The Proposed Design of the Digital Euro: A Critical Analysis

Mikolai Gütschow, Dresden University of Technology (TUD), Germany

Bernd Lucke[1], University of Hamburg (UHH), Germany

September 2025

revised November 2025

Abstract

We analyse the Commission's draft regulation for the establishment of the digital euro (DE). While well-intentioned, the design proposed by the Commission exhibits serious flaws. In particular, both the offline and the online versions of the DE show clear disadvantages compared with cash and online commercial bank money, respectively — for example, severe limitations on the store-of-value function of digital euros and strict holding limits unknown in current forms of money. There is essentially no discernible benefit to customers. Privacy remains comparable to current private payment systems, yet concerns persist about potential user re-identification at the central level. Competition, innovation, and trust are greatly undermined by the use of proprietary rather than open-source software. The enforcement of mandatory acceptance places competing means of payment at a disadvantage, even when technologically superior. The DE also distorts competition between banks and non-banks, as DE issuance and basic services are costly and unprofitable for banks. Banks may therefore resort to issuing a DE-based stablecoin that would be superior to the DE for both customers and banks, thereby undermining the ECB's control over monetary policy. We show how these flaws can be addressed and outline an improved design for a European CBDC based on open software and elements of blockchain technology.

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

[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. Mikolai Gütschkow can be reached at mikolai.guetschow@tu-dresden.de, ORCID 0009-0006-4489-7069. The authors thank Christian Grothoff and his team for very valuable comments.

JEL: E42, E58, E52

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.

Due to concerns about such developments, central banks consider offering private agents a digital form of central bank money either as a replacement for (physical) cash or as a complementary means of payment. 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.

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 launched a two-year investigation phase in July 2021 to address key design and distribution challenges. 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) 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. The ECB presented its opinion on the draft resolution in October 2023, cf. ECB (2023a).

The COM proposal is still under the scrutiny of the co-legislators. In this paper, we analyze the draft regulation. 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. After providing our view on a better approach to the DE in Section 5, 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 euro, however, is a competence of the ECB enshrined in Article 128 TFEU. This also applies to the

issuance of a digital euro, cf. Grünewald et al. (2021). Also, Article 127 TFEU 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 and 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.

The delineation of spheres is not always clear. Legal tender is issued with certain security features. But does this imply that security features of the DE are a matter of issuance and not also a matter relevant for use? Along the same line, are *design* features of the payment infrastructure and its interfaces (both user interfaces (UI) and application programming interfaces (API) of private payment services providers (PSPs)) an exclusive competence of the ESCB due to their role in "the smooth operation of payment systems"? It may be more appropriate to agree on a "shared competence" that justifies scrutiny of and legislation by the co-legislators.

Finally, it should be mentioned that the proposed regulation establishes the digital euro as a direct liability of the ECB or an NCB, but does not grant the owner of the DE a legal claim against the issuer and explicitly rules out any contractual relationship between owner and issuer (Recital 62). This is done in complete analogy to banknotes, the other form of central bank money available to the public, i. e. non-banks. But this symmetry ignores the fact that banknotes are physical items under full physical control of their owners, while a DE is not.

Rather, a DE – as its name suggests – merely exists in a digital form and owners depend on software or hardware components to access it, similar to commercial bank money. Trust in commercial bank money hinges on the fact that its owners have a legal claim against their PSP to have any deposits on checking accounts converted at par against banknotes or coins any time. The proposed regulation, however, does not grant owners of digital euros a similar legal claim against the ECB or NCBs. Nor does it grant a legal claim against central banks to the reverse

exchange: have banknotes converted at par into digital euros. In fact, such a conversion would be impossible if the holding limit has been reached.

The important delineation to note in this context is the limited reach of Article 12 (1): "The digital euro shall be convertible with euro banknotes and coins at par." While not explicitly mentioned, this Article does not apply to the ECB or any NCB, since it is part of Chapter III (Legal Tender). Legal tender is defined in Article 7 as the power to discharge from a payment obligation. Since DE owners have no contractual relationship with and no claim against their central bank, no payment obligation either way does exist.

2.2 Functional distinctions

Besides the legal distinction between competences, there is the important 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 or 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.

The title of the COM proposal mentions merely "the establishment of the digital euro". This is misleading since 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).

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 there is strong evidence that alternative design choices for the payment object and the payment infrastructure have not been studied.

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). Also, the IA does not consider designs with asymmetric anonymity as proposed by Chaum (1988) and Dold (2019). 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.

Why have alternative design choices not been studied in the IA? 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. 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 can be raised. 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 objectives that guide the establishment of a DE and its infrastructure. To these objectives, 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). Based on Recitals 1, 3, 5, 7, 68, 70-73 and Section 1 of the Explanatory Memorandum, Table 1 provides a list of explicit goals associated with the introduction of the DE and its infrastructure.

< Insert Table 1 here >

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 note that goals G1-G9 may be in conflict with each other. For instance, if third-party digital currencies offer faster or securer 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.

Indeed, G10 and G11 could also be interpreted as subordinate goals 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. In the case of privacy, this interpretation is also consistent with public concerns as "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 (IG) may be identified. These are goals not explicitly mentioned in the proposed regulation, but more or less clearly articulated in other official text. 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 and while strengthening competition in payment services is not addressed in the Recitals, the explanatory memorandum mentions "supporting a stronger and more competitive, efficient and innovative European retail payments market and digital finance sector". Hence, IG1 in Table 2.

The explanatory memorandum views the digital euro as supporting the "EU's open strategic autonomy". ECB (2020) 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". Hence, IG2 in Table 2.

The EU also seems to aim at reducing market shares of foreign-owned PSPs and supporting EU-based PSP's (IG3). This is not the same as IG2, since 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).

In ECB (2020, p. 9) the ECB voices concerns about "a significant decline in the role of cash as a means of payment" and a "significant potential for foreign CBDCs or private digital payments to become widely used in the euro area". Such developments would reduce the effectiveness of the ECB's monetary policy and its primary goal to ensure price stability (Article 127 TFEU). Against the background of these challenges to its mandate, the ECB states that the digital euro could serve "as a new monetary policy transmission channel". Since monetary policy is the means to achieve price stability, another goal – for unclear reasons held implicit - is preserving or even enhancing the ECB's ability to fulfill its mandate (IG4). Finally, it seems fairly clear that an implicit goal consists in extending the reach of the Euro beyond the borders of EU and Eurozone (IG5), since ECB (2020) lists "reasons to issue a digital euro: … (v) to foster the international role of the euro" (p. 9).

< Insert Table 2 here >

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 private profit opportunities.

Also, IG3 (reduce market share of foreign PSPs) would be compatible with IG1 only if foreign PSPs currently enjoy dominant market positions to an extent detrimental to free competition. But if this were the case, enforcement of EU and national antitrust and anti-collusion laws would seem a more natural response than establishing a CBDC.

Further, IG5 (extend the DE to third countries) may be in conflict with G1 (foster innovation) and G4 (resilience). Agreements with third countries on the use of the DE would require mutual consent on regulation – and if the third country takes a cautious approach, innovation could be hampered. Also, 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 and among 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.

3.3 Non-goals

Finally, there are some non-objectives, i. e. goals the Commission seems to dislike. We just give two examples. First, 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. In their view, software should be open-source rather than proprietary to ensure that no abuse of private data can occur and that there 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 non-objective NG1: Freedom of choice with respect to hardware and software.

Second, providing central bank money as a store of value for private non-banks is also a non-goal (NG2). This 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 since cash is free of issuer risk. If cash is gradually replaced by CBDCs, it could be desirable for the DE 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 DE's store-of-value role (cf. Article 16).

4. Analyzing the proposed design of the digital euro

4.1 Scope

As drafted in COM (2023a), the DE is to be a retail currency; cf. Recital (1). Article 16(1) empowers the ECB to impose holding limits. In light of G5 (preserve the functioning of the monetary system), ECB authors like Bindseil (2020) or Meller and Soon (2023) have argued that these limits must be low to prevent destabilization of commercial banks through deposit outflows. In this context, limits of €3,000 for individuals and zero for companies have been proposed, effectively restricting the DE to retail use.

With zero limits for companies, DE business-to-business (B2B) transactions would require conversion of commercial bank money into DEs, immediate transfer via the DE infrastructure, and prompt reconversion by the payee. Why should firms engage in this? It would be simpler to bypass the DE and transfer the commercial bank money directly. There is thus no compelling reason for DE B2B payments or transactions from businesses to consumers (B2C) — unless the DE infrastructure proves significantly safer or cheaper than current options. But cost advantages are unlikely, as the ECB must maintain the competitiveness of the TARGET/TIPS system if it intends to preserve it. And since private infrastructure is widely regarded as secure, B2B and B2C transactions are likely to continue relying on commercial bank money.

Zero holding limits for companies apply offline as well; cf. Article 16(4). Hence, companies can receive offline payments only via internet-connected devices that instantly convert DEs into commercial bank money. This contradicts the claim that the offline DE serves payments "in rural or remote areas without a (stable) communication network" (Recital 5), and the ECB's assertion (2024a) that "offline functionality would enable payments to be made without an internet connection … in locations with limited network coverage, and in the event of power cuts." Unlike cash, the DE appears ill-suited for such cases.

Also due to the holding limits, the DE falls short of a classical monetary function: storing value. This increases the likelihood that customers will prefer commercial bank money as a (likewise digital) means of payment, but without holding limits and with broader functionality.

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 alignment of their national legislation with all relevant EU rules on the DE, Eurozone residents will generally be unable to make or receive DE payments

when transacting with non-Eurozone residents. This stands in sharp contrast to euros in the form of commercial bank money or cash, which are widely accepted outside the Eurozone, especially in countries with many Eurozone tourists.

The Explanatory Memorandum refers to the DE serving "future use cases in industry 4.0 and web3," and Recital 55 mentions "payments between machines." However, both the prescribed account-based architecture with holding limits tied to legal entities and the fact that the DE is not programmable (Art. 24(2)) contradict this. The DE thus fails to support additional use cases that could give it an edge over cash or commercial bank money, or position it as a competitor to innovative programmable payment solutions.

Takeaway 1:

In terms of scope, the DE offers no advantage and faces four major limitations compared to cash or commercial bank money: it is confined to retail payments, lacks a meaningful store-of-value function, cannot serve as retail payment system in offline scenarios and is unusable outside the Eurozone unless a bilateral agreement is in place. These constraints make cash and commercial bank money more functional and widely accepted, casting doubt on whether the DE will achieve broad acceptance (G8 and IG5).

4.2 Risks

4.2.1 Insolvency risk and risks to financial stability

One reason the DE might be preferred to commercial bank money (though not to cash) is the absence of issuer insolvency risk. Under Article 4(2), the DE is a direct liability of the

Eurosystem, like banknotes. In a banking crisis or run on private institutions, DE holdings are immune to the insolvency risk of the private banking sector. In this respect, DE is equivalent to cash.

But how does the DE affect banks' insolvency risk? Besides banknotes, the DE introduces a second form of central bank money available to customers—another outlet for deposit conversions during a crisis. Any such conversion into DE or cash reduces bank reserves and increases insolvency risk. Article 13(3) grants users the right to convert cash and commercial bank money into DE at full face value —a process known as "funding" (the reverse being "defunding"). For the latter case this is explicitely stated to be possible "at any point in time, on a continuous basis." As a result, depositors can shift commercial bank funds into central bank money instantly—subject only to the DE holding limit.

By contrast, if banknotes were the only available form of central bank money, deposit conversions would require physical visits to ATMs or bank branches. In a crisis, this may involve queues, closed branches, or empty ATMs. Reserve outflows would be slower without an instant digital method for converting deposits. In this sense, Article 13(3)(a) undermines goal G6 (stability of the monetary system).

Moreover, Article 13(3) is not fully consistent with Articles 8 and 12(1). While Article 12(1) affirms that DE and cash are always equal in value and Article 8 grants both legal tender status, Article 13(3)(a) gives customers a legal right to receive DE—rather than cash—up to the holding limit. Banks cannot meet this obligation by offering cash as a substitute. If they could, they might slow reserve loss during a crisis by avoiding instant, digital disbursements.

Lawmakers might consider amending Article 13(3) to allow banks—under exceptional circumstances and with ECB approval—to require that DE funding occur via cash. This would relieve them of the obligation under 13(3)(a) to provide DE funding continuously, letting them invoke

13(3)(b) instead. While customer claims on banks would remain unchanged, such a measure could significantly slow reserve depletion in acute crises.

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.

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 devices such as smartphones, tablets, or smartwatches (Article 2(31)). We first examine risks associated with offline use.

Offline payments are settled instantly by updating DE holdings on local devices (Article 30(1) and (3)) without connection to the payment infrastructure. The security of offline DE thus depends on the tamper resistance of hardware. Article 35(1)(c) tasks the Eurosystem with "safeguarding the security and integrity of ... local storage devices." Whether it can meet this obligation is uncertain. Grothoff and Dold (2021) note that "hardware protections typically fail against well-equipped adversaries" and cite successful attacks on all major architectures, including Intel, Samsung, ARM, AMD, and SIM cards.

Once compromised, devices could enable multi-spending[2]. Unlike counterfeit cash, which typically exhibits detectable flaws, unauthorized copies of DEs are exact and indistinguishable. Moreover, such copies could be used without limit, rendering potential financial damage unbounded. Note that any multi-spending event would remain undetected until the recipient reconnects to the internet to deposit the DE. (It is unclear how this aligns with the concept of instant settlement in Article 30(1).)

The risk of multi-spending and undue money creation due to attacks on hardware security is underscored by a formal result from Gilbert and Lynch (2002), who proved the impossibility of designing a distributed system that simultaneously ensures consistency, availability, and partition tolerance (CAP). Applied to DE, consistency prevents multi-spending, availability ensures continuous payment functionality, and partition tolerance allows operation during offline periods. The CAP theorem thus implies that offline DE, by enabling partition tolerance, must compromise either consistency or availability—or both.

In simple terms: offline DE cannot be both fully protected against multi-spending and reliably available at all times. Whether the Commission is unaware of the CAP theorem or chose to disregard it is unclear. In any case, the inherent conflict between CAP properties makes cash a more reliable bearer-based instrument, undermining goal G8. It is also hard to see how goal G4 (resilience of payment systems) can be achieved with a currency that is either sometimes unavailable or vulnerable to fraud.

We suggest that consistency and availability should take precedence over partition tolerance. This would mean either abandoning offline DE altogether—simplifying the system to a single

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

online variant—or limiting it to an emergency fallback when online payments are unavailable or insecure.

In principle, measures might be devised that allow retroactive identification of fraudulent users. But this seems incompatible with the cash-like privacy of the offline DE established by Article 34(1): No personal data of payer or payee is recorded—except during funding or defunding.

Moreover, 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). Nor is it certain whether funding and defunding data alone, however detailed, would suffice to detect DE forgery[3]. ECB (2024b) vaguely refers to a "minimum amount of data compatible with the need to detect forgery," leaving open whether, despite Article 34(1), storing transaction data and disclosing it in suspicious cases will be necessary.

In any case, the owner of a compromised device may indefinitely avoid reconnection. If he exploits someone else's device and transfers the DEs from there, anonymity may render the fraud untraceable. The design of *offline* DE thus severely impedes fraud detection, undermining G10. Notably, Article 32 explicitly limits fraud detection to *online* DE.

There is a substantial risk that offline DE anonymity may facilitate other types of criminal activity. Relay attacks (cf. Tu and Piramuthu 2020) could simulate proximity payments over the Internet, enabling transfers between devices that are not physically close. This would allow criminals to coerce victims into transferring offline DE to a perpetrator's device. If anonymity holds, the perpetrator would be untraceable and would face lower detection risk than with cash or commercial bank money.

[3] 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.

Digital crime can be automated and scaled, targeting many victims at once. Low holding limits per device do not prevent substantial criminal gains: small individual amounts can add up. Moreover, if blackmail involves sensitive information and minor financial loss, a significant share of such crime may remain undetected.

Tampering with offline DE devices—by foreign attackers or organized crime—could cause far greater harm than banknote forgery. Lower privacy standards may thus be justified. Cash will likely be perceived as less vulnerable to fraud and more reliable in terms of privacy, reinforcing concerns that achieving goal G8 (wide acceptance) for offline DE may be difficult.

Also, note that any holding or transaction limit places offline DE at a disadvantage relative to cash. Even if similar limits were imposed on cash, they would be hard to enforce and easy to bypass. Cash enables private holdings and payments at amounts that offline DE cannot match due to regulatory limits. Yet both are free of issuer risk. Thus, privacy concerns may seriously hinder goal G8 (wide acceptance), as individuals may prefer cash to offline DE.

Last but not least, the draft regulation is silent on liability: Would responsibility for fraud lie with the user, the device manufacturer, or the Eurosystem—and under what conditions? To foster DE adoption, lawmakers should consider explicit liability rules that exempt users except in cases of intent or gross negligence. While such protection may already follow from general legal principles and the privacy guarantees of Article 34(1), codification would reduce uncertainty and reassure users. The same may hold true for device manufacturers.

Takeaway 3:

Offline DE offers cash-like privacy within stricter holding limits than cash. Since hardware is inherently vulnerable, offline DE entails higher liability risks for users and possibly for the Eurosystem – with no reduction in issuer risk. It also cannot be both reliably available and

immune to fraud, undermining G4 and G10. Therefore, users may prefer cash. Criminals, however, might value digital anonymity for scalable extortion and blackmail.

4.2.3 Security risks and risks to privacy – online version

The online DE depends almost entirely on PSPs for distribution. Under Article 13, PSPs must offer customers the ability to open DE payment accounts (DEPAs) and manage DE payments through their services. Customers may enable automatic transfers of excess DE holdings to a non-DE payment account (NDEPA) ("waterfall") and automatic coverage of excess DE payments from this NDEPA ("reverse waterfall"). As Article 13(6) excludes any contractual relationship between users and the Eurosystem, PSPs remain users' sole point of contact.

The security of online DE payments matches that of commercial bank money, as both rely on the PSP's existing systems. PSPs will integrate DE management into their platforms and protect its integrity using the same mechanisms applied to commercial bank transactions. They will also connect to the Eurosystem's DE infrastructure as they do when managing reserves. Thus, security neither incentivizes nor discourages the use of online DE.

The situation is different with respect to privacy. For online DE transactions, PSPs must collect and store the same non-anonymized data as for commercial bank money, with storage decentralized across PSPs. Unlike commercial bank money, however, the ECB's digital euro infrastructure will also record all individual transactions centrally (cf. Article 30(2)). These records must not contain personal data that "directly identify individual digital euro users" (cf. Articles 34(4) and 35(4)). But Article 30(1) and (2) require that online DE transactions be settled instantaneously "at the moment of recording the transfer of the digital euros concerned

from the payer to the payee." This implies that the ECB will see all transactions and the corresponding DEPA identifiers.

Such access raises privacy concerns. While Article 34(4) requires PSPs to separate names and other personal data from DEPA identifiers, preventing direct identification, it remains unclear whether indirect identification based on DEPA identifiers is possible. Scientific evidence suggests that pseudonymized payment data can allow individual re-identification (cf. Lubarsky, 2017). Kikuchi (2021) shows that the likelihood increases with the number of records linked to a pseudonym. Such indirect identification would be legally permissible, as the draft regulation prohibits only direct identification[4].

While the ECB likely has no intention of re-identifying users, some—perhaps many—users may remain skeptical. As ECB (2024) notes: "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 legally and technically feasible may fuel fears of secret surveillance, undermine trust in the DE and harm the wide acceptance goal (G8)[5].

Such concerns could be addressed by excluding any form of identification, including indirect re-identification, and by ensuring that the Eurosystem cannot link transactions to fixed pseudonyms. For example, the Eurosystem could be informed that a transfer is taking place between two PSPs, identified only by a random transaction ID. The associated DEPA numbers would be exchanged exclusively between the PSPs, bypassing the Eurosystem. The receiving

[4] 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 [… They] would process personal 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."

[5] 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.

PSP would learn only the amount and the account to be credited, remaining unaware of the payer's account.

As a result, the ECB would not know which accounts are involved, but would merely register a transfer between PSPs (cf. Chaum et al. (2021)). This setup would closely mirror current commercial bank money transfers, where the Eurosystem moves reserves between banks without information on the underlying customer accounts. It would even offer stronger privacy than today, as the payer's identity would no longer be disclosed 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 liability in cases of theft, security breaches, or malfunctions—whether in online or offline DE use. Unlike commercial bank money, the DE is a direct liability of the ECB (Article 4(2)), not of the PSP providing access. Hence, the liability rules of PSD2, which govern PSP responsibilities in cases of fraud or unauthorised payments, cannot be directly applied.

This raises fundamental questions: If a criminal hacks a DE-enabled device or account, replicates digital euros, and spends them multiple times before detection, who bears the loss? The user—despite no negligence? The PSP—despite neither issuing nor holding the DE? The device manufacturer? Or the Eurosystem—as the issuing authority?

Article 35(1)(c) assigns the Eurosystem responsibility for safeguarding offline devices but is silent on liability if protection fails. Article 13(6) excludes any contractual relationship between users and the ECB or national central banks, leaving unclear how compensation claims could be pursued.

European law defines PSP liability in detail under PSD2 (Articles 73–92) but offers virtually no guidance on the ECB's liability toward private actors. Under Article 340(3) TFEU, the ECB is liable only "in accordance with the general principles common to the laws of the Member States" and only for damage "caused by its servants in the performance of their duties." This creates doubt about ECB liability for systemic flaws, institutional negligence, or failure to address known vulnerabilities. Without explicit liability rules, legal uncertainty may erode the very trust in central bank money that the DE aims to strengthen.

Takeaway 5:

The introduction of the DE raises unresolved questions about liability in cases of theft, malfunction, or security breaches. Since the DE is a direct liability of the ECB—not the PSP—existing PSD2 rules may not apply, be justified, or proportionate. The draft regulation does not clarify whether users, PSPs, or the Eurosystem would be liable for resulting financial losses. Such legal ambiguity could seriously 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."[6] 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.

It is unclear why Article 17(2) explicitly allows merchant service charges—defined as "a fee paid by the payee to a payment service provider when acquiring a digital euro payment transaction"—while PSPs are prohibited from charging natural persons for DE usage. Clearly, merchants could avoid charges by having natural persons handle the company's DE transactions free of charge. Waterfall and reverse waterfall mechanisms could then convert digital euros into or from commercial bank money at no cost, with final settlement between the individual and the company taking place entirely in commercial bank money.

Merchants and PSPs would ultimately pass on uncovered DE costs via higher prices, making customers bear them indirectly. As most users may remain unaware of this, the perception of DE as cost-free could support—or at least not hinder—goal G8 (wide acceptance).

Mandatory acceptance (Articles 7(2), 9(a)) requires enterprises of a certain size, and all firms accepting "comparable digital means of payment", to install and operate the technology needed for DE payments and to cover related costs. PSPs may charge merchants for DE services, up to specified limits (cf. Article 17(2), (6)). Unlike voluntary systems like credit cards, DE must be accepted. Undesirably, cost pressures may compel firms to abandon alternative voluntary systems, even if these offer superior functionality or better match customer preferences.

[6] Article 17(1) prohibits PSPs from charging fees to natural persons. No similar provision exists for merchants. Only implicitly might Article 7(2), which defines the DE as legal tender at full face value, preclude surcharges on DE payments. However, this would apply equally to natural and legal persons, whereas Recital 40, for unclear reasons, limits the fee prohibition to natural persons alone.

Mandatory acceptance supports G2 (reduce fragmentation) and G8 (wide acceptance), but may undermine G3 (payment system efficiency) and G1 (promote innovation). Among implicit goals, it furthers IG2 (EU control over payment infrastructure) and IG3 (reducing foreign PSPs' market share), yet likely conflicts with IG1 (increasing competition).

Like merchants, PSPs face potentially significant costs when providing DE services. Article 14(1) obliges retail credit institutions to offer all basic DE functions, requiring software integration, maintenance, customer support, and compliance with AML/CFT rules under Directive (EU) 2015/849 (KYC). PSPs also serve as users' sole point of contact, while the ECB and NCBs—though ultimately liable for the DE—remain uninvolved. Yet under Article 13(1), PSPs may not charge natural persons for basic services.

The regulation leaves unresolved how PSPs can recover costs for managing a liability that is not theirs. Without Eurosystem compensation, they may be forced to cross-subsidize DE services by raising other fees or lowering deposit rates. Since basic DE payment services are free, most DE users will perceive the DE as costless, and even those who do not use it will indirectly finance it through higher fees or lower rates.

Cross-subsidization could trigger a substitution effect: customers may favor the cost-free DEPA over NDEPAs or other deposit accounts if the latter become less attractive. While this promotes G8 (wide acceptance), it undermines the appeal of traditional banking. Holding limits under Article 16(1) may thus be needed to avert risks to G6 (monetary stability).

Turning to Eurosystem costs, Recital 41 states that it will not charge PSPs "for the costs it bears to support their provision of digital euro services." PSPs, however, may view this as entirely inverted: DEs are neither assets nor liabilities on their balance sheets, and basic DE services are commercially unprofitable. From their perspective, they provide these services solely to fulfil a legal duty—serving the Eurosystem's interests, not their own. In fact, the Eurosystem

outsources core CBDC functions to private institutions—responsibilities that, in the eyes of PSPs, should lie with the central bank itself.

Even if the Eurosystem covers its own costs—e.g. for DE development, infrastructure, and clearance—this would reduce NCB profits and, by extension, national budget contributions. Therefore, the DE would be no free lunch for taxpayers: it adds to payment system costs, ultimately borne by private agents—either via higher prices or reduced public resources.

Alternatively, the Eurosystem may offset costs by drawing on PSPs. Recital 9 suggests issuing DE by converting their central bank reserves. Since most reserves are held in the ECB's deposit facility and earn the deposit facility rate (DFR), this would lower the ECB's interest expenses—cutting into banks' risk-free income.

For example, if the DFR is 2% and €1 trillion in DEs are issued (as in Bindseil and Panetta 2020), this would yield €20 billion annually—far exceeding DE-related costs. However, under traditional reserve scarcity, the ECB could not offset these costs merely by lowering reserve remuneration.

Takeaway 6:

Wide acceptance (G8) is legally enforced by prohibiting PSP fees for basic DE services and requiring most merchants to accept DE. Yet who bears direct costs matters little, as all expenses ultimately fall on private agents.

Takeaway 7:

Although users may believe the DE is cost-free, this is a misperception. Unless other payment systems are drastically scaled back or removed, the DE adds another layer of costs for private agents.

4.4 Convenience and inclusiveness

Convenience is crucial for the wide acceptance of the DE (G8). The online DE will likely match commercial bank money in ease of use—assuming users have sufficient digital skills and their DEPAs are linked to NDEPAs via waterfall mechanisms. However, for users who dislike waterfall options, DE holding limits make payments less convenient than those via commercial bank money, cards, or private systems like PayPal.

People with limited digital skills or economic knowledge may struggle to distinguish between offline DE, online DE, and commercial bank money, or to grasp complex holding limit rules across accounts and devices and involving waterfall mechanisms. Increasingly demanding and still-unknown security and authentication requirements, along with occasional disruptions on private devices when software is updated, further complicate matters. Finally, the growing number of payment options (e. g. cash, credit card, giro card, online/offline DE, PayPal, Wero, Apple Pay, Google Pay) may leave consumers perceiving the market as fragmented, contrary to goal G2.

For anybody, offline DE payments are likely far less convenient than cash. A proximity connection must be established between devices, which may fail due to technical faults or user error. High-security authentication, such as 2FA, will likely be required, and holding limits on either device may prevent transactions. These hurdles are especially problematic for the elderly and people with disabilities, undermining financial inclusion (G7). In contrast, cash is unaffected by such issues and remains more accessible and reliable in everyday use.

To promote inclusiveness, Article 14(3) and (4) requires that most PSPs and some government-appointed entities provide face-to-face digital support for people with disabilities or limited

digital skills. The designated entities must also offer basic DE services to individuals without an NDEPA. These provisions raise several issues that merit further attention:

First, Article 14 should explicitly state that inclusion support and basic DE services must be free of charge, since requiring payment for the former would be unjust and the entities designated by Member States should be bound by the same rule as PSPs.

Second, it remains unclear whether vulnerable third-country nationals such as asylum seekers or migrants without a residence permit are entitled to the (free) services outlined in Article 14(3) and (4). Many of these may just have limited proficiency in the domestic language, but neither a lack of digital skills nor a physical or mental disability.

Third, if digital inclusion and basic DE services are offered free of charge, the financial burden shifts to designated public entities and PSPs. Given the number of beneficiaries and the time required per client, this burden may be significant. Providers may then seek to cut costs, resulting in poor service quality, long waiting times, or access barriers—undermining the goal of inclusiveness (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 goal IG1 (increasing competition in payment services) aligns with the explicit goal G9 (preserving the euro's role in retail payments) only if the DE holds a competitive edge over private technologies or foreign digital currencies. However, it remains unclear where such an edge would come from.

A framework aimed at promoting competition and innovation (IG1 and G1) should largely remain neutral with respect to the technology or infrastructure used—by the DE or its competitors—as long as payment services are efficient and resilient (G3 and G4). Yet, two major breaches of this neutrality principle stand out.

First, the draft regulation requires the DE to be distributed by PSPs (Article 13). It will be cost-efficient for them to process DEs via their existing infrastructure. But this keeps the DE on equal footing with private euro payment solutions and prevents it from gaining a competitive edge over them at the infrastructure level[7].

Second, Article 24(2) prohibits the DE from being programmable money. While Article 24(1) allows the ECB to enable conditional payments, more extensive programmability would conflict with the DE's role as legal tender. To ensure full fungibility, features like time limits or use restrictions to specific goods or services are ruled out.

This design choice, though justified, imposes a significant technological limitation. As Recital (7) notes, demand for programmable money may emerge beyond conditional payments. Even

[7] 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.

governments might seek broader functionality—for instance, to ensure that social transfers are spent on eligible goods or at trusted merchants who then would be allowed to convert such funds into fully fungible euros.

The prohibition in Article 24(2) places the DE at a technological disadvantage compared to competing currencies with broader programmability. While the restriction could in principle be lifted if greater flexibility proves necessary, competing payment solutions may by then have advanced so far that it will be difficult for the DE to catch up.

Hence, the legal framework prevents the DE from offering superior infrastructure and limits its technological potential by restricting programmability to conditional payments. This places the DE at an inherent competitive disadvantage in pursuing goal G9 (preserving the euro's role in retail payments). However, this is—perhaps more than fully—offset by the regulation's grant of legal tender status (Article 8) and the mandatory acceptance requirement (Article 7(2)).

The latter grant the DE an advantage over other payment solutions that would likely be favored in a genuinely open market. The draft regulation implicitly concedes that the DE may not achieve goal G9 without regulatory privileging—being the only digital means of payment with legal tender status and mandatory acceptance. Its success would thus reflect not inherent superiority but the effect of legal design.

This raises the question of whether the DE will actually achieve IG1 (increasing competition in payment services). While the DE is, trivially, a new market participant, the key issue is whether it will stimulate greater competition among non-state digital payment solutions and thereby promote efficiency (G3) and innovation (G1).

It is unclear why this should be the case. A public payment solution—free for users, legally privileged, and entitled to unlimited use of competitors' infrastructure at no cost—enters a

market long served by private PSPs. Their market share and profits are likely to decline, reducing incentives for investment and innovation.

Greatly harmful to innovation is the almost parasitic way in which the DE would utilize private infrastructure. PSPs must expect that all their infrastructure investment will, by law, also benefit the DE—depriving them of competitive advantage through technology or service quality. Yet competition via pricing is equally unviable, as DE usage is free (for basic services) and central banks are under no obligation to operate the DE profitably.

Takeaway 9:

Infrastructure constraints and limited programmability place the DE at a structural disadvantage compared to private solutions, raising doubts about its ability to preserve the euro's role in retail payments. Despite this potential inferiority, its usage is promoted by legal tender status and mandatory acceptance. This may deter innovation and investment by private PSPs and ultimately weaken competition.

4.5.2 Competition between banks and non-banks

The draft regulation differentiates between banks and non-banks[8]: Banks are required to provide DEPAs and basic DE services upon client request (Article 14(1)), while non-banks may, but are not obliged to do so (Article 13(1); see also Recital 28).

As previously noted, basic DE services are inherently unprofitable for PSPs, as no fees may be charged. Moreover, when customers fund DE by converting deposits, banks lose both the

[8] By "banks" we mean "account servicing payment service providers" (ASPSPs) as defined in Article 1 of Directive (EU) 2015/2366 (aka Second Payment Services Directive (PSD2)). A "non-bank" is any other PSP.

reserves and their remuneration. Funding DE therefore results in bank losses equal to the interest income that would have been earned on the foregone reserves.

If DE in circulation is €1 trillion and the DFR is 2%, total annual funding costs for PSPs would be €20 billion. Yet under Article 13(1), non-banks may opt out of offering DE services, leaving banks to bear the full cost while being unable to earn revenue from basic DE services. This creates an uneven playing field and gives non-banks a regulatory advantage. Since many are foreign-owned (e.g. PayPal, Stripe, Worldpay, Visa or Master Card), this setup runs counter to implicit goal IG3, which seeks to reduce foreign market share and support EU-based PSPs.

Note, however, that competition between banks and non-banks is already severely distorted, as banks receive substantial risk-free interest on their large excess reserves. Lucke and Meyer (2024) argue that this is undeserved income as excess reserves are risk-free and unconnected to any productive activity. The unequal DE funding burden partly offsets this undeserved competitive advantage of banks. In this sense, one distortion is mitigated by another.

If non-banks choose to provide DE services, their DEPAs must be linked to NDEPAs at banks. As a result, banks still bear the funding cost through lost interest income on reserves. To address this, Article 17(2) allows banks to charge non-banks a proportionate inter-PSP fee, which may include a "reasonable margin of profit" but must not exceed fees for comparable digital payment methods. Under Article 17(3) and (4), the ECB must regularly monitor relevant developments.

Inter-PSP fees are a suitable way to ensure that non-banks contribute to DE funding costs. However, there is no need to define proportionality criteria by law or to assign the ECB a supervisory role. Non-banks can opt out of DE provision, leaving the full burden of funding costs to the banks. This gives non-banks strong bargaining power, and banks have clear

incentives to offer competitive terms. In this context, concerns about market power abuse by banks appear unwarranted.

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 rightly notes that the euro may eventually compete with third-country CBDCs, crypto-assets, or stablecoins. This paper focuses on one potential competitor from that broad field: a stablecoin issued by Eurozone banks and fully backed by reserves.

Suppose banks label it the private digital euro (PDE). Each bank would issue PDEs by segregating an equivalent amount of euro reserves from its general holdings. Segregation entails placing these reserves under the control of an independent fiduciary tasked with ensuring that their value always matches outstanding PDEs. PDE holders would enjoy contractual priority claims on segregated reserves in the event of bankruptcy and have instant convertibility into cash or DE—even during insolvency. Thus, PDEs would match the DE in terms of issuer risk.

If clients request to convert cash or deposits into PDEs, banks can issue the corresponding amounts and credit them to a PDE payment account (PDEPA), set up like a DEPA. Waterfall and reverse waterfall functions are not required due to the absence of holding limits but can be implemented if desired.

As long as the ECB operates in an excess reserve regime, banks continue to earn DFR interest on segregated reserves. In terms of interest income, the PDE is thus Pareto-superior to the DE for both banks and clients. If the DFR is 2%, banks could offer 1% on PDEPA holdings, making PDEs more attractive than DEPAs, which earn 0% under Article 16(8). Banks would retain 1% risk-free interest income on reserves that they would lose if the customer opted for the DE.

As noted, PDEPAs do not require holding limits. This makes the PDE more attractive than the DE, as it can be used without restriction as a 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 proposed. As long as banks hold or can acquire sufficient reserves, no limit on PDEs is needed—and DE holding limits may prove obsolete since PDEs consistently offer better returns.

Moreover, banks do not require a separate settlement infrastructure for PDE transactions. When a customer initiates a PDE payment, the PDEs can be instantly converted into DEs, credited to his DEPA, transferred via the DE infrastructure to the payee's DEPA, and—if arranged by the payee—converted back into PDEs. Payer and payee may not even notice the use of their DEPAs, which may hold a non-zero balance only for a few milliseconds during the transaction.

Banks would incur minimal costs in establishing a stablecoin like the PDE. Customer interfaces and software can largely be replicated from the DE setup. There are no additional costs for settlement infrastructure, and expenses for KYC, customer support and inclusiveness merely shift from DE to PDE. Costs for regulatory approval and fiduciary services should be small.

Naturally, a stablecoin like the PDE may become unviable if the ECB returns to a regime of reserve scarcity. However, the ECB is expected to maintain excess reserves for the foreseeable future, and PDE setup costs are likely low. Contractual terms could allow banks to discontinue the PDE at any time, with all holdings converted one-to-one into DE or cash. Banks therefore

face little risk in launching such a stablecoin. As long as large excess reserves exist, it is a free lunch—profitable for banks and preferable to the DE for their customers.

One aim of the DE is to preserve the ECB's monetary policy influence as cash use declines. Paradoxically, it may prompt the emergence of private alternatives like the PDE, whose holdings—though potentially central to payments and thus price stability—the ECB might find difficult to control. If the DE does not help maintain the ECB's possibly slipping control of monetary policy, it would be next to useless for achieving goals G5, G6 and implicit goal IG4.

Takeaway 11:

A stablecoin backed by reserves may outperform the DE and reduce DE usage to almost zero. In that case, the DE would fail to enhance the ECB's control over transaction-relevant money and be a futile effort to safeguard price stability.

4.5.4 Technological dependencies and implications for competition

The draft regulation promotes innovation and competition (G1, IG1) but is silent on rules regarding openness, patents, or public access to technical documentation. Without such rules, large parts of the DE's software and hardware are likely to be proprietary and protected as trade secrets. This may impede future improvements and distort competition if only the original vendors can maintain or extend core functionalities.

Proprietary implementations can hinder interoperability and raise integration costs for third-party providers, especially when documentation is incomplete or restricted. Security researchers also face obstacles when evaluating the robustness and privacy of closed systems. Vulnerabilities may go undetected longer, and once disclosed, only the rights holder may be

able to fix them—delaying critical responses and increasing systemic risk. Even with contractual update obligations, exclusive control over the code base can prevent timely remediation by others.

Given the regulation's goals of fostering innovation (G1), ensuring resilience (G4), and increasing competition (IG1), the narrow reference to open standards in Article 26—limited to interoperability with private digital means of payment—appears problematic, especially in the absence of any mention of open-source licensing. Aligning the DE's implementation with the EU's Open Source Strategy (COM(2020) 7149 final) would enhance technological sovereignty, reduce long-term dependencies, and create a more level-playing field for providers.

Takeaway 12:

The draft regulation fails to align the DE's technical implementation with the EU's open-source strategy. In the absence of clear provisions, proprietary technology may hinder interoperability, restrict independent security review, and reinforce vendor lock-in. Full disclosure of the technical stack would enhance transparency, promote competition, and support Europe's goal of digital sovereignty.

5. How to build a useful Digital Euro

Significant revisions to the current draft of the Digital Euro are urgently necessary to meet both the explicit and implicit goals outlined in the Draft Regulation – and, in our view, also the COM's non-goals. As a public good financed by taxpayers, the digital euro does not aim to generate profits like privately operated payment systems; therefore, it does not require proprietary technology for protection. Instead, it can and should rely on open standards, open protocols, and free, open-source software. This approach would facilitate innovation (G1) and

increased competition (IG2) in digital payments, along with reducing fragmentation in the retail payments market (G2), as open standards ensure interoperability among various implementations and operators.

With enhanced competition and innovation comes greater efficiency (G3) and resilience (G4), since multiple implementations based on the same open standard ensure that if one implementation or operator encounters issues, others can continue to operate. This is a stark contrast to proprietary technology, where a single solution serves all users, creating a single point of potential failure. Establishing the digital euro on existing open-source technology would also support interoperability with systems outside the Eurozone that utilize similar technology. Furthermore, this would lead to cost savings, as research and development expenses could be shared with other countries or private agents.

Obviously, open-source implementations do not allow for proprietary technology such as "secure hardware", which is the fundamental building block of the offline digital euro in the current draft regulation. This is no show-stopper, though: As laid out in Section 4.2.2, it is anyhow mathematically impossible to prevent double-spending for offline payments, i.e., when both the payer and the payee are disconnected from the rest of the system. "Secure hardware" can only circumvent this reality as long as it has not yet been successfully attacked. The draft regulation should refrain from promising such a feature. Instead, it may account for trust-based offline payments similar to cheques, where the payee trusts the payer that they can successfully redeem the value when coming back online, as currently offered by some blockchain implementations. This honest approach to offline payments underscores the necessity of defining legislative rules for fraudulent behavior in offline scenarios, which is currently lacking in the proposed regulation.

Widespread adoption (G8) of the digital euro is primarily intended to stem from its status as

legal tender, requiring mandatory acceptance throughout the Eurozone. While regulatory pressure might have an effect, it may easily entrench a suboptimal payment technology that would not be viable in a competitive environment. Instead, the digital euro should attract users through its usefulness, convenience, and significant advantages over competing payment systems. These advantages could include advanced features such as programmability, allowing it to compete with stablecoins. Additionally, emphasizing a high level of privacy and data protection (G11) could effectively match the anonymity of cash in the realm of online payments.

A potential technological foundation could be found in distributed ledger technology (DLT), such as open-source blockchains. The digital euro could take inspiration from successful stablecoins, which demonstrate that this technology effectively addresses real-world problems, such as reducing time and cost for cross-border payments and powering programmable transactions.

However, there are also disadvantages of DLT: The high degree of replication incurs considerable overhead in terms of settlement delays and energy consumption, leaving its suitability for high transaction numbers questionable. For instance, the Ethereum blockchain, which underpins the two biggest stablecoins in terms of market capitalization, USDC and Tether, handles no more than 15-20 transactions per second on its decentralized base layer, whereas centralized card payment networks reportedly support several 10,000 transactions per second (VISA (2018)).

While advocates of DLT rightfully emphasize the absence of a requirement for trust in a central payment operator, this might be less of a concern for a system provided by a central bank. On top, there are misconceptions regarding the anonymity of blockchain-based payments. In fact, all transactions are publicly recorded on the blockchain. Once an account identifier is linked to

a person’s identity, tracing transactions back to individuals becomes straightforward for anyone, not just the payment system operator.

To improve on DLT, we suggest merging an efficient centralized architecture for settlement with decentralized storage of sensitive data. In such a design, despite having a single issuer, it need not be a single point of failure, as one might use traditional database-sharding and replication techniques to distribute the risk of failures. In addition, the usage of a permissioned blockchain for public verification of the central issuer's ledger is a possible way to increase trust in the system.

For instance, the open Taler payment protocol and its free-software reference implementation GNU Taler initiated by Dold (2019) realizes such a system: Here, a central provider issues signed tokens that users hold in self-custody, i.e., in a decentralized way much like cash. The signing process occurs blindly, preventing the provider from linking a redeemed token back to the payer's identity. Since the provider and the commercial banks are unaware of individual user balances, neither can be held responsible for lost tokens. As a consequence, users are incentivized to limit the amount they hold in order to reduce potential financial loss, rendering strict holding limits unnecessary. In this scheme, payers remain anonymous, while payees are identifiable as they have to verify the tokens' validity with the central provider to prevent double-spending. According to Tinn (2025), such “asymmetric privacy” is desirable both from a welfare and efficiency standpoint, as it combines the possibility for oversight and detection of illegal activities (G10) with the protection of consumer privacy (G11).

6. Conclusions

The Commission proposes a retail-oriented DE with legal tender status, intended to address concerns over monetary policy, financial stability, and payment system resilience in a digitalized economy. However, its design raises serious doubts about the DE's necessity and effectiveness.

The offline DE, intended to substitute cash in proximity payments, lacks a competitive advantage over cash. Its dependence on hardware security exposes it to risks of fraud and multi-spending absent in cash and not addressed 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. Given these shortcomings, widespread acceptance appears unlikely.

The online DE closely resembles commercial bank money, differing mainly in its lower issuer risk. But this alone may not create substantial demand, given that deposits are insured up to 100,000 euros. Banks must offer basic DE services free of charge and bear the associated costs as well as the funding costs. This distorts competition with non-banks and is likely to impede financial innovation.

Additionally, the DE may distort market incentives by crowding out private payment solutions without demonstrable gains in efficiency or security. PSPs are required to provide DE services free of charge while the DE runs on their infrastructure, forcing them to support a direct competitor. This discourages innovation, as any technological advances would benefit the DE without yielding a competitive edge. Rather than promoting a dynamic financial ecosystem, the DE could suppress the development of new payment technologies.

Finally, the broader economic and monetary implications of the DE remain uncertain. While intended to strengthen central bank money in a digitalized economy, the DE may have adverse effects—especially in times of stress. Easy conversion of bank deposits into DEs could amplify liquidity risks. Moreover, legal and economic conditions may favor the rise of a reserve-backed stablecoin that outperforms the DE, thereby undermining its intended role and the ECB's ability to ensure price stability.

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. In Section 5 we described along which lines a European CBDC could be shaped to improve on the weaknesses of the DE's design as presently proposed.

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

Chaum, David, Christian Grothoff,Thomas Moser (2021): *How to issue a central bank digital currency.* Available at SSRN: https://ssrn.com/abstract=3965032

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

Grünewald, Seraina, Corinne Zellweger-Gutknecht, Benjamin Geva (2021): Digital Euro and ECB Powers, Common Market Law Review, Vol. 58, Issue 4, pp. 1029– 1056, https://doi.org/10.54648/cola2021066,

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

Tinn, Katrin (2025): *A theory model of digital currency with asymmetric privacy.* Management Science. https://doi.org/10.1287/mnsc.2024.06830

VISA (2018): *VISA Fact Sheet: What you need to know about one of the world's largest payment companies.* https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

Tables:

Table 1 Explicit 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.

Table 2 Implicit Goals	
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.