared to private payment solutions, making it difficult to preserve the euro's role in retail payment markets. Yet, despite its potential inferiority, DE usage is artificially enforced through legal tender status and mandatory acceptance. This setup risks discouraging innovation and investment by private PSPs, ultimately weakening competition in the payments market.

4.5.2 Competition between banks and non-banks

The EU's second Payment Services Directive (PSD2) distinguishes between "account servicing payment service providers" (ASPSPs) and other PSPs. Roughly, ASPSPs are deposit-taking credit institutions (henceforth: "banks"), while other PSPs comprise electronic money institutions, payment institutions, post office giro institutions (henceforth: "non-banks"), as well as Eurosystem or government institutions when acting in specific capacities (e.g., providing DE payment services for unbanked individuals). See PSD2 (Directive (EU) 2015/2366, Article 1) for exact definitions.

The draft regulation treats banks and non-banks differently: While banks are obliged to provide DEPAs and basic DE services upon request of their clients (Article 14(1)), non-banks may, but need not do so (Article 13(1))[17]. See also Recital (28).

As previously noted, providing basic DE services is inherently unprofitable since no fees may be charged. Moreover, when customers fund DE by converting bank deposits, banks must transfer reserves to a designated "digital euro in circulation" (DECA)[18] account at the ECB. Associated with the banks' loss of reserves is a loss of reserve remuneration. Thus, funding DE will typically imply annual losses for banks equivalent to the interest income they would have earned at the deposit facility rate (DFR) on the foregone reserves.

If DE in circulation amounts to €1 trillion and the DFR is 2%, say, total annual funding costs borne by PSPs would be €20 billion. However, under Article 13(1), non-banks can choose not to offer DE services, leaving banks to bear the full funding costs despite being unable to generate revenue from providing basic DE services. This creates an uneven playing field, as the regulation effectively grants a competitive advantage to non-banks. Given that non-banks are often foreign-owned PSPs (e.g., PayPal, Stripe, Worldpay, and US-based credit card schemes), this design appears to contradict implicit goal IG3, which aims to reduce the market share of foreign-owned PSPs and support EU-based PSPs.

---

[17] The wording of Article 13(1) suggests that non-banks may also have the discretion to offer DE services to certain clients while declining to do so for others. Lawmakers may wish to clarify whether this is indeed intended

[18] It appears that no official terminology has been established for this account thus far.

Note, however, that competition between bank and non-bank PSPs is currently severely distorted, as banks receive substantial risk-free income on fully liquid assets due to the ECB's decision to create and remunerate large excess reserves. Banks do not provide any service that justifies these payments, which reduce the dividends the Eurosystem pays out to national budgets (cf. Lucke and Meyer, 2024). As long as the Eurosystem's monetary policy remains in a regime of excess reserves, the unequal treatment of banks and non-banks with respect to DE funding partially offsets the undeserved competitive advantage banks enjoy. In this sense, while one competitive distortion remains, it is somewhat mitigated by another.

However, if the ECB were to return to a monetary policy of scarce reserves, banks would need to borrow reserves to fund DEs for their clients rather than merely forgoing undeserved income. Since the regulatory framework should remain independent of the ECB's monetary policy decisions, it would be preferable to design a system in which no competitive distortions arise under any monetary policy regime.

If non-banks choose to provide DE services, DEPAs at these institutions must be linked to NDEPAs at banks, as most non-banks do not offer account services beyond DEPAs. Consequently, DE funding would still be borne by banks through the loss of interest income on reserves. To address this, Article 17(2) of the draft regulation allows banks to recover distribution costs by charging non-banks a proportionate inter-PSP fee. This fee may include a "reasonable margin of profit" but shall not exceed "fees or charges for comparable digital means of payment". Under Article 17(3) and (4), the ECB is required to regularly monitor and explain relevant developments.

Inter-PSP fees are an appropriate mechanism to ensure that non-banks bear their share of DE funding costs. However, there is no clear need to legally define proportionality criteria for these fees or to assign the ECB a supervisory role in this matter. Non-banks retain the option to refrain from providing DE services altogether, thereby leaving the full burden of DE funding costs with the banks. This gives non-banks a strong negotiating position, and banks have compelling incentives to offer competitive terms to encourage non-banks to participate in DE distribution. Given this dynamic, concerns about potential market power abuse by banks are unwarranted. Lawmakers should therefore consider removing from the draft regulation any provisions related to the proportionality of inter-PSP fees.

Takeaway 10:

The draft regulation creates an uneven playing field by shifting the full burden of DE funding costs onto banks. Since non-banks are often foreign-owned PSPs, this contradicts the implicit goal to reduce the market share of foreign-owned PSPs and support EU-based PSPs. Proportionality rules for inter-PSP fees are unnecessary and should be deleted.

4.5.3 Competition between DE and stablecoins

The explanatory memorandum correctly emphasizes that future developments may see the euro compete with third country CBDCs, crypto assets or stablecoins. In this paper, we focus on just one specific competitor that may arise from this rather broad field of alternative digital currencies: A stablecoin, issued by Eurozone banks and backed one for one with reserves.

Suppose banks call this stablecoin the private digital euro (PDE). Each bank can issue PDEs by segregating the corresponding amount of euro reserves from its general reserve holdings. Segregation means putting reserves under the legal control of an independent fiduciary charged to ensure that segregated reserves are always at least equal in value to issued PDEs. PDE holders are contractually granted superiority claims on segregated reserves in case of bankruptcy and an instant convertibility of PDEs into cash or DE at any point in time, even if under insolvency procedures. Hence, PDEs would be equally safe as the DE in terms of issuer risk.

If clients request to convert cash or deposits into PDEs, each bank can issue the corresponding PDEs and credit them to a PDE payment account (PDEPA) created in complete analogy to DEPAs. Waterfall and reverse waterfall functionalities between the client's PDEPA and his NDEPA can also be established. But since there are no holding limits on PDEs, a waterfall functionality is actually not necessary.

As long as the ECB conducts monetary policy in a regime of excess reserves, banks would still earn DFR interest income on segregated reserves. Hence, in terms of interest income, the PDE is Pareto-superior to the DE for banks and their clients. If the DFR is 2%, banks could offer customers 1% interest, say, on PDEPA holdings. Clients will prefer this to the 0% interest envisaged for DEPAs under Article 16(8) and banks will find PDE issuance profitable with a risk free return of 1% annually on the amount of PDE issued.

As noted, PDEPAs do not require holding limits.This may be another attractive feature that makes customers prefer the PDE over the DE: The PDE, unlike the DE, can serve as an unrestricted store of value. Banks would also be free to allow positive PDE holdings for companies (for which a DE holding limit of zero has been suggested): As long as banks have or can acquire sufficient reserves, no limit on PDE holdings must be imposed – and DE holding limits may well turn out to be obsolete if PDEs strictly dominate DEs in terms of returns.

Moreover, banks do not need a settlement infrastructure for PDE transactions. Rather, when a customer initiates a PDE payment, his PDEs can be instantly converted into DEs credited to his DEPA from where they are instantly transferred via the DE payment infrastructure to the payee's DEPA and – if the payee has arranged so - instantly converted back to PDEs. In fact, payer and payee may not even notice that their DEPAs are used in the transaction and their DEPAs may always have zero balance except for a few milliseconds during a transaction.

Effectively, while the PDE is a store of value and a unit of account, it would not necessarily be a medium of exchange. This is not a limitation: PDEs could, in principle, also be used for this purpose, but given its instant convertibility into DEs, it is presumably much easier to use the DE for transactions. That way, the PDE will be universally accepted - basically free-riding on the DE's status of legal tender and its mandatory acceptance.

Also, banks will have only very little cost in establishing a stablecoin like the PDE. Customer gateways and software can basically be copy-pasted from what is necessary to set up the DE. No additional costs for KYC or settlement infrastructure will arise. Costs for customer support and inclusiveness essentially just shift from DE to PDE. There will just be some costs for obtaining regulatory permission, for the fiduciary and - more on a voluntary level - marketing costs.

Naturally, a stablecoin like the PDE may not be a viable option for banks if the ECB's monetary policy returns to a regime of reserve scarcity. In this case, reserves would be costly, and this would destroy the profitability of the PDE. But the ECB is expected to operate monetary policy

on excess reserves for years to come and PDE setup costs are likely low. Contractual conditions may give the banks the right to discontinue running the PDE any time, with all holdings being converted one for one to DE or cash. It appears that banks face no great risk in setting up such a stablecoin. It will be a free lunch as long as large stocks of excess reserves exist – profitable for banks and preferable for both customers and companies over the DE.

Interestingly, the PDE would completely turn around the playing field between banks and non-banks. As explained in the previous subsection, the DE created an unlevel playing field where non-banks were enjoying an advantage over banks. But introducing the PDE, banks could change this in their favor: Banks would be able to take advantage of the remuneration of reserves at the DFR, while non-banks could not[19].

Hence, if banks introduced a PDE, this may – alas via another competitive distortion – be helpful to achieve implicit goal IG3, reducing the market share of foreign-owned PSPs and support EU-based PSPs. The undesired flip side of this, however, consists in the fact that explicit goals G5 and G6 as well as implicit goal IG4, all of which relate to the ability of the ECB to conduct its monetary policy, may be compromised.

To see this, note that a primary motivation for introducing the DE was the ECB's concern that it may not be able to properly conduct monetary policy if cash is used less and less in an increasingly digitalized payments market. Apparently, the ECB is concerned that its influence on reserves - the other form of central bank money - may be insufficient to fulfill its mandate. This may be true since in a regime of excess reserves there is no nexus between the stock of reserves and the quantity of central bank money used in payments. For this reason, the ECB favors introducing the DE as a new form of central bank money specifically tailored to be used in transactions.

Now suppose that banks respond to the introduction of the DE by introducing a stablecoin PDE. As under a regime of excess reserves both banks and customers are better off using the PDE rather than the DE, DE balances on DEPAs may actually become negligible: Due to higher interest income on PDEPAs, almost all money is held there except for the very brief moments of time when a payer sends money via DEPAs to a payee.

Neither cash nor DE would then be a useful target of monetary policy. Money used for transactions would correspond to the segregated component of total reserves, but this segregation is a completely private matter and the ECB has no instrument by which it can induce banks to segregate more or less reserves. i. e. issue more or less PDEs. Likewise, the ECB has no influence on customer demand for PDEs.

Hence, the DE would not help maintain the ECB's possibly slipping control of monetary policy in an increasingly digitalized payments market. Such a development would make the DE next to useless for achieving goals G5, G6 and implicit goal IG4.

[19] Either way, there would be a distortion of competition. The only way to solve this would be to grant non-banks accounts at the central bank and access to the deposit facility. This is an ongoing debate outside the scope of this paper.

Takeaway 11:

A stablecoin backed by reserves may outperform the DE and reduce DE usage to almost zero. In this case, the DE will be a futile effort to enable the ECB to ensure price stability and stability of the financial and monetary system.

4.5.4 Technological dependencies and implications for competition

The draft regulation supports innovation and competition as core policy objectives (see G1 and IG1), yet it remains silent on the technological conditions under which the digital euro is to be implemented. In the absence of specific provisions regarding openness, patent restrictions, or public access to technical documentation, it is to be expected that significant parts of the DE's software and hardware stack will be proprietary and potentially protected by trade secrets. Such an outcome may hinder future improvements to core components and distort competition, particularly if only the original vendors are able to maintain or extend key functionalities.

From a technological perspective, proprietary implementations can impede interoperability and raise integration costs for third-party providers, especially when documentation is incomplete or restricted. Moreover, security researchers face considerable obstacles when assessing the robustness and privacy guarantees of closed systems. Vulnerabilities in proprietary systems often remain undiscovered for longer periods, and when disclosed, only the rights holder may be in a position to address them. This slows down the response to critical issues and can increase systemic risk. Even when contractual obligations to provide updates exist, exclusivity over the code base may prevent timely remediation by others.

Given the regulation's goals of fostering innovation (G1), ensuring high resilience (G4), and increasing competition (IG1), the reference to open standards in Art. 26 only with regards to interoperability with other, private digital means of payments, paired with the omission of any reference to open-source licensing appears problematic. Aligning the DE's implementation with the EU's Open Source Strategy (COM(2020) 7149 final) would strengthen technological sovereignty, reduce long-term dependencies, and level the playing field for providers.

Takeaway 12:

The draft regulation does not ensure alignment between the DE's technical implementation and the EU's open-source strategy. Without clear provisions, the use of proprietary technology may hamper interoperability, limit independent security scrutiny, and entrench vendor lock-in. Full disclosure of the technical stack would improve transparency, foster competition, and support Europe's strategic objective of digital sovereignty.

5. Conclusions

The European Commission's proposal for a digital euro (DE) introduces a retail-oriented central bank digital currency (CBDC) with legal tender status, aiming to address concerns over monetary policy effectiveness, financial stability, and the resilience of the payments system in an increasingly digitalized economy. However, our analysis highlights significant shortcomings in the proposed design, raising doubts about the necessity and effectiveness of the DE as

envisioned. The regulation largely follows design and implementation decisions taken by the ECB rather than proposing a legislative framework in line with and derived from a clear set of objectives for the DE.

The offline DE, intended to serve as a substitute for cash in proximity payments, lacks a clear competitive advantage over cash. Its reliance on hardware security measures exposes it to risks of fraud and duplication that cash does not face and which are ignored in this proposal. Additionally, it suffers from significant drawbacks in terms of convenience and inclusiveness, as its usage requires digital literacy, device compatibility, and authentication procedures that may be challenging for certain population groups, such as the elderly or individuals with limited digital skills. Given these limitations, it is unlikely that the offline DE will achieve the goal of widespread acceptance.

The online DE, by contrast, resembles commercial bank money in most respects, differing primarily in its lower issuer risk. Yet, this benefit alone may not suffice to generate significant demand, as customers enjoy deposit insurance up to 100,000 euros in commercial banking. Moreover, the legal structure of the DE imposes costs on banks, which are mandated to provide DE services at no charge while simultaneously bearing the funding costs. This leads to a regulatory asymmetry by distorting competition between banks and non-banks and could hinder innovation in the financial sector.

Additionally, the DE risks distorting market incentives by crowding out private payment solutions without necessarily improving the efficiency or security of digital transactions. By mandating that PSPs provide DE services at no charge while allowing the DE to operate on private payment infrastructure, the regulation effectively compels PSPs to support a direct competitor. This setup reduces the incentive for PSPs to invest in innovation, as any improvements they develop would be immediately available for DE usage without giving them a competitive advantage. As a result, the DE could stifle the development of new payment technologies rather than fostering a more dynamic and competitive financial ecosystem.

Finally, the proposal's broader economic and monetary implications remain uncertain. While the DE aims to support the role of central bank money in a digitalized economy, its introduction may have unintended consequences for the banking sector, particularly in times of financial stress. The ability to seamlessly convert commercial bank deposits into DEs could amplify liquidity risks, potentially destabilizing the financial system rather than reinforcing it. Furthermore, the legal and economic conditions favoring the emergence of a stablecoin backed by euro reserves could result in an alternative that outperforms the DE in all aspects, undermining its intended role and challenging the ECB’s control over digital payments.

Overall, the proposal in its current form raises fundamental questions about the trade-offs involved in introducing the DE. While the objectives of ensuring monetary stability, increasing competition, and reducing dependence on non-EU financial infrastructure are commendable, the proposed framework may ultimately be counterproductive. Without substantial revisions to its design, including a reassessment of its competitive positioning, privacy implications, and economic impact, the DE risks becoming a suboptimal solution that neither effectively replaces cash nor outperforms existing digital payment options.

References:

Bindseil, Ulrich (2020): *Tiered CBDC and the financial system*, Working Paper Series, No 2351, European Central Bank, Frankfurt am Main, January. Bindseil, Ulrich, Tiered CBDC and the Financial System (January, 2020). http://dx.doi.org/10.2139/ssrn.3513422

Bindseil, Ulrich, Fabio Panetta (2020): *Central bank digital currency remuneration in a world with low or negative nominal interest rates*, VoxEU, Centre for Economic Policy Research, London, October 5th. https://cepr.org/voxeu/columns/central-bank-digital-currency-remuneration-world-low-or-negative-nominal-interest

Bofinger, Peter, Thomas Haas (2020): *CBDC: A systemic perspective*. No. 101. WEP-Würzburg Economic Papers. https://www.wiwi.uni-wuerzburg.de/fileadmin/12000000/Downloadpool/WEP/wep101.pdf

Chaum, David, Amos Fiat, Moni Naor (1990): *Untraceable Electronic Cash.* Goldwasser, Shafi (eds) Advances in Cryptology — CRYPTO' 88. CRYPTO 1988. Lecture Notes in Computer Science, vol 403. Springer, New York, NY. https://doi.org/10.1007/0-387-34799-2_25

COM (2023a): *Proposal for a regulation of the European Parliament and the Council on the establishment of the digital euro*, European Commission, COM (2023) 369 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0369

COM (2023b): *Impact assessment report accompanying the proposal for a regulation of the European Parliament and the Council on the establishment of the digital euro*, European Commission, Staff Working Document SWD (2023) 233 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023SC0233

COM (2023c): *Annexes to the proposal for a regulation of the European Parliament and the Council on the establishment of the digital euro*, European Commission, COM (2023) 369 final. https://www.eumonitor.eu/9353000/1/j4nvirkkkr58fyw_j9tvgajcor7dxyk_j9vvik7m1c3gyxp/vm4cn8y949vo

ECB (2020): *Report on a Digital Euro.* https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

ECB (2021): *Digital euro experimentation scope and key learnings.* https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

ECB (2023a): *Opinion on Draft Regulation.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023AB0034

ECB (2023b): *A stocktake on the digital euro, October 18th, 2023.* https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/ecb.dedocs231018.en.pdf?6fbcce71a4be7bb3b8fabc51fb5c7e2d

ECB (2024a): *Progress on the preparation phase of a digital euro - First progress report.* https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202406.en.html

ECB (2024b): *State of play on offline DE*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240411_item3updateofflinedigitaleuro.en.pdf

Di Iorio, Alberto, Anneke Kosse, Ilaria Mattei (2024): *Embracing diversity, advancing together - results of the 2023 BIS survey on central bank digital currencies and crypto*, BIS Papers No. 147, Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap147.pdf

Dold, Florian (2019): *The GNU Taler System. Practical and Provably Secure Electronic Payments*, Thèse de Doctorat No. 195897, Université de Rennes 1. https://theses.hal.science/tel-02138082/file/DOLD_Florian.pdf

IMF (2023): *Central Bank Digital Currency – Initial Considerations*, International Monetary Fund, Washington D.C. https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/11/14/Central-Bank-Digital-Currency-Initial-Considerations-541466?cid=em-COM-123-47455

Meller, Barbara, Oscar Soons (2023): *Know your (holding) limits: CBDC, financial stability and central bank reliance*, ECB Occasional Paper No. 326. http://dx.doi.org/10.2139/ssrn.4543369

Gilbert, Seth, Nancy Lynch (2002): *Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services*. SIGACT News, 33(2):51{59, June 2002. https://doi.org/10.1145/564585.564601

Grothoff, Christian, Florian Dold (2021): *Why a Digital Euro should be Online-first and Bearer-based*. https://www.taler.net/papers/euro-bearer-online-2021.pdf

Lucke, Bernd, Dirk Meyer (2024): *Zentralbankverluste und leistungslose Zinseinkommen für Geschäftsbanken – ein Vorschlag zur Abschöpfung*, ZBB (Zeitung für Bankrecht und Bankwirtschaft), 2024, 252, August. https://doi.org/10.15375/zbb-2024-0405

Tu, Yu-Ju, Selwyn Piramuthu (2020): *On addressing RFID/NFC-based relay attacks: An overview*. Decision Support Systems 129: 113194. https://doi.org/10.1016/j.dss.2019.113194