25. September 2023 (v1)

EPICENTER .WORKS for digital rights

Digital Euro and Right to Cash

Policy Analysis from a Human Rights Perspective

Introduction

This policy paper analyses the legislative proposal from the European Commission on the establishment of a digital euro[1] and the accompanying proposal on the legal tender of euro banknotes and coins[2], which were both released on 6th June 2023. Our analysis will focus on the fundamental rights aspects relevant to this legislation, its effect on citizens and a particular focus will be given to the privacy implications of each proposal.

We welcome the Right to Cash proposal and see it as a necessary step to tackle severe problems for financial privacy, financial literacy and the stability of the Eurozone. We support the proposal on the establishment of a digital euro as a much needed alternative to privacy invasive private digital means of payment, but only under the following three conditions:

- Firstly that it that it brings a level of privacy as close as possible to cash payments, which has to be significantly better than current digital payment systems, also with regards to user privacy towards the ECB and payment service providers.
- Secondly that this proposal does not undermine the stability of the Eurozone, in particular that (offline) payments in digital euro are protected from double spent.
- Thirdly, that it is built as a digital public infrastructure based on Free and Open Source Software, and open, inclusive and transparent standards and development processes.

Under these premises, this paper outlines risks we identified and proposes solutions where possible.

The Right to Cash

Banknotes and coins (cash) are not just the most privacy preserving means of payment, they are also the most inclusive and enhance financial literacy by their haptic and analog nature. They are resilient to power outages, even long-lasting ones. Availability of cash money is a precondition for societal

1 2023/0212 (COD) https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2023/0212(COD)&l=en .
2 2023/0208 (COD) https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2023/0208(COD)&l=en .

participation for financially excluded people, such as the less digital literates, unbanked, undocumented, elderly and young people. A European Union that is respecting its citizens' fundamental rights has to ensure the wide availability and acceptance of analog means of payment.

Hence, we are very supportive of the intention of the proposed regulation to ensure the status of euro banknotes and coins as legal tender. In our assessment, the circulation of cash money is already under threat in several Member States and there is a worrying trend in that direction in the majority of them. As the explanatory memorandum and the Recitals acknowledge and as is stipulated in Article 15 (2), this legislative proposal on the legal tender of euro banknotes and coins[3] is necessary irrespective of the digital euro and also needs to be evaluated on its own merits.

Ensuring Effective Access to and Acceptance of Cash

We want to strongly uphold Articles 4, 8 and 9 as the main pillars of the proposal. Without the sufficient and effective access to cash throughout the territory of a Member State and the ability to rely on cash as a means of payment for physical commercial transactions, exclusionary effects would proliferate against the most vulnerable parts of society. Ultimately, this also undermines the euro as a legal tender.

The unilateral refusal of cash by the payee[4] which is established in Article 4 can be exempted based on Article 5 only in so far as it is based on legitimate grounds and temporary, with a burden of proof on the payee for each individual case. We support these provisions and in particular the requirement of such refusals to be only permissible on a temporary basis.[5] Currently, in many EU countries payers can observe "No Cash" signs and policies in shops, which constitute a permanent and ex-ante unilateral exclusion of cash according to Article 3 (4) to which the payer hasn't consented. While we interpret the proposal as being clear on this point, we would strongly argue for the introduction of an Article about the Prohibition of the unilateral exclusion of payments in Cash. Such a provision can be found in Article 10 of the proposal for the digital euro and is lacking in the proposal for the right to cash. The purpose of this provision would be to clarify that such unilateral blanked ex-ante refusal of cash would constitute a violation of this provision and exemplify it with these signs. See below why such clarification seems needed.

In this light, Recital 10 describes the regulatory cooperation between the Commission, the European Central Bank ("ECB") and national competent authority ("NCA") currently with the aim of

> *"identifying cases of widespread ex ante unilateral exclusions of cash and inadequate access to cash in specific national territories or regions".*

The word "widespread" should be removed.

However, the possibility of introducing additional exceptions to the principle of mandatory acceptance at a later stage by delegated acts of the Commission is rather worrying, even though they shall not undermine the effectiveness of the legal tender status of euro cash. In particular, Recital 11 states that these exceptions should be without prejudice to the possibility for Member States to adopt national legislation introducing exceptions to the mandatory acceptance.

These wide-ranging powers of the Commission and Member States to establish exceptions to this Regulation is not in line with the judgement of the European Court of Justice (ECJ), which is referenced by Recital 11 of the proposal on the legal tender of euro banknotes and coins and Recitals 14 and 19 of the proposal for establishing the digital euro. It is true that the ECJ states that

3 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the legal tender of euro banknotes and coins COM/2023/364 final.

4 the recipient of the payment, e.g. the vendor

5 Article 5 (1) (a) limits cash refusal by the payee to legitimate **and** temporary grounds.

> **"***It follows from the information contained in paragraphs 46 to 49 of the present judgment that that* ***status as legal tender calls only for acceptance in principle*** *of banknotes denominated in euro as a means of payment,* ***not for absolute acceptance****."*[6]

However, it goes further and states

> *"[... M]oreover, is it necessary for the use of the euro as the single currency and, more specifically, for the preservation of the effectiveness as legal tender of cash denominated in euro that the* ***EU legislature lay down exhaustively and uniformly the exceptions to that fundamental obligation,*** *provided that every debtor is* ***guaranteed to have the possibility, as a general rule, of discharging a payment obligation in cash.****"*[7]

The current proposal is therefore not in line with the jurisdiction of the ECJ, it even stated that § 14 (1) sentence 2 German Central Bank Law ("Bundesbankgesetz" – "BbankG") is violating Article 3 (1) (c) TFEU, since it interfered with the exclusive competence of the EU in the matter of monetary policy.

> *"Article 2(1) TFEU, read in conjunction with Article 3(1)(c), Article 128(1) and Article 133 TFEU, and with the third sentence of the first paragraph of Article 16 of the Protocol on the ESCB and the ECB, must be interpreted as meaning that, irrespective of any exercise by the European Union of its exclusive competence in the area of monetary policy for the Member States whose currency is the euro,* ***it precludes a Member State from adopting a provision which,*** *in the light of its objective and its content,* ***establishes legal rules governing the status of legal tender of euro banknotes."***[8]

Moreover, future delegated acts by the Commission on exceptions are clashing with the demand of the ECJ to lay down an exhaustive and uniform list of exceptions.

If Member States introduce different exceptions, particularly because there is already an existing kind of infrastructure of only cashless payments, this negative development is rather consolidated than improved. This is particularly true for the development in some Nordic countries[9] where more and more shops are only using non-cash payments.

Moreover, Martin Selmayr, Head of Representation of the European Commission in Austria, stated in an article[10] that the exception of the mandatory principle to accept cash constitutes the individually negotiated contract to exclude cash. He said, especially smaller shops could unilaterally exclude the use of cash, because they are small and it would not be like if a big supermarket chain would do it.[11] However, precisely this scenario shall be prohibited by the proposal regarding the mandatory acceptance of cash. Article 3 (4) defines exactly that an

---

6 ECJ, judgement of 26. January 2021, C-422/19 and C-423/19, para 55.
7 ECJ, judgement of 26. January 2021, C-422/19 and C-423/19, para 55.
8 ECJ, judgement of 26. January 2021, C-422/19 and C-423/19, para 58.
9 https://www.nfcw.com/2022/08/16/378650/norway-finland-and-new-zealand-top-list-of-countries-closest-to-becoming-cashless/ .
10 https://www.derstandard.at/consent/tcf/story/3000000182964/was-die-eu-kommission-plant-um-bargeld-abzusichern .
11 "Probably the most significant exception, however, are private agreements that are protected by freedom of contract: Contractual partners – for example, a restaurant and its customer – can agree that they will process the payment digitally. This also applies in principle to "ex ante exclusions", as it is legally formulated in the regulation. This refers to situations in which, for example, a restaurant operator visibly displays a "No Cash" sign. The customer can then decide whether to sign the contract and commit to card payment or to buy elsewhere. "Ex-ante exclusions" are also only permissible if they are proportionate, Selmayr explains. "For a small tobacconist this will be the case, for a large supermarket rather not." (ebd.)

> *"**'ex ante unilateral exclusion of cash' means a situation when a retailer or service provider unilaterally excludes cash as a payment method** for example by introducing a **'no cash' sign**. In this case, the payer and payee do not freely agree to a means of payment for a purchase."*

First of all, in some Member States, e.g. Germany or Austria, smaller shops prefer cash as it does not bring charges of Visa/Master Card or other payment systems with it.

Secondly, such kind of ex ante exclusion is also a violation of consumer rights as regulated in the Directive on Unfair Terms in Consumer Contracts[12], which is transposed into national law of the Member states. Not individually negotiated clauses are not valid according to Article (3) (2) of the Directive on Unfair Terms in Consumer Contracts:

> *"A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, [...]."*

This shows that such an ex ante exclusion is prohibited for different reasons and by several European acts. Such kind of ex ante exclusion is not individually negotiated and also does not fall under the other exceptions mentioned in the regulation. This evident confusion should be met with clarifications in the proposal. Moreover, it should be made clear that accepting cash must not be made more expensive or less convenient than other means of payment. The proposal should be amended accordingly.

Enforcement

As always with EU law, if the aims of this legislation will be achieved strongly depends on enforcement in each Member State. We concur with the general enforcement structure of the proposal to oblige Member States to designate national competent authorities, give them the obligation to report and intervene to uphold Articles 8 and 9, while providing the Commission the power to step in should Member States not fulfill these duties. Therefore, we support the language in Article 8 (5) which empowers the Commission to independently assess the situation in each Member State and, via implementing acts, prescribe measures to be taken on a national level. It is vital that this provision upholds the phrasing "**despite the findings of the annual report**" because only then can such an independent assessment take place.

Subsequently, we would question the decision in Article 12 to make the amount of penalties for infringements of this legislation a purely national prerogative. Such penalties will most likely be targeted at enterprises for not accepting cash or financial institutions not providing sufficient or too expensive/burdensome access to cash (e.g. ATM fees, availability of human tellers in banks, etc.). Proportionality of penalties will be difficult to achieve in light of the great variance of the companies potentially targeted by them and the rarity of national penalties calculated as a revenue percentage[13]. Given that infringement proceedings around national penalty levels are extremely rare, a Recital should clarify that implementing acts of the Commission based on Article 8(5) can also address national penalty provisions.

Importantly, we believe complaints raised by affected groups are an integral part of any proper enforcement infrastructure. In particular the horizontal nature of this proposal reaching into all areas of life can only be enforced with inclusive complaint reporting. While we applaud the

12 COUNCIL DIRECTIVE 93/13/EEC, of 5 April 1993, on unfair terms in consumer contracts, (OJ L 095 21.4.1993, p. 29).
13 See page 13-15 https://en.epicenter.works/document/1522 .

acknowledgement of user complaints in the Explanatory Memorandum, the implementation in Article 14 critically falls short of this potential and renders it meaningless.

Article 14 should lay out what happens once a complaint is received, which procedurally guarantees apply and in which time frame a remedy can be expected. For example, critically low density of ATMs in rural areas or discrimination in the financial sector of vulnerable groups like Romani and Sinti directly affects societal participation, freedom to conduct business and the role of the euro as legal tender. Article 14 leaves all this up to the Member State, while in other areas the Commission has proposed legislation for the known systemic problems in the national enforcement of EU data protection law.[14] These same known problems will be repeated, if Article 14 is not strengthened. Should the right to cash be taken seriously, Article 14 needs to be drastically expanded to establish procedural guarantees for the complainant and oblige Member States to adhere to procedural guarantees and provide effective access to remedies.

It is extremely worrying that the current wording of Article 14 excludes civil society organizations ("CSOs"), as they are neither natural persons nor enterprises. CSOs are vital to empower otherwise disenfranchised people like the elderly, migrants or unbanked. They fulfill the role of an immune system in a democracy and they can sound the alarm earliest to start a debate about societal concerns. Hence, Article 14 should include all natural and legal persons.

Article 8 (4) establishes that Member States have to include in their annual reporting the remedial measures they commit to ensure effective access to and acceptance of cash, while saying such measures shall enter into force without undue delay. Hence, the reporting obligation in this provision should include also measures that have been implemented since the last reporting.

Reporting and Transparency

The annual reporting obligations for Member States according to Article 13 could provide an important foundation for an EU wide discussion on access to cash. To achieve this benefit, it would be helpful if Article 13 included the obligation by the Commission to publish those reports in a summary page and provide translations.

Furthermore, reporting obligations for Member States should go beyond "detailed data and assessment of the situation" by also including the methodology according to which this data was gathered, processed and analyzed. Additionally, it would be very easy and informative to include the complaints received by the national competent authority per type of stakeholder and the remedies taken in the reports. Lastly, we recommend the Commission to also be obliged to publish an annual transparency report that includes their analysis of the situation throughout the Union, trends they observe, summaries of discussions between the ECB, the Commission and national competent authorities, as well as explanations for and evaluation of delegated acts adopted by the Commission based on this Regulation.

Article 9 (2) establishes that the Commission may specify in implementing acts the "common indicators" with which Member States monitor and assess access to and acceptance of cash in all of their territory. We suggest adding concrete methodologies for the gathering of these indicators to the powers vested in the Commission. Otherwise, the annual reporting risks divergence between Member States which prevents comparability across the Union.

Digital Euro

With the proposed regulation the EU establishes a digital euro as legal tender, after about ca. 130 states, like China, India and Nigeria, in the world already introduced or are about to introduce such

14 2023/0202(COD) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0348 .

kind of digital currency with different acceptance and success rates.[15] Already in 2021, the G7 laid down "Public Policy Principles for Retail Central Bank Digital Currencies ("CBDCs")"[16] The digital currencies like BitCoin and Ether started already in 2009 and are now still around, but rather volatile and used for speculations. The fact that states want to issue a non-volatile version of a digital currency seems to be rather late and raises several fundamental concerns regarding privacy.

So far it is not clear for what kind of concrete use cases the digital euro should be an alternative to offline or online transactions. The latter has already many possibilities, e.g. Visa, Apple Pay or PayPal. However, the digital euro does constitute an alternative outside of a system that is using data for commercial purposes and process them in third countries that often do not comply with the GDPR. Nevertheless, the current proposal has limits, is not constructed as a digital public infrastructure and misses essential privacy safeguards. Therefore, a real alternative payment method would have been rather to create and promote European competitors to companies like Master Card or VISA, as several other world regions have done. This type of European competition on the payment service provider ("PSP") market is not achieved with a digital euro, since it is a digital asset like cash.

PSPs are obliged to offer digital euro accounts and provide customer support.[17] Whereas surcharges for digital euro payments are prohibited, merchant fees are foreseen and will be centrally regulated to be cost-covering or competitive, whichever is lower.[18] This leads to high permanent costs on the side of the merchant and for PSPs no revenue model exists. Subsequently, the roll-out of the digital euro is a large-scale operation that touches on most people's economic lives, that creates significant and ongoing adaptation cost. As there are no benefits for the PSPs or merchants to support the digital euro, the proposal solely relies on the power of the legal tender to force ubiquitous adoption. Only in case of a privacy-preserving digital legal tender there would be some benefits for people, such as independence of bank accounts for which an ID card and regular residency status is required, third party corporations, etc. Nevertheless, right now the digital Euro requires also some proofs of residency etc. This is why, there should be an alternative like a chargeable card for small amounts and direct debit and less preconditions in order to be able to use the digital Euro.[19] Even though the regulation does not foresee fees for digital euro users, costs created by the roll-out would most likely be shifted to consumers. For high adoption rates on the consumer and merchant side, it must be guaranteed that no shift of costs will appear. At the same time it must be guaranteed that the costs for cash and digital euro or other online payment methods are equal in order to encourage merchants to accept a wide range of payment methods, also for transactions of varying amounts.

As the digital euro is a central bank digital currency, it is an electronic equivalent to cash. The digital euro shall be available as online and offline version. The online version can be compared to payments with debit cards or bank transfer. The offline version of the digital euro shall be a digital version of cash and an alternative to card or contactless payments.

In the case of online payments, the digital euro account can be linked to a normal account and any sums received that exceed a certain limit, e.g. € 3,000, automatically flow over to the non-digital euro account. This concept is called the "waterfall functionality"[20]. In case the amount that shall be

15 https://www.reuters.com/markets/currencies/study-shows-130-countries-exploring-central-bank-digital-currencies-2023-06-28/ .
16 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf .
17 Article 13.
18 Article 7 (4) and Article 17.
19 ECB (2023): prsentation on digital financial inclusio, slide 6, https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230510_item5financialinclusion.en.pdf .
20 Recitals 36, 37, 39.

transferred is exceeding the digital euro funds on the wallet, funds from the non-digital euro account are automatically mobilized (reverse waterfall functionality).[21] Of course, within this framework, payments can be tracked by payment service providers and are no more anonymous than current bank transfers. They would be treated like private digital means of payment, consistent with current AML/CFT requirements, as explained further below. Moreover, there are also technical issues with the "waterfall functionality" which incurs high costs in order to be properly implemented in the light of privacy by design, if it is possible at all.

Another issue of privacy or rather security is the way the digital euro is designed. Currently it is discussed[22] that it might be token and not blockchain based. Token based means simply that it digitally represents a certain value/existing assets. Blockchain, however, is a decentralised privately owned system which saves a new block to the chain after a transaction, containing data who owns what and when ownership changed. The ECB will save the claims of the bearer of the token in a data base. These tokens can be transferred from peer to peer, also offline.

However, independently from the specific technology used, each digital euro has potentially an identifier and can be traced, similar to the blockchain, at least how it is currently described in the proposal. The blockchain is also not anonymous, since each transaction is public. But although privacy was the major priority of both citizens and business stakeholders in the consultation leading up to this proposal[23], the Commission has not delivered details and instead proposed a **privacy nightmare architecture** for the digital euro.

The privacy framework solely relies on the promise not to look. Safeguards that prevent the observability of user behavior, tracking and profiling on a technical level are currently missing in the proposal. There are also no rules that govern the re-identification of users or that limit the transfer or purposes of the processing of transaction data. For the online digital euro, the full transaction history of everyone is stored comparable to bank transfers. Contrary to other systems, that observability is not limited to the payee, but also includes the payer/consumer.[24] Even though user names and identifiers are replaced with user aliases once the data moves from the PSP towards the ECB, AML, CFT and other entities, this pseudonymity can be stripped away and the user re-identified without their consent, which the proposal justifies with AML in the public interest.[25] This revocation of the pseudonymity is notwithstanding other forms of re-identification based on behavioral data in the transaction history. The regulation needs to include safeguards against these risks that are agreed democratically and shouldn't leave such decisions to implementing acts.

For offline digital euro payments, the device identifier is processed by the PSP and ECB[26], whereby tracking of individual users becomes extremely easy. Contrary to other privacy friendly payment systems[27] the digital euro provides no reliable technical guarantees to protect a user's privacy. Additionally, the proposal is also not providing legal remedies to mitigate the risks arising from the flawed privacy architecture. In Recital 71 it states:

> *"[t]he settlement of digital euro transactions should be designed in such a way that neither the European Central Bank nor national central banks can attribute data to an identified or identifiable digital euro user."*[28]

21 Recital 36.
22 Q 22: https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb.faq_digital_euro.en.html .
23 https://www.ecb.europa.eu/pub/pdf/other/ .
Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf#page=11 .
24 https://en.wikipedia.org/wiki/GNU_Taler .
25 Article 31, Article 32 and Recital 78. Public interest in the sense of Article 6 (1) (d) GDPR.
26 Annex III and Annex IV.
27 e.g. https://taler.net/en/ or https://en.wikipedia.org/wiki/Monero .
28 Recital 71.

But in Article 37 (4) (b) a.o. the identifier of the local storage device for offline digital euro payments, shall be processed for AML measures.

Both statements contradict each other. This is why this issue should not only be engaged with in the Recitals, such kind of security requirements should be codified clearly in the regulation itself, i.e. it shall be described how the anonymity is secured when using offline payments that are not traceable, despite the final settlement infrastructure, i.e. when the records of the digital euro holdings are updated and how the digital euro is distributed, or attributed to a user wallet. Transaction data should also not be stored on the local storage device, even if this is only accessible to the holder of the device. The ECB itself researched on the possibility of anonymity vouchers, meaning a payee can spend a certain amount once or split it up.[29] Additionally, the European Data Protection Board recommended a threshold for transactions below which no tracing for online transactions is pursued.[30] Such guarantees are vital for the digital euro's success. Without reliable legal and technical safeguards, trust from citizens in any form of technical implementation of the digital euro would be misplaced.

Last but not least, the digital euro proposal must be seen in the light of the recent Payment Services Proposal[31], containing rules about open banking which are not privacy friendly. Therefore, the payment data generated by the use of the digital euro shall only be processed for purposes contained in an exhaustive list and not for commercial purposes or shared with third parties within the open banking framework. Following these considerations, this should be kept in mind when implementing the digital euro and choosing the company who is developing the digital euro. This operator should be a GDPR adhering company that is not subject to legal rules of third countries. We would also recommend a prohibition of Very Large Online Platforms from playing any role in the development of the digital euro.[32]

Architectural Considerations

In the end, the issued digital euros will be saved in the settlement infrastructure of the Eurosystem, i.e. some kind of data base of the ECB. This settlement infrastructure is part of the Eurosystem and Recital 64 explains that online digital euro payment transactions should be settled within seconds and final settlement of online transactions should be recorded immediately in the settlement infrastructure.

Regarding the payment function itself, specific secure parts of a chip in a mobile device shall be used, as explained in Recital 69.

29 ECB (2019): Exploring anonymity in central bank digital currencies, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf .
30 EDPB (2022): Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective, https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf .
31 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM/2023/367 final.
32 This list currently includes Amazon, which are supposedly involved in the development of the digital euro, while other European Open Source initiatives have been excluded by the ECB. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 .

Regarding offline payments, the settlement[33] works differently and without third parties, i.e. the settlement would rely on the local storage[34] (secure hardware). Although Recital 65 states that the settlement itself shall take place in the local storage of the devices of payer and payee[35]

This difference of settlement and final settlement is also stipulated respectively for online and offline payments in Article 30. The ECB published a digital euro glossary[36] which explains the different terms.

There might be an issue regarding **double spending**, meaning a digital Euro is duplicated and spent several times, comparable to print money. The technical design to prevent this scenario should be specified in the law as well as possible remedies and dispute resolution mechanisms for those affected by such an event. Regarding the issue of double spending, the Deutsche Bundesbank published a paper on "Eurosystem experimentation regarding a digital euro Research workstream on hardware bearer Instrument" and explains further the security features regarding the settlement infrastructure to prevent counterfeiting or double expenditure. The main focus lies on physically tamper-proof secure elements as well as isolated storage, that allows for the implementation of different control elements, e.g. holding limits and to store AML/KYC data.[37]

In general, the security issues are similar to those that arise when paying via NFC with a mobile phone, but with this proposal they suddenly pose a system risk to the Eurosystem and not only to individual private bank accounts. To be clear, adversaries could in theory use vulnerabilities in Secure Elements to double spend offline digital euros to obtain physical goods or exchange them for cash and this attack might be possible on a massive scale, particularly when combined with shutting down internet access. In the scenario where any of the proprietary vendors of Secure Elements has a vulnerability in one of their chips, such chips are by-design not able to be physically updated. This means such vulnerabilities survive as long as the device containing the chip is in use and could be used systematically to double spend money.

As the security design of such chips is often used to protect it from its users, it could deprive users from using Free and Open Source Software ("FOSS") – developed mostly by private individuals, groups or volunteers – also on smartphones, tablets and smartwatches. Due to the fact that FOSS could be seen as untrusted or simply overlooked when focusing on the two dominant Smartphone operating systems. Therefore, it should be taken into account while developing the digital euro infrastructure and drafting the proposal that, even the EU follows an Open Source Software Strategy[38]. It ensures the necessary transparency towards the citizens to establish trust into the solution as well as maintain sovereignty against any particular proprietary vendor. Moreover, the use of special cards or USB-like physical wallets should be promoted as mobile phone alternatives by the Eurosystem, as these are more easily and in a cheaper way replaceable. We would welcome such amendments in order to emphasize the role of the digital euro as a digital public infrastructure.

---

33 ECB digital euro glossary:
local storage settlement model: *A settlement model referring to Secure Elements in the end user's devices performing the technical tasks of verification and recording, in line with rules set by a central bank.*
Secure Element (SE): *A tamper-proof chip with pre-installed software that can store confidential and cryptographic data and run secure applications.*
34 ECB digital euro glossary: **local storage:** The secure storage and computational capabilities of an end user's physical devices, such as smart cards or mobile phones.
35 Article 2 (15)
36 https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220420.en.pdf .
37 https://www.bundesbank.de/resource/blob/873282/bd327431598f204c2ebac99f197ce863/mL/eurosystem-experimentation-regarding-a-digital-euro-data.pdf , p. 5.
38 https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en .

The proposal contains no provisions about liability in case of fraudulent transactions or how collisions in the settlement infrastructure would be resolved, for example when attackers shut down internet coverage in areas affected by double spend attacks. This seems to be a critical mistake in the current proposal that cannot be rectified easily. We would suggest a re-evaluation about the technical feasibility of the offline digital euro in light of attack scenarios outlined above.

Privacy Considerations in the Digital Euro

The reference made regarding AML-regulations shows even more threats to privacy. The proposal is still lacking a detailed description of privacy features or safeguards for the user. In Article 22 (2) of the Regulation it is made clear that digital euro users shall not be required to have or open non-digital euro payment accounts or accept other non-digital euro products.

The legislation distinguishes between offline and online digital euro payments. According to Article 14 (1) digital euro users who only use offline payments and do not connect their digital euro account to their bank account can access basic digital euro payment services. To include everyone, a vast range of devices shall be used. In the Recitals, they are called „local storage devices".[39] Before one can use the digital euro, one has to get an account at a PSP. They check the identity and whether one lives in the EU / a €-member state,[40] otherwise there are exceptions for people who do not fulfill these criteria. This basically means it is like registering a SIM card nowadays, so it is not anonymous at all to obtain digital euros.

Also, AML laws still apply. According to Article 14 (5) the Anti-Money-Laundering Authority ("AMLA") and European Banking Authority ("EBA") state that they should issue guidelines on the interaction between AML/CFT requirements and basic digital euro payment services, which contradicts the promise of anonymity.

The desire for anonymity in the digital euro, however, was more about the offline digital euro as a cash alternative. Cash is anonymous. Nobody knows who I am when I hand over a coin for goods. It should be the same with the digital euro. The current possibilities to pay with digital means, e.g. Apple Pay, GooglePay, PayPal, sofort.de, credit card etc. are mostly even worse regarding privacy than the digital euro, at least regarding the use of personal data for commercial issues and the central observability of all financial behavior of the user. However, the proposal foresees a unique digital euro payment account number that shall be given to each digital euro payment account,[41] so that it is pseudonymised and supposedly impossible to trace back to the real name of the account holder via the front end for suppliers and Central Banks. In reality, re-identification will be possible and is also foreseen in certain cases, as outlined above. However, the problem is that the proposal does not yet outline a procedure for AML and KYC. Article 32 (2) of the Regulation stipulates that the ECB should consult the EDPS before establishing an AML procedure, which of course can identify a person. The question is still whether this is necessary for any amount transferred or only above a transaction limit or in specific cases? Article 34 (1) (e) stipulates that payment service providers act in the public interest if they carry out AML/KYC measures. It would be disproportionate to deteriorate the privacy of all transactions in digital euro because of changing AML soft law that aims to detect and prevent a minority of illegal transactions. Ultimately, this problem can only be resolved with legal safeguards for user privacy and architectural guarantees of the digital euro enshrined in the regulation.

AML/KYC must be included in the technical architecture, The account-based approach makes it impossible to do both privacy preservation and AML/KYC compliance. The only way to achieve both is

39 Article 2 (31) ***'mobile device'*** *means a device that enables digital euro users to authorise digital euro payment transactions online or offline including in particular smarticle phones, tablets, smartwatches and wearables of all kind.*

40 Article 13 (1) (a).

41 Article 22 (3).

to use a system similar to BIC: using tokens and blind signatures, that would guarantee transparency of sales and privacy of purchases with much less (legal, technical) burden than tracking accounts and contracts.

Article 37 (4) (b) states that PSPs should only store the identifier of the local storage device used for offline payments, i.e. in the funding and defunding and registration process as described in Article 34 (b) and (c). Meaning, according to Article 37 (2) transaction data shall not be retained, so offline payments shall be anonymous for the PSP. Yet, the prohibition to retain transaction data by the PSP does not provide for the privacy-friendly architecture where such data is never processed by the PSP in the first place.

Unlike cash, even offline payments with the digital euro do not provide the same degree of anonymity for small amounts. Unfortunately, the exact technical implementation is still unclear and might also change over time. Even if offline payments are not supposed to be tracked, an assignment of individual transactions of the digital wallet with the merchants is possible ex post for the clarification of potential money laundering offenses. Combined with a time-based component, it is possible to create a movement profile or profiles about preferences or consumption patterns of a person.[42]

However, according to Article 32 fraud prevention is to be established by the ECB with the aim to "have the full picture".[43] Such a system shall in a way be comparable to already existing payment schemes and promise to ensure that an individual euro user is not identified by the central fraud detection and prevention mechanism, whereby the last requirement is contradicting the meaning of fraud detection.

Although the proposal tries to aim for privacy, it makes naturally reference to AML and KYC as well as fraud detection measures, as the settlement infrastructure is part of the Eurosystem, which underlies strict rules. This contradicts especially the aim of offline digital euro payments which should be anonymous like cash. Even though many provisions state that personal data is only processed in specific cases and mostly in a pseudonymous way so that an individual is not directly identifiable, the annexes lists which kind of data is processed by which institution. The worrying part is that the actual privacy preserving safeguards are not stated in the proposal itself. It refers in the Recitals, but also expresses in Article 32 (2) that

> *"[T]he **European Central Bank shall consult the European Data Protection Supervisor prior to developing the details** on the operational elements of the fraud detection and prevention mechanism."*

The same goes for the statement in Article 5 (2), which refers again to details of measures, rules and standards, which still need to be adopted by the ECB and in case privacy issues are touched, the European Data Protection Supervisor ("EDPS") shall be consulted.

Of course, we welcome that the proposal includes the EDPS. However, the regulation either contains the necessary safeguards for the protection of personal data or the EDPS will also not be able to unilaterally design an architecture against the political pressure of the Commission, the ECB and the anti-money laundering authority. Such kind of technical details regarding privacy and the concrete functioning of the digital euro should be decided democratically and enshrined in the legislation. This proposal right now only lays down the basis to introduce the digital euro, but refers to privacy issues only in a broad sense. This opens the doors for implementing acts deciding the actual privacy for every user of this digital currency. As outlined above, the main priority from all stakeholders in the consultation of this proposal was privacy. It seems puzzling why the Commission failed to address many vital questions.

42 Recital 34.
43 Recital 68.

As such kind of fraud detection mechanisms are already established in the current payment systems, e.g. for bank transfers etc., it must be possible to stipulate rules more precisely.

Furthermore, AML and KYC mechanisms simply make anonymous payments not as anonymous anymore, Article 37 (4) states exactly what kind of data shall be made available to the Financial Intelligence Unit and other competent authorities for AML purposes. This is also valid for offline digital euro and includes the amount funded or defunded, the identifier of the local storage device for offline digital euro payment, the date and hour of the funding and defunding transaction as well as the account numbers used for funding and defunding.

In the end, according to the proposal even the offline version of the digital euro would not be fully anonymous. The privacy features are not as promising as they seem. At least for small amounts and sums, totally anonymous payments with the offline digital euro should be made possible. If the digital euro should be a real alternative for cash, this amount of trust shall be given to citizens using this new means of payment.

Technically, it is planned that, for example, all issued tokens are stored as a kind of back-end infrastructure at the ECB,[44] so that so-called "double spending" is prevented.[45] However, this also means that at least the merchant must always be online in order to be able to cross-check with this list or another kind of verification system must be created and included in the proposal. The person paying with the digital euro offline must have a digital euro account with some payment service provider that is not necessarily linked to their normal account.[46] The digital euro can be loaded onto any device,[47] most likely a smartphone or wearable with a corresponding app. For this account, the person receives an identifier and must also prove to live in the euro area or a special agreement is signed by the Member States in case a person is from a Member State that is not part of the euro area[48].

Hence, the current proposal foresees KYC as the precondition for any digital euro transaction. Such identification information should not be transmitted with digital euro transactions if any comparison to cash is to be drawn. However, the problem of money laundering prevention (AML measures) remains. If the all transactions are truly anonymous, then money laundering could potentially not be detected. But, in a suspicious case, the "contracts" on which the purchase is based can be demanded from the traders. However, it is not possible to find out whether the person who owns the wallet actually concluded these contracts or whether the offline digital euros were stolen.

This means that **the digital euro is not as anonymous as cash, even** for **offline payments of small amounts.** This is why, it should be clarified in the digital euro proposal as well as in the proposal for an AML regulation[49] that **AML/KYC cannot be a kill-switch for privacy.** The proposal needs to be amended in order to include privacy safeguards that provide users with guarantees Impervious to changes in secondary law and technical implementations. Small offline digital euro payments have to be possible in a completely anonymous way. Clarity about the level of financial privacy of citizens using the digital euro needs to be codified in the proposal and enforced by

44 Article 2 (29); ECB digital euro glossary: **back-end infrastructure:** *All hardware and software components (e.g. servers, applications) necessary for data storage and processing of digital euro holdings and transactions. The infrastructure interacts with front-end services or other back-end infrastructures via defined* interfaces. Its functions include processing payment instructions and storing data on updated digital euro holdings.
45 Martin Summer, Hannes Hermanky, MONETARY POLICY & THE ECONOMY Q1– Q2/22 91, A digital euro and the future of cash, p. 14.
46 Article 13 (4) (b), (7).
47 Article 2 (1).
48 Article 18 (1), (2) a).
49 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing COM/2021/420 final.

mandatory notifications in case of re-identifications of users by anyone else. Furthermore, differences for the privacy guarantees of payers and payees should be explored to bring the proposal in line with privacy requirements, while still keeping AML measures possible. Sadly, this discussion around safeguards is only starting after the Commission has already launched its proposal.

European Digital Identity Wallet and the Digital Euro

According to Article 25, the frontend functionalities of the digital euro shall be coupled with the European Digital Identity Wallet (EUDI Wallet). Epicenter.works commented extensively on the reform of the eIDAS regulation, which is currently in the trilogue stage and the outcome of which is still very much unclear.[50] The **centralization towards one single software solution** for eGovernment, public transport, social media, banking, commerce and many other areas of life is already creating a dangerous single point of failure. Tying payment into the EUDI Wallet as well, increases this danger manifold and further erodes citizen trust in their financial privacy.[51]

Furthermore, integration with the EUDI Wallet should not limit the availability of the digital euro to devices that support this particular software. Many people in the Eurozone do not have a modern smartphone, lack the digital literacy to operate such technology safely or lack the income to even afford them. Similarly, a significant part of the population decides not to use smartphones from the two dominant vendors Apple and Google. Such open smartphone operating systems should not be excluded from the digital euro. Therefore, it should be promoted that other kind of "local storage devices" can be used as well, e.g. certain kind of cards or memory sticks that can be used as physical wallet.

Regulated Access to Secure Elements

Success of the digital euro implementation on handhelds and wearables will depend on access to certain hardware functionalities on the device. In general, such access entails the risk of undermining the security features of mobile devices. This risk can be adequately resolved with propoer secure architecture, that allows regulated third party access. Article 33 obliges equipment manufacturers of mobile devices to allow providers of front-end services effective interoperability with hardware features and software features necessary for storing and transferring data to process online or offline digital euro transactions, on fair, reasonable and non-discriminatory terms. The same article provides a caveat to ensure that interoperability does not compromise the integrity of the hardware and software features concerned. Concretely, can we find a reference to the NFC and Secure Element technologies necessary in Recital 69.

The primary risk that a smartphone or other local storage devices can be lost, stolen or broken at any time, could only be addressed by needing several of them. The NFC standard which serves as the communication medium for digital euro transaction is completely open. The software that runs on tamper-resistant security chips, i.e. Java cards and the "applets"[52], is completely proprietary, patented, secret and only accessible to a small group of industry actors. It should be in the interest of the public that independent assessments of the security architecture of our currency is made possible. The trade-off to make the security of a consumer device dependent on hardware elements might be acceptable. **Betting the stability of the Eurozone on proprietary security** of opaque business practices is irresponsible and should not be acceptable. Open standards would also help to prevent security gaps in secure elements that cannot be fixed.

50 https://en.epicenter.works/documents?field_tags_tid=19 .
51 As outlined in a recent open letter signed by 24 NGOs, academics and research institutions about the current obstacles in the negotiations. https://en.epicenter.works/document/4762 .
52 https://www.oracle.com/docs/tech/java/java-card-data-sheet-19-01-07.pdf .

Monetary Policy and Financial Stability

At times, fears arose in the media that people would rather hold their savings as digital euros than in their bank accounts, and thus that a run on the banks could take place that would endanger the financial system.[53]

The Commission tried to calm these fears with the introduction of holding limits in Article 15 and 16 of the proposal and the waterfall mechanism[54]. The holding limits shall be introduced according to Article 16 which regulates the limits to the use of the digital euro as storage of value. Therefore, the ECB shall introduce respective instruments, in particular, adhering to financial stability safeguards.

The Lisbon Treaty gave the ECB the status of a European Union organ[55], it has legal personality,[56] together with the National Central Banks ("NCBs"), it forms the Eurosystem. They are making monetary policy, independently from politics. The main task is to provide price and financial stability.[57] In order to pursue these tasks, it can issue legal acts on its own.[58]

This is why the ECB would contradict its mandate if it would allow an unlimited store of value when introducing the digital euro. It would provoke a "run on the banks" and risk financial instability. Obviously, this cannot be the goal of the introduction of the digital euro. With the decision to prohibit interests on the digital euro, it is emphasized that the digital euro is an alternative to cash and not like money in a bank account that is rather a claim against the bank that each bank account holder possesses.

However, the competence for the introduction of holding limits is a bit contradictory and should be rephrased unambiguously. In Article 16 (1) it says that the ECB shall develop instruments to limit the use of the digital euro as a store of value, but Article 37 (5) states that the Commission is empowered to adopt implementing acts on transaction and holding limits.

In general, the EU has the exclusive competence regarding monetary policy for the Member States whose currency is the euro.[59] It is clear that the ECB shall define and implement the monetary policy of the Union.[60] However, in case of a clash between implementing acts of the Commission regarding holding limits and financial stability, it should be made clear in the proposal that such implementing acts shall not interfere with the primary task of the ECB to ensure financial and price stability, particularly in the light of the possibility of the ECB to issue legal acts of its own.

For smooth transactions despite the holding limits, the waterfall mechanism mentioned in Article 13 (2) in conjunction with Article 16 comes into play. If an online digital euro account receives more than the holding limit allows, it directly transfers the funds to the non-digital euro account that is connected to it (waterfall functionality).[61]

This kind of waterfall mechanism is introduced in order to implement the aforementioned holding limits and as an instrument to ensure financial stability and the prevention of misuse of the digital euro as store of value. Furthermore, according to Article 16 (8) the digital euro shall not bear interest, which aims to further discourage people to use the digital euro as a store of value.

53 https://www.politico.eu/article/politico-pro-central-banker-boe-super-supervision-digital-euro-delay-r-expectations/ .
54 Recital 36.
55 Article 13 (1) TEU.
56 Article 282 (3) (1) TFEU.
57 Article 127 (2) TFEU.
58 Article 127 -133, 138 in conjunction with Article 282 (4) (1) TFEU.
59 Article 3 (1) (c) TFEU.
60 Article 127 (2) TFEU.
61 Recital 36.

Article 4 (2) states that the digital euro shall be a direct liability of the ECB or of national central banks towards digital euro users. And Article 2 (11) stipulated as well, that digital euro exchanged for cash or funds, are creating a direct liability of the ECB or a national central bank towards that digital euro user. Recital 9 clarifies that it is the same case with euro banknotes and coins nowadays.

This kind of "liability" is also explained on the website of the ECB.[62] Cash is central bank money and electronic payments are private money. The former is public and therefore backed by the public sector. Commercial banks also create money when they for example grant loans. This private money is also the same as the balance on the bank statement. It is converted to central bank money when withdrawing it from the ATM.[63] The customer has a pure claim against the private bank to receive the money stored on the bank account. The digital euro, however, is an equivalent to cash and therefore public money, issued by the central bank, there is not a claim against the PSP to hand out the stored money like having a claim regarding the money on the bank account. The money is stored in the digital euro wallet, like in a money purse. These definitions in the digital euro glossary[64] of the ECB illustrates the differences quite well.[65]

Moreover, Article 13 (6) states explicitly that digital euro users do not have any contractual relationship with the ECB or the national central banks ("NCBs"). This means, they have **no claims against the ECB or NCBs**, meaning it is **not** a kind of public money that is more secure than money of private banks or more protected against a financial crisis in the sense of bailing out the PSPs, because central banks cannot go insolvent.

Nevertheless, Article 31 (2) of the proposal regarding switching of digital euro payment accounts is disconcerting, because it states that in case a PSP is operationally not in a position to provide digital euro payment services or has lost the payment account-related data, the ECB and NCBs may authorise switching the account to another PSP.

This could imply that this is also valid in case of the insolvency of a PSP and therefore imply that the ECB is liable in the sense of being held legally accountable since the digital euro is its "liability". However, as explained above, the difference here is, that the ECB does not bail out private banks and money that is lost because of insolvency of private banks that exceed the deposit guarantee scheme. The money on classic bank accounts is not public money issued by the ECB, but a claim of a private individual against their private bank. Hence, the digital euro is cash like, i.e. it is public money and stored in the wallet of the digital euro user on a mobile device, not at a bank. A PSP is providing a kind of frontend solution, maybe like an app or similar software. In case everything of the infrastructure of the PSP is lost to provide for the digital user account data, due to insolvency, fire in a data center, etc., it shall be possible to switch and reopen the account at another PSP in order to continue using the digital money. This money is not lost or like in an insolvency used for satisfying creditors which are ranked higher to be satisfied in case of insolvency above deposit insurance.

62 https://www.ecb.europa.eu/stats/policy_and_exchange_rates/banknotes+coins/circulation/html/index.en.html .
63 https://www.ecb.europa.eu/ecb/educational/explainers/html/digital_euro_central_bank_money.en.html
64 https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220420.en.pdf .
65 ***Digital Euro***: A retail central bank digital currency (rCBDC) that the Eurosystemmay issue in the future.
retail central bank digital currency (rCBDC): central bank liability in digital form offered to the general public (e.g. individual users, business users and governments or other public authorities) for retail payments.
wholesale central bank digital currency (wCBDC): A central bank liability in digital form used by eligible entities (usually banks) for the settlement of wholesale payments.
synthetic central bank digital currency (sCBDC): A digital asset issued by private-sector firms (i.e. not by a central bank) and backed by central bank liabilities. It is therefore not a CBDC.

This is why it should be made clear in the proposal that the ECB is not bailing out PSPs in case of failure nor does "direct liability" mean that digital euro users can claim money directly from the ECB in case a PSP is insolvent or similar. Moreover, it shall be made clear that these transaction limits only apply to the digital euro and not cash. There is already a limit on cash payments within Europe to protect against money laundering. But it should be taken into account that rather small payments do not qualify for money laundering and criminals will rather stick to cash.

Sincerely,
epicenter.works – for digital rights