



Introducing a digital euro and guaranteeing the right to cash in Europe

EDRi Position Paper¹

1. Summary

EDRi welcomes the EU Right to Cash proposal as a crucial measure to protect and restore access to privacy-preserving payment options, as it ensures the availability of cash as the default, most inclusive, and privacy-preserving means of payment in Europe.² We consider the parallel adoption of the right to cash as a prerequisite for the introduction of a digital euro.

EDRi welcomes, in principle, the premise to establish a public digital payment infrastructure as a viable alternative to existing commercial and privacy-invasive digital payment systems. Unfortunately, the current European Commission proposal for the establishment of a digital euro (Digital Euro Regulation) contains severe shortcomings, particularly with regards to the protection of privacy.³ We argue that the level of privacy protection of the digital euro must be as similar to cash as possible and must be built as truly public infrastructure.

This paper identifies a number of major problems that need to be resolved in order for the digital euro to become an inclusive, reliable, and rights-respecting digital contender to dominant commercial digital payment solutions.

In a digital society, people need a public alternative to private digital payment methods, which are too often coupled with invasive personal data collection and abuse. We welcome the intention of the European Commission and the European Central Bank (ECB) to build a public digital payment infrastructure that can provide such an alternative and complement cash.

1 This position paper has been authored by EDRi with contributions from EDRi members epicenter.works and Open Future.

2 'Proposal of the European Commission for a Regulation of the European Parliament and of the Council on the legal tender of euro banknotes and coins' (Right to Cash Regulation), 28.6.2023, 2023/0208 (COD).

3 'Proposal of the European Commission for a Regulation of the European Parliament and of the Council on the establishment of a digital euro' (Digital Euro Regulation), 28.6.2023, 2023/0212(COD).



This also means that all key rules and design decisions must be under the control of democratically legitimate public institutions and must have the interests of the people using the payment infrastructure at their centre.

Unfortunately, the digital euro as proposed by the Commission leaves key architectural privacy considerations to be decided by implementing and delegated acts outside of the democratic process. Instead, those considerations need to be prescribed in the legislation itself. The current proposal provides no reliable guarantees for the user against pervasive tracking of their payments and has a privacy architecture that falls short of European data protection standards. Furthermore, the proposal makes it impossible for people to know in which concrete scenarios and by whom their payment data can be accessed. As a result, the proposed digital euro would have a privacy score closer to existing digital payment solutions like PayPal or Visa, and be far worse than paying with cash.

A digital euro that replicates key features of cash, on the other hand, would be a major innovation for people in the EU. It would enhance privacy in both online and offline payment scenarios and be built on free software and open standards in accordance with the Open Source Strategy of the European Union.⁴ Europe needs a privacy-preserving, inclusive digital payment method that can be used free of charge by everyone. We urge the co-legislators to ensure that this is realised in the Digital Euro Regulation.

2. The right to cash

Banknotes and coins (cash) are not just the most privacy-preserving, but also the most inclusive, means of payment. Cash enhances financial literacy by its haptic and analogue nature, it is long-lasting and resilient to power outages and cyberattacks. The availability and general acceptance of cash is a precondition for societal participation for financially excluded people, such as people with certain disabilities, people who are less digitally literate, unbanked, undocumented, or elderly.

A European Union that respects people's fundamental rights has to ensure the wide availability and acceptance of cash. EDRi therefore welcomes the proposed regulation to guarantee

⁴ European Commission, Open source software strategy 2020-2023 (C(2020) 7149 final), 21 October 2020.



the crucial status of euro banknotes and coins as legal tender in the EU (Right to Cash Regulation).

Today, the circulation of cash is already under threat in several Member States and there is a worrying trend in that direction in the majority of the remaining ones. EDRi strongly recommends, therefore, to uphold Articles 4, 8 and 9 as the main pillars of the proposal. Without the sufficient and effective access to cash throughout the territories of all EU Member States 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, and by that undermine the euro as a legal tender.

Currently, in many EU countries, payers can observe “No Cash” signs and policies in shops and restaurants, which constitute a permanent and *ex-ante* unilateral exclusion of cash. EDRi therefore welcomes the explicit obligation in Article 4(2) for all payees to accept cash, and that the exceptions established by Article 5 only allow for the unilateral refusal of cash by payees where they are temporary and based on legitimate grounds, with a burden of proof on the payee for each individual case.

However, the power bestowed on the Commission by Article 6 to unilaterally create additional exceptions to the mandatory cash acceptance should be removed. Such wide-ranging powers risk undermining the very purpose of this Regulation and are incompatible with the European Court of Justice’s own jurisprudence, according to which only the legislator can define any exemptions to the acceptance of legal tender.⁵

The Commission proposal also includes a rather weak enforcement regime that risks turning the Right to Cash Regulation into a paper tiger. While it is crucial that the proposal empowers the Commission to adopt additional rules on cash acceptance in case a member state’s status quo is not in line with the right to cash, the proposal does not specify EU-wide penalties for non-compliance by private actors. If penalties can be decided by member states, those with little interest in the right to cash are also more likely to enact low consequences for non-

5 It is “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,” from ECJ, judgement of 26 January 2021, C-422/19 and C-423/19, para 55.



compliance. Instead, the Right to Cash Regulation should include minimum penalties across the EU.

EDRi welcomes the transparency around ways to seek remedies included in Article 14, but notes that the provision should open up remedies to all natural *and* legal persons, not only enterprises, and add procedural guarantees for complainants for effective redress in case of infringements of the right to cash.

3. How to build a digital euro

Cash is currently the only payment method that allows consumers to pay anonymously. There are no identification requirements to access cash and no transaction data are stored when paying with cash. This is why the introduction of any digital euro must always be accompanied by the right to cash.

In an increasingly digital society, where more and more transactions are made through digital payment instruments like cards, mobile applications and private payment services, cash transactions are often not possible (as in e-commerce transactions) or increasingly perceived as less convenient (in point of sale transactions). Current commercial digital payment methods, however, store enormous amounts of personal data — including personal identifiers and information about the transaction, like who paid when for what — that reveal intimate details about everyone's private lives. In many cases, transaction data are used for profiling and are shared with third parties for purposes beyond the initial payment service, for example marketing and surveillance advertising.

A digital euro has the potential to provide a democratic and inclusive alternative, provided it allows payments both online and offline, with limited identification requirements and strict limits on the storage and sharing of personal information.

Make it token-based

Payment systems can be account-based or token-based. "In an account-based system, a payment is made by debiting the payer's account and crediting the payee's account. This implies that the transaction must be recorded and involved parties identified," explains Thomas Moser



of the Swiss National Bank.⁶ An account-based payment infrastructure therefore puts its trust into the known identity of the account holder. This is why an account-based system needs to establish processes for verifying the identity of the payer. Bank deposits and SEPA transfers are examples of account-based payment systems.

In a token-based system, a payment is made by transferring a token that represents monetary value. The prime example is cash: when handing over coins or banknotes, there is no need to record the transfer or identify the parties involved. The possession of the token is enough. When paying for a cup of coffee with cash, for example, the only thing the merchant needs to worry about is that the coins used to pay are not fake. Most importantly, the merchant does not need to know anything about the payer. The only requirement of a token-based system is that the payee must be able to verify the token's authenticity.

"The critical distinction is the information carried by the information asset. In an account-based system, the assets (accounts) are often associated with transaction histories that include all of the credit and debit operations involving the accounts. In a token-based system, the assets (tokens) carry information about their value and the entity that issued the token. The only possibility of attaining the transaction privacy property of cash, therefore, lies in token-based systems," Moser explains further.⁷

The Digital Euro Regulation must therefore prescribe that the European Central Bank implements a token-based system that achieves the same level of privacy protection from which people benefit when they make cash payments.

Add strong privacy safeguards

The Commission proposal contains insufficient privacy safeguards. Its privacy framework appears to rely solely on the ECB's promise not to look at all the data that are being processed. Safeguards to prevent the observability of user behaviour, tracking and profiling at a technical level are currently lacking.

Instead, we urge that the new payment infrastructure must follow the data minimisation principle of the EU's General Data Protection Regulation, and only process personal data that are

6 Christian Grothoff and Thomas Moser, "How to issue a privacy-preserving central bank digital currency", SUERF Policy Briefs No 114, June 2021.

7 Ibid.



absolutely necessary for the provision of the digital euro. That does not preclude the ECB to identify payees, for example for tax or anti-money laundering (AML) purposes, but it requires the technical impossibility for the ECB and other actors involved in running the infrastructure to identify and profile individual payers or track individual payment histories. Online payments (both point of sale and e-commerce) are the main use case where the Digital Euro Regulation can ensure additional privacy for people using the digital euro.

In addition, the Regulation must include a strict purpose-limitation provision for the use of any personal information generated as part of the processing of transactions by both private payment service providers and banks, including the ECB. Personal data processed for payments should never be shared or used for purposes unrelated to enabling the original payment, such as for marketing or surveillance advertising. That means that the digital euro should also not be part of the open banking framework created by the EU.

The proposed Digital Euro Regulation mentions "state-of-the-art security and privacy-preserving measures" but does not specify any such measures. To ensure that this provision does not remain an empty shell, EDRi recommends including explicit privacy-by-design language in the Regulation. This must explicitly specify in which cases payment data are protected and when and who can potentially access what and for which purpose. Such technical standards for security and privacy-enhancing measures cannot be outsourced to delegated acts.

To ensure that offline transactions are as anonymous as cash, the ECB and any other institution running the digital euro infrastructure should never store users' transaction data. This does not preclude individuals to use wallet apps or payment services that offer the storing of their own transaction history.

Although the possibility to attach a user's wallet to an existing bank account is not precluded, any requirement to establish mandatory links of digital euros to their current owner should be removed. They are fundamentally incompatible with the Regulation's stated goal to create a digital euro that offers a level of privacy equal to cash. Better protection of privacy can also be



achieved with cryptography, such as blind signature techniques,⁸ as well as by enabling low-amount payments via anonymous, (re)chargeable payment cards.

Build truly public infrastructure

EDRi in principle welcomes the proposed Digital Euro Regulation, as it demonstrates the ambition of the European Commission and the ECB to implement a public digital infrastructure for digital payments that can serve as an alternative to dominant commercial payment instruments.

We also note with interest that the digital euro proposal takes advantage of some of the newly-introduced vertical interoperability provisions contained in the EU Digital Markets Act in order to limit the risk of vendor lock-in to gatekeeper services.

However, the proposal should clarify that an infrastructure as critical as a digital legal tender should never be built and operated as a proprietary and closed-source system by for-profit corporations. Instead, the Digital Euro Regulation must prescribe that the core infrastructure is operated by the Eurosystem (i.e. ECB and central banks), and that it is transparently developed and implemented based on free and open source software,⁹ and open, patent-free standards.

This open technical approach will ensure Europe's digital sovereignty and enable permissionless innovation in payments, for example by app developers and other software and hardware companies. As emphasised in the European Commission's own Open Source Software Strategy, "open source allows for incremental innovation, based on the sharing of knowledge and skills. Openness increases trust in public services. It helps to solve complex technological problems by getting others to contribute unexpected solutions." The use of free and open source software also "multiplies Europe's efforts on its digital capacities and strategic infrastructures."¹⁰

8 Blind signatures are a form of digital signature in which the content of a message is disguised (blinded) before it is signed. They are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes. Blind signatures were introduced by David Chaum (1983), "Blind Signatures for Untraceable Payments", *Advances in Cryptology*. Vol. 82. pp. 199–203.

9 "Free" software does not relate to free as in gratis, but as in freedom. Read more about free software. Free Software Foundation Europe (FSFE), "What is Free Software", available at <https://fsfe.org/freesoftware/freesoftware.en.html>

10 European Commission, Open source software strategy 2020-2023 (C(2020) 7149 final), 21 October 2020.



That also means the digital euro should never rely entirely on vendors' security hardware and firmware, such as Secure Elements, that is today built into many modern smartphones. These Secure Elements currently operate as proprietary black boxes, the security of which users, regulators, infrastructure providers, and policymakers are unable to verify. Otherwise, we would have to trust a small number of foreign companies, mostly from the U.S. and Asia, that those Secure Elements are secure enough to protect the functioning of the Eurozone and prevent the misuse of the system, for instance for large-scale double-spending of digital euro.

What is more, Secure Elements are based on irremovable microchips whose firmware can, by design, not be updated. In case software vulnerabilities are found, millions of Europeans would therefore be forced to use unsecure devices for paying in digital euros. In addition to free and open source software implementations, the use of payment cards or USB key-like physical wallets should therefore be promoted as alternatives by the Eurosystem, as these are easier, cheaper, and more easily replaceable than smartphones.

The Digital Euro Regulation must make sure that the entire core infrastructure stack is under the control of democratically legitimate public institutions, without dependencies on commercial platforms or private infrastructure providers.

4. Recommended reading

Epicenter.works, "Right to Cash and Digital Euro: Policy Analysis from a Human Rights Perspective", September 2023, available at <https://en.epicenter.works/document/4878>.

Grothoff, Christian and Moser, Thomas, "How to issue a privacy-preserving central bank digital currency", 1 June 2021, available at <https://ssrn.com/abstract=3965050>.

Taler Systems SA, "GNU Taler: Features", available at <https://taler.net/en/features.html>.
