# Digital Euro: Frequently Asked Questions Revisited

JOE CANNATACI, University of Groningen, Netherlands
BENJAMIN FEHRENSEN, Bern University of Applied Science (BFH), Switzerland
BERND LUCKE, University of Hamburg, Germany
MIKOLAI GÜTSCHOW*, Dresden University of Technology (TUD), Germany

The digital euro FAQ published by the European Central Bank (ECB) provides answers to 25 frequently asked questions about the digital euro, the envisioned retail central bank digital currency for the euro area. In this article, we question the answers based on our analysis of the current design in terms of utility, cost, and technical feasibility.

In particular, we discuss the following key findings: (**KF1**) The design process has been exclusionary, with critical decisions being set in stone before public consultations. Alternative design ideas have not even been discussed by the ECB. (**KF2**) Secure and robust implementation of the offline design is technically infeasible. (**KF3**) The legal and financial liabilities for the various parties involved remain unclear, while (**KF4**) the design lacks well-specified economic incentives for operators as well as a discussion of its economic impact on merchants. (**KF5**) The ECB fails to identify tangible benefits the digital euro would create for society, in particular given that the online component of the proposed infrastructure mainly duplicates existing payment systems. Finally, what concerns us most is (**KF6**) the monitoring of all online digital euro transactions by the ECB, conflicting with privacy requirements.

CCS Concepts: • **Social and professional topics** → **Government technology policy**; *Surveillance*; • **Information systems** → **Digital cash**; • **Security and privacy** → Tamper-proof and tamper-resistant designs;

Additional Key Words and Phrases: digital payment, security, retail CBDC, privacy of means of payment

**ACM Reference Format:**
Joe Cannataci, Benjamin Fehrensen, Bernd Lucke, and Mikolai Gütschow. 2025. Digital Euro: Frequently Asked Questions Revisited. *J. ACM* 0, 0, Article 0 (December 2025), 10 pages. https://doi.org/XXXXXXX.XXXXXXX

## 1 INTRODUCTION

The Eurosystem under the leadership of the European Central Bank (ECB) has been working for several years towards providing a retail central bank digital currency (CDBC). Since the presentation of the ECB's current plans (in the following referred to as "the digital euro") and a European Commission draft legislative proposal in summer 2023 [15], the ECB has started to provide information material to the public, including a list of frequently asked questions (FAQ) about the digital euro [9].

In this article, we provide a detailed criticism of the ECB's proposed design by responding to its official FAQ. Section 2 starts with a brief overview of the digital euro design according to publicly available documents [8, 10, 14, 15]. Section 3 gives a summary and short explanation or our key

Authors' addresses: Joe Cannataci, j.a.cannataci@step-rug.nl, University of Groningen, Groningen, Netherlands; Benjamin Fehrensen, benjamin.fehrensen@bfh.ch, Bern University of Applied Science (BFH), Biel/Bienne, Switzerland; Bernd Lucke, University of Hamburg, Hamburg, Germany, bernd.lucke@uni-hamburg.de; Mikolai Gütschow, Dresden University of Technology (TUD), Dresden, Germany, mikolai.guetschow@tu-dresden.de.


0004-5411/2025/12-ART0 $15.00
https://doi.org/XXXXXXX.XXXXXXX

findings and the major problems with this design. Our detailed analysis of the answers of the ECB can be found in Appendix A—clearly highlighting that the current answers fall short. We conclude with recommendations for a successful digital euro in Section 4. The aim of this article is to provide a more comprehensive discussion of the current design to enable informed decisions, but not to argue against the introduction of any potential common digital payment system for the euro area.

## 2 DIGITAL EURO DESIGN

The ECB proposes "the digital euro", suggesting a single digital version of the euro. In fact, its design encompasses two mostly separate parts as depicted in Figure 1: The online version that mainly adds another layer of complexity to the existing digital payment infrastructure; and the offline version that is supposed to mostly resemble physical cash by providing full anonymity and operation with only occasional Internet connectivity. Both follow a two-tiered architecture, where the ECB acts as the central trusted instance for issuance and settlement. Participating payment service providers (PSPs) such as banks or public entities [15, Rec. 29] interact with end-users for identification and authentication adhering to legal know-your-customer (KYC) and know-your-business (KYB) requirements. Using the digital euro is free of charge for end users, while PSPs are allowed (and expected) to charge fees up to a certain cap from merchants, who are expected to be legally required to accept the digital euro [15, Rec. 16,20].

*Online version.* Users of the online version have to open a separate digital euro account (DEA) at a PSP. Different to common bank accounts, these are interest free and subject to a holding limit to ensure financial stability of the contemporary commercial bank system [10, p. 8-9]. In order to ease user experience despite this holding limit, it is possible to link a commercial bank account to the DEA for automatic defunding in case the reception of a transaction would raise the balance above the holding limit ("waterfall"), and for automatic funding in case the amount to be paid exceeds the DEA balance ("reverse waterfall") [14, p. 15,17]. The holding limit for non-business users is discussed to be around €3000 [7], while business users are not allowed to hold digital euros at all for the online version (with still unclear implications for offline usage), thereby making the linking of a commercial bank account for the waterfall a requirement [8, p. 12-13]. All online digital euro transactions are completely visible to the PSP, while the transaction data for the central settlement at the ECB is at best pseudonymized [10, p. 3]. To ensure the validity of digital euro transactions, the ECB maintains a central database of all DEA balances (**KF6**) [14, p. 18-20].

*Offline version.* The offline version [10, p. 4-6] builds on a completely separate technical basis: a digital bearer (token) that represents a certain value, issued and validated at the ECB as a central instance. Aiming to prevent digital copies of the bearer and double spending, the bearer is stored on a dedicated device (e.g., smartphone or smartcard) supported by so-called "secure hardware"—a separate piece of hardware for sensitive data protected against high-level software and hardware attacks. Those bearers are meant to be passed transitively between users without central settlement, and to not record any trace of the transactions, thereby providing full privacy for both payer and payee in offline transactions. However, Internet connectivity and identification is required for initial funding (conversion of cash or commercial bank money to digital euros) and final defunding (conversion of digital euros to cash or commercial bank money), among others to ensure the holding limit shared with the online version [14, p. 14,16]. Potential fraud such as double spending can only be detected with a delay during defunding (**KF2**), and the ECB leaves the question of liability in case of such fraud open (**KF3**).

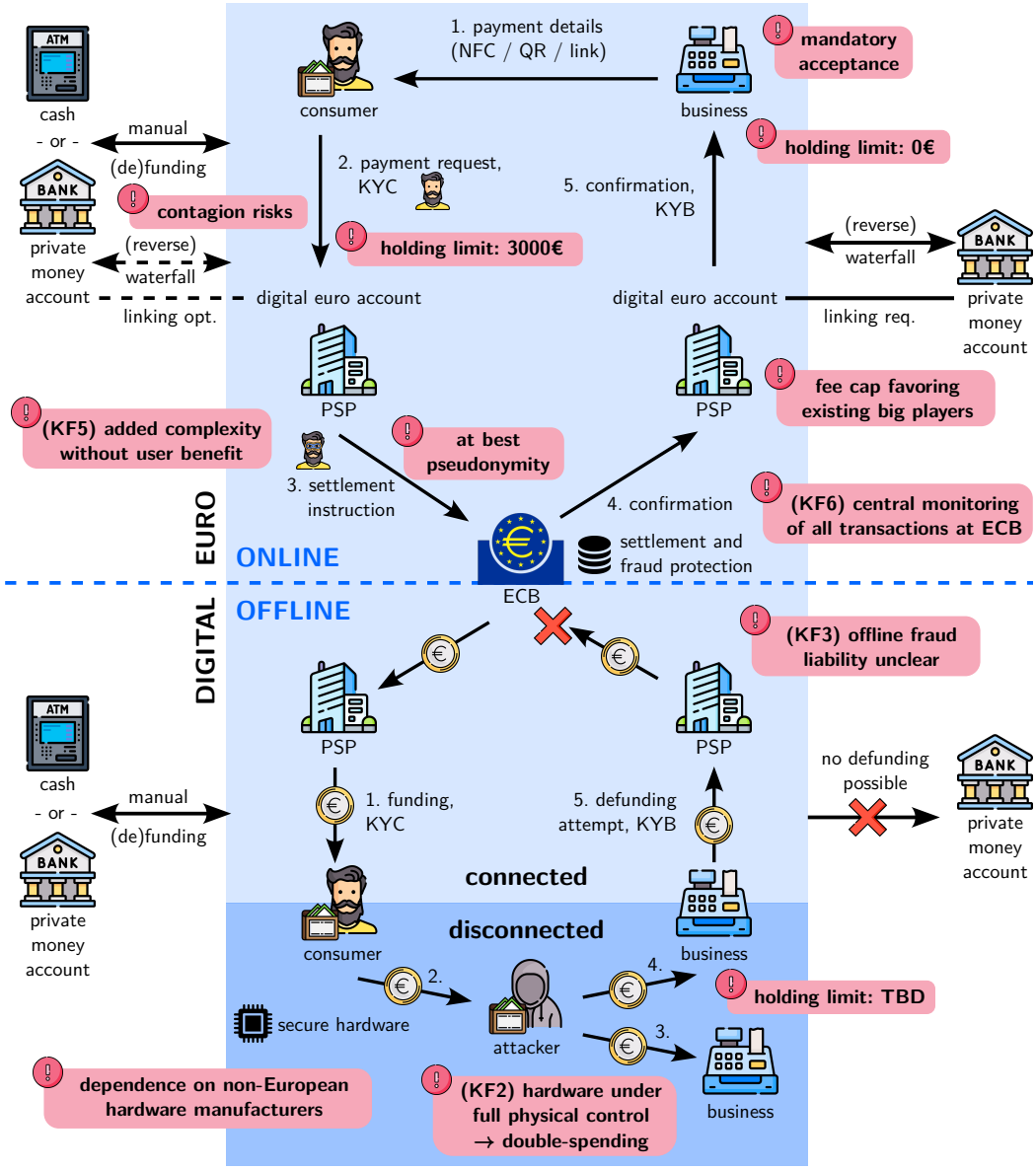


Fig. 1. **The two versions of the digital euro** with highlighted design shortcomings (cf. Section 3): The online version adds another layer of complexity to already existing payment systems, with no clear benefit for the user (**KF5**), but with centralized control and monitoring of transactions at the ECB (**KF6**). The offline version is supposed to allow for transitive and completely anonymous payments and aims to prevent forgery by the use of supposedly "secure hardware". However, it is unlikely that the wallet hardware will withstand all possible attacks given that it is under complete physical control of the wallet owner as a potential attacker (**KF2**). A successful attacker can double-spend an unlimited amount of times, as the validity of the payment bearer can only be checked as soon as the payee reconnects to the Internet. The offline version has no clear definition of liability in case of such fraud (**KF3**).

## 3 QUESTIONING THE DIGITAL EURO FAQ

The ECB's FAQ on the digital euro [9] aims to address public concerns and to provide clarity on the proposed design and implications of the digital euro. However, a deeper look reveals significant shortcomings in addressing key issues. While the FAQ attempts to justify the digital euro, its current design raises more questions than it answers, particularly regarding security, privacy, economic effects, and overall utility. The project risks being overly complex, economically burdensome, and technically flawed without clear benefits to users or society. The full detailed analysis of the FAQ is provided in Appendix A. We summarize our key findings in the following.

### 3.1 Governance and transparency: exclusionary process (KF1)

The proclaimed openess of the digital euro design finding process (**Q15**) is questionable, given that many of the core design features—such as the online-offline separation, the waterfall concept, and the reliance on "secure hardware"—have been defined before public consultations began [30]. On the contrary, the ECB has largely ignored expert advice on how to design for privacy, security, and usability [3, 21, 40, 44]. The ECB engagement with private companies (**Q16**) has excluded small and medium enterprises by setting high thresholds for potential participants, requiring, among others, a yearly average total net turnover of €100,000,000 [6, 13]. The digital euro rulebook (**Q18**) is developed behind closed doors and leaves no room for questioning fundamental digital euro design choices impacting privacy (**KF6**), security (**KF2**), and usability (**KF5**).

### 3.2 Security: ignoring obvious attack vectors (KF2)

The ECB promises "secure instant payments (...) even when you have (...) no network reception" (**Q7**), i.e., reliable offline operation without double-spending risks. This contradicts the mathematically proven CAP theorem [20], which states that no distributed system can be partition-tolerant (being disconnected), available (still work), and consistent (without double-spending) at the same time. The ECB hopes to overcome mathematics with "secure hardware", in this case meant to "protect the information stored on the device" from its owner [11], ignoring the fact that hardware security history has made it evident that consumer-grade hardware eventually cannot withstand physical attacks (cf. Figure 2). This approach to "security by obscurity" contradicts Kerckhoffs' principle—a fundamental concept in cryptography which asserts that the security of a system should not depend on the secrecy of its algorithm [28]. The security of G+D's platform, a likely candidate solution for the offline digital euro implementation [19] which proposes exactly such a system, has been ranked as "low" in a recent survey due to secrecy being the main line of defense against double-spending [1]. By proposing a "forgery check during defunding" [11], the ECB acknowledges the risk of hardware-level attacks or implementation bugs, but thereby contradicts the claim of offline payments being "safe and instant", and further puts the promised complete anonymity of offline transactions into question.

The "reverse waterfall" mechanism, the automatic digital euro funding without user intervention, poses a significant security threat as a compromised digital euro account could be used to obtain unlimited money from the linked commercial bank account. The ECB promises "state-of-the-art technologies" to counter cyberattacks on the digital euro (**Q23**). This term is doubly misleading: First, there is, to our knowledge, no other large-scale deployment of digital offline payments. Second, it does not imply the application of the most modern or secure solutions available, but rather just "what everybody else does". The central database of all (online) digital euro transaction being such a high-value target for cyberattacks (**KF6**), this is most probably not enough.

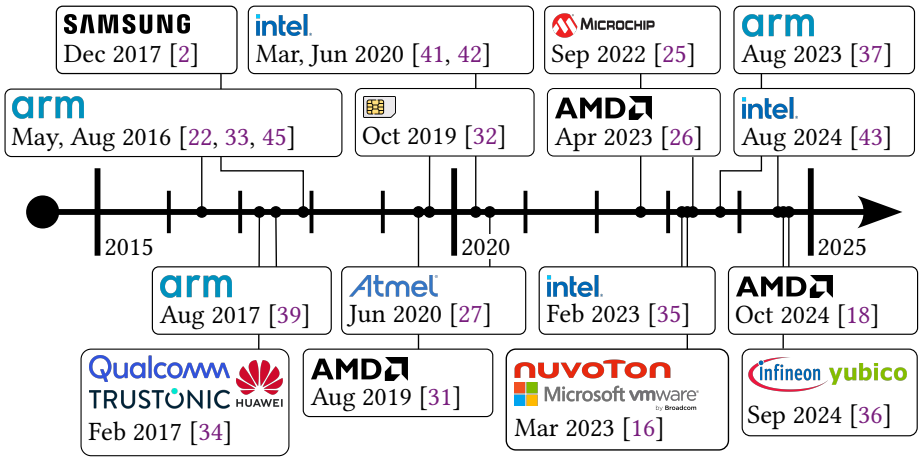


Fig. 2. Secure offline payments require securing a piece of hardware against its owner (**KF2**). History suggests this is impractical for consumer-grade hardware. Each box in the figure represents an attack that broke the security promises made by its vendor. We cannot demand people to purchase new devices anytime a "secure hardware" is dysfunctional.

### 3.3 Legal and financial: unclear liability (KF3)

The ECB has not clarified compensation mechanisms for fraud victims in offline scenarios (**Q7**). It barely states that "either the PSP, the merchant or, in some cases, the consumer would be liable", never the ECB itself [8]. It also remains unclear how the ECB will react when the double-spending protection has been overcome, enabling unlimited digital euro creation for every owner of wallets relying on the affected hardware. As this eventually poses a financial threat to the (digital) euro, the offline functionality would need to be disabled for the given type of payer's devices—which is only possible when all payee's devices become connected—until the affected hardware is replaced. Apart from not mentioning the security and financial risks connected to the offline version, the ECB also keeps quiet about the additional costs and complex logistics incurred by such hardware breaches.

Coining the digital euro as being "risk-free" (**Q1**, **Q24**) is misleading: Being backed by a central bank may make it a counterparty risk-free store of value for citizens, but the underlying payment system is still exposed to a broad range of risks, as discussed in this article. The ECB, as the responsible public operator of the digital euro, and ultimately the general public, must take these risks into consideration.

### 3.4 Economical: unclear incentives and market distortions (KF4)

While the ECB emphasizes the advantages of the digital euro for merchants (**Q5**), it fails to mention the likely substantial costs of integration into their business systems. The legally enforced roll-out throughout virtually all points of sale in the eurozone will create a high demand for qualified IT integrators, allowing them to charge a high premium over normal integration costs.

Supervised intermediaries—the PSPs—are expected to "perform all end-user services" (**Q6**). This entails operation and onboarding including costly KYC and KYB requirements, which need to be reimbursed solely by the fees charged to merchants (**Q21**), since the digital euro is promised to be "free for basic use" for consumers. The proclaimed "economic incentives similar to other digital means of payments" for PSPs (**Q6**) beg the question of where benefits for the PSPs will come from. To cope with costs, one (generally undesirable) option might be to compromise security if fraud liability stayed at the ECB—which is unclear (**KF3**). Another option for commercial banks could

be to earn interest on user-facing digital euros under their management via the ECB's deposit facility, by offering an extra euro account tightly integrated with the digital euro where users could earn interest. Since non-bank PSPs have no access to the deposit facility, this would be an unfair advantage for commercial banks.

While the ECB wishes for "innovation and competition in the digital payment markets" (**Q6**), it remains unclear how new or smaller PSPs will be able to compete with big players having a pre-existing user base. The uniformity of the service offering and the fee cap favor market oligopolization among digital euro PSPs. At the same time, a legally mandated digital euro could sideline and displace established national digital payment systems, leaving less consumer choice and eventually stiffling innovation.

### 3.5 Utility and costs: unclear benefits for society (KF5)

The ECB claims various advantages of the digital euro, including no costs for end-users, universal acceptance in physical shops and online, support for person-to-person payments, a higher level of privacy than other digital payment methods, resilience to cyberattacks and technical disruptions, technological independence contributing to Europe's strategic autonomy, and non-reliance on Internet connectivity (**Q1**, **Q2**, **Q3**). The only tangible advantage compared to cash is the ability to pay digitally and online, while a comparison of the digital euro design to existing digital payment systems only leaves the legally enforced acceptance throughout the euro area as a clear improvement for the user. Many payment systems can be used for person-to-person payments, online, and at points of sales; and are also free of charge for consumers, with merchants covering the fees. Being a central bank liability makes no effective difference to the vast majority of Europeans, given that bank deposits are generally insured up to €100,000, while digital euro holdings are expected to be limited to €3,000 [7] as well as interest-free and thereby less attractive for savings (**Q20**). The claims of improved resilience to cyberattacks lack supporting evidence in terms of concrete measures provided in public documents [8, 15]. Using the offline version in case of technical disruptions such as power outages is only possible after a manual funding process which still needs Internet connectivity. Given the convenience option of automatic funding in the online version, it seems questionable to which extent people would have offline digital euros available when their Internet goes down. While the digital euro could reduce the dependence on non-European payment providers, the offline version still depends on proprietary, predominantly non-European hardware. Embracing open standards and free software [17] instead of relying on proprietary technology would allow for easier integration with alternative European hardware and end-user devices and help to establish trust in the system (cf. Appendix C). The high risks of the offline version have been articulated for **KF2**, and the online version offers even less privacy than other digital payment systems due to the existence of a central transaction database (**KF6**).

While having little clear advantages, the digital euro project brings significant disadvantages for euro area citizens: First, with an initial project budget of €1.3 billion [23], it is far from being a "cheap (...) form of public money" (**Q17**), especially when compared to more innovative and cost-efficient digital payment systems [38], with developments costs of less than 1% of that amount (**Q25**). The high additional costs for mandatory roll-out to all merchants, support, and onboarding (**KF4**) are not even included in that number. In fact, all costs of the digital euro are eventually borne by the citizens of the euro area, whether they want to use it or not, contrary to the ECB's claim that the digital euro would be free of charge for basic use (**Q20**). Second, while the ECB and the European legislation may try to avoid it (**Q4**), bringing yet another digital payment system to the market will likely further erode the use of physical cash, which is the most power-outage-resilient, inclusive, accessible, and privacy-preserving payment system we know of.

| | Digital Payment System | | | | | Digital Euro | | |
|---|---|---|---|---|---|---|---|---|
| Feature | Credit Card | PayPal | Wero | Bitcoin | GNU Taler | Online | Offline | Cash |
| Online operation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Offline operation | (✓) | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ |
| Payer anonymity | ✗ | ✗ | ✗ | (✗) | ✓ | ✗ | ✓ | ✓ |
| Payee anonymity | ✗ | ✗ | ✗ | (✗) | ✗ | ✗ | ✓ | ✓ |
| AML compliance | ✓ | ✓ | ✓ | (✗) | ✓ | ✓ | (✗) | (✗) |
| Security[1] | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ |
| no illicit remote access | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ |
| no double-spending | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| reasonable finality | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗[2] | ✓ |
| Prior funding needed | ✗ | ✗ | ✗ | ✓ | ✓ | ✗[3] | ✓ | ✓ |
| Libre software | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ | - |

[1]security requires all three aspects [2]forgery check at deferred online defunding [3]using waterfall approach

Table 1. **Comparison of the two digital euro versions to other digital payment systems and cash.** The online version differs significantly from the offline one in terms of both privacy and security. Since the former is designed with an architecture similar to already existing third-party payment systems (**KF5**), it matches those quite closely with respect to the available features, but fails to deliver on additional possible benefits such as payer anonymity. The offline version seems to resemble cash most, but contains inherent security flaws (**KF2**) and requires Internet connectivity for a prior manual funding operation.

### 3.6 Privacy: untercutting existing systems (KF6)

The ECB compares the digital euro to cash and emphasizes privacy (**Q9**), matching clear consumer preference for payment privacy in recent surveys [4, 5, 12]. Unfortunately it fails to deliver: While the offline version indeed promises full transaction privacy with respect to the payment infrastructure, it remains unclear how an offline fraud incident (**KF2**) would be handled without any recorded transaction history (**KF3**). Given the convenience functions of the online version such as automatic deposit and withdrawal, and given that Internet is available in many situations, people are likely to stick to the online version of the digital euro, probably in the illusion that their transaction data is private there, too.

However, the online digital euro mirrors the design of typical digital payment systems (cf. Table 1) where all transactions are completely visible to the PSP, with at most organizational or legal, but no strong cryptographic safeguards against data misuse. And, even worse, the ECB will maintain a central database of all online digital euro transactions, where it, as they state, "would not be able to directly connect transactions to specific individuals" (**Q9**). Published documents solely reference pseudonymization of individuals, i.e., using unique identifiers instead of real names and personal identities for digital euro accounts. However, this still allows the creation of "patterns of life" and detailed insights into citizen's private lives, where it is enough to relate a single transaction with a certain individual to obtain their whole transaction history—indeed not "directly", but with little effort. This will enable an unprecedented level of easy mass surveillance and represent a high-value target for cyberattacks as payment data would no longer be siloed across thousands of organizations, databases, and incompatible formats [3].

Article 8 of the European Convention on Human Rights provides the basis for the understanding of privacy being a fundamental human right, which however is not absolute but subject to derogations. Any privacy-intrusive measure must pass a number of tests derived from the wording and subsequent interpretation of Article 8, as commented on in more detail in Appendix B: There needs to be a clear legal basis for the measure, which at the same time needs to establish clear safeguards for privacy and remedies for breach of privacy, and the measure must be both necessary and proportionate in a democratic society. The privacy-intrusive nature of the online version, where PSPs provision digital euro accounts to verified identities and can thus relate every single transaction to an individual, is commonly justified by the necessity of Anti-Money Laundering (AML) legislation. This oversees the fact that a payment system with KYC-compliant money inflow and income transparency through identifiable payees can serve an equally good purpose in countering criminal activities, while offering anonymity on the payer's side [21]. But even if one were to accept that the two tests of legal basis and necessity have been met by the draft regulation [15, 15], it would seem that it is the test of proportionality which the digital euro would fail. The privacy risks implied by a central database which is already discussed being in reach of intelligence services and police forces [24] are significantly disproportionate to the functionality or any other advantage gained for the citizen (**KF5**). It is unfortunately not a given that all intelligence services of all EU member states will forever be trustworthy to not misuse their access to such a huge database for nefarious purposes. Instead of "privacy by design", at this moment in time, the digital euro is promising "less privacy through flawed design".

## 4 RECOMMENDATIONS

Section 3 and in more detail Appendix A question many of the design decisions of the digital euro in response to the official FAQ by the ECB. To summarize, we give a short list of recommendations for a successful digital version of the euro or any other CBDC:

(1) **Acknowledge the impracticability of the offline version.** Instead of spending money and time on a design idea based on the unrealistic assumption of unbreakable hardware (**KF2**), the ECB should focus on the online version as a single digital euro system, and acknowledge the fact that a digital currency will never be as resilient as physical cash to extraordinary events like blackouts.
(2) **Build on existing solutions and Free/Libre Software.** Given that explicit design goals of the digital euro include user trust in the payment system, interoperability between participating payment service providers, and being a role model for CBDCs worldwide, the digital euro should be based on open designs and Free/Libre Open Source Software (FLOSS) instead of proprietary technology and security by obscurity (**KF2**).
(3) **Provide a real advantage to users.** Instead of merely adding another layer to the existing payment infrastructure under centralized ECB oversight (**KF6**), the digital euro needs to provide a compelling, unique selling point to be successful (**KF5**). One such advantage could be cash-like payer anonymity for online transactions.
(4) **Convince instead of enforce.** If the digital euro provided a real advantage, it would not be necessary to enforce its acceptance and put pressure on merchants to accept it with the associated additional costs. Thus, applicable legislative plans should be changed to make the acceptance of digital euros completely voluntary.

Overall, unless clear and uncontroversial benefits of the digital euro are established, we advise against the introduction of the digital euro as currently proposed.

## ACKNOWLEDGMENTS

This document takes inspiration from the well-known C++ FQA [29] that takes an outsider's perspective on the rosy FAQ on the C++ programming language written by the C++ core community. We thank Emmanuel Benoist, Christian Grothoff and Özgür Kesim for extensive inspiration, editing and support. We thank Jens Palsberg, Richard Stallman and Tanja Lange for constructive feedback. This work was supported by the German Federal Ministry of Education under grant ConcreteContracts. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not necessarily reflect those of any of the funding agencies.

## REFERENCES

[1] Chavanette Advisors. 2024. *Galactic Grid: Your Guide to the Complex Landscape of Retail Central Bank Digital Currency Technology Providers.* Technical Report. Chavanette Advisors.
[2] M. Dorjmyagmar, M. Kim, and H. Kim. 2017. Security analysis of Samsung Knox. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*. 550–553. doi:10.23919/ICACT.2017.7890150
[3] Antoine d'Aligny, Emmanuel Benoist, Florian Dold, Christian Grothoff, Özgür Kesim, and Martin Schanzenbach. 2022. Who comes after us? The correct mindset for designing a Central Bank Digital Currency. *SUERF Policy Note* 279 (June 2022), 1–9.
[4] European Central Bank. 2021. *Eurosystem report on the public consultation on a digital euro.* Technical Report. https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf.
[5] European Central Bank. 2022. Study on the payment attitudes of consumers in the euro area (SPACE) – 2022. https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf.
[6] European Central Bank. 2022. Tender ID: PRO-007480. per Email, https://www.ecb.europa.eu/ecb/jobsproc/proc/pdf/2022-ojs040-099799-en.pdf.
[7] European Central Bank. 2023. Financial Stability Review. https://www.ecb.europa.eu/press/financial-stability-publications/fsr/html/ecb.fsr202311~bfe9d7c565.en.html.
[8] European Central Bank. 2023. A stocktake on the digital euro - Summary report on the investigation phase and outlook on the next phase. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs231018.en.pdf.
[9] European Central Bank. 2024. FAQs on the Digital Euro. https://www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb.faq_digital_euro.en.html. Accessed: December 2, 2024.
[10] European Central Bank. 2024. 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.
[11] European Central Bank. 2024. State of play on offline digital euro—11th ERPB technical session on digital euro. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240411_item3updateofflinedigitaleuro.en.pdf.
[12] European Central Bank. 2024. Study on the payment attitudes of consumers in the euro area (SPACE) – 2024. https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.space2024~19d46f0f17.en.pdf.
[13] European Central Bank. 2024. Tender ID: PRO-009488. not public, available upon request.
[14] European Central Bank. 2024. Update on the work of the digital euro scheme's Rulebook Development Group. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240103_RDG_digital_euro_schemes_update.en.pdf.
[15] European Commission. 2023. Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369
[16] Francisco Falcon. 2023. Vulnerabilities in the TPM 2.0 reference implementation code. https://blog.quarkslab.com/vulnerabilities-in-the-tpm-20-reference-implementation-code.html.
[17] Free Software Foundation. 1996. What is Free Software? https://gnu.org/philosophy/free-sw.html.
[18] Stefan Gast, Hannes Weissteiner, Robin Leander Schröder, and Daniel Gruss. 2025. CounterSEVeillance: Performance-Counter Attacks on AMD SEV-SNP. In *Network and Distributed System Security (NDSS) Symposium 2025.* Network and Distributed System Security Symposium 2025 : NDSS 2025, NDSS 2025 ; Conference date: 23-02-2025 Through 28-02-2025.
[19] Giesecke+Devrient. 2024. New survey indicates digital euro must also work offline. https://www.gi-de.com/en/group/press/press-releases/new-survey-indicates-digital-euro-must-also-work-offline. Accessed: October 15th, 2024.
[20] Seth Gilbert and Nancy Lynch. 2002. Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services. *SIGACT News* 33, 2 (jun 2002), 51–59. doi:10.1145/564585.564601

[21] Christian Grothoff and Thomas Moser. 2021. How to issue a privacy-preserving central bank digital currency. *SUERF Policy Briefs* 114 (June 2021).
[22] R. Guanciale, H. Nemati, C. Baumann, and M. Dam. 2016. Cache Storage Channels: Alias-Driven Attacks and Verified Countermeasures. In *2016 IEEE Symposium on Security and Privacy (SP)*. 38–55. doi:10.1109/SP.2016.11
[23] Sandali Handagama. 2024. European Central Bank Shows It's Serious About Enabling Digital Euro Offline Use. https://www.coindesk.com/policy/2024/01/11/european-central-bank-shows-its-serious-about-enabling-digital-euro-offline-use/.
[24] Maximilian Henning. 2024. EU Council discusses Digital Euro: And how much privacy should it be? https://netzpolitik.org/2024/eu-council-discusses-digital-euro-and-how-much-privacy-should-it-be/. Last accessed December 2024.
[25] Olivier Hériveaux. 2022. Triple Exploit Chain with Laser Fault Injection on a Secure Element. In *2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*. 9–17. doi:10.1109/FDTC57191.2022.00011
[26] Hans Niklas Jacob, Christian Werling, Robert Buhren, and Jean-Pierre Seifert. 2023. faulTPM: Exposing AMD fTPMs' Deepest Secrets. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 1128–1142.
[27] Jan Jancar, Vladimir Sedlacek, Petr Svenda, and Marek Sys. 2020. Minerva: The curse of ECDSA nonces (Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces). *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020, 4 (2020), 281–308. doi:10.13154/tches.v2020.i4.281-308
[28] Auguste Kerckhoffs. 1883. La cryptographie militaire. *Journal des sciences militaires* IX (January, February 1883), 5–38, 161–191.
[29] Yossi Kreinin. 2009. C++ FQA Lite. https://yosefk.com/c++fqa/.
[30] Christine Lagarde and Fabio Panetta. 2020. *Report on a digital euro.* Technical Report. European Central Bank.
[31] Mengyuan Li, Yinqian Zhang, Zhiqiang Lin, and Yan Solihin. 2019. Exploiting Unprotected I/O Operations in AMD's Secure Encrypted Virtualization. In *USENIX Security Symposium*.
[32] Adaptive Mobile Security Limited. 2019. Simjacker Technical Report. https://www.enea.com/info/simjacker/.
[33] Moritz Lipp, Daniel Gruss, Raphael Spreitzer, Clémentine Maurice, and Stefan Mangard. 2016. ARMageddon: Cache Attacks on Mobile Devices. In *Proceedings of the 25th USENIX Conference on Security Symposium* (Austin, TX, USA) *(SEC'16)*. USENIX Association, USA, 549–564.
[34] Aravind Machiry, Eric Gustafson, Chad Spensky, Christopher Salls, Nick Stephens, Ruoyu Wang, Antonio Bianchi, Yung Ryn Choe, Christopher Kruegel, and Giovanni Vigna. 2017. BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments.. In *NDSS*.
[35] Joseph Nuzman. 2023. CVE-2022-38090: Improper isolation of shared resources in some Intel(R) Processors when using Intel(R) Software Guard Extensions may allow a privileged user to potentially enable information disclosure via local access. https://www.cve.org/CVERecord?id=CVE-2022-38090.
[36] Thomas Roche. 2024. EUCLEAK: Side-Channel Attack on the YubiKey 5 Series—Revealing and Breaking Infineon ECDSA Implementation on the Way. https://ninjalab.io/eucleak/.
[37] Xhani Marvin Saß, Richard Mitev, and Ahmad-Reza Sadeghi. 2023. Oops..! I Glitched It Again! How to Multi-Glitch the Glitching-Protections on ARM TrustZone-M. In *32nd USENIX Security Symposium (USENIX Security 23)*. 6239–6256.
[38] Taler Systems SA. 2024. GNU Taler. https://taler-systems.com/.
[39] Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo. 2017. CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management. In *Proceedings of the 26th USENIX Conference on Security Symposium* (Vancouver, BC, Canada) *(SEC'17)*. USENIX Association, USA, 1057–1074.
[40] Harald Uhlig, Mike Alonso, and Jon Frost. 2023. Privacy in Digital Payments—Escaping the Panopticon. *Georgetown Journal of International Affairs* 24, 2 (2023), 174–180.
[41] Jo Van Bulck, Daniel Moghimi, Michael Schwarz, Moritz Lipp, Marina Minkin, Daniel Genkin, Yarom Yuval, Berk Sunar, Daniel Gruss, and Frank Piessens. 2020. LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection. In *41th IEEE Symposium on Security and Privacy (S&P'20)*.
[42] Stephan van Schaik, Andrew Kwong, Daniel Genkin, and Yuval Yarom. 2020. SGAxe: How SGX Fails in Practice. https://sgaxeattack.com/.
[43] Luca Wilke, Florian Sieck, and Thomas Eisenbarth. 2024. TDXdown: Single-Stepping and Instruction Counting Attacks against Intel TDX. In *ACM CCS 2024*.
[44] Karl Wüst, Kari Kostiainen, Noah Delius, and Srdjan Capkun. 2022. Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy-Preserving Regulation. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 2947–2960. doi:10.1145/3548606.3560617
[45] Ning Zhang, Kun Sun, Deborah Shands, Wenjing Lou, and Y Thomas Hou. 2016. TruSpy: Cache Side-Channel Information Leakage from the Secure World on ARM Devices. *IACR Cryptol. ePrint Arch.* 2016 (2016), 980.

Received 10 January 2025; revised -; accepted -