weizenbaum
institut

// Consultancy on a Digital Euro

Statement of Weizenbaum Research Group "Trust in Distributed Environments"

October 30th, 2020

We, the Weizenbaum research group Trust in Distributed Environments, greatly appreciate the opportunity to participate in the European Central Bank's public consultation on the design of a digital euro.

In the following, we publish our answers to the consultation questionnaire. We focus on questions within our interdisciplinary area of expertise. In this document, we leave out all questions that we did not answer, as well the "About the respondent" section of the questionnaire.

Do you envisage any challenges associated with a digital euro that would prevent you or others from using it? If so, what are they?

As a payment network, the introduction of a digital euro can be seen from the perspective of a two-sided market. Adoption of users and shops need to occur simultaneously in order to incentivize each other to join the network. High setup costs and lack of incentives for shops and stores might lead to similar adoption issues then those known from the electronic functions of the German ID card.

Additionally, we see challenges related to a potential lack of trust:

- Potential users could mistrust the privacy guarantees offered by a digital euro. For example, users could have the mental model of a faraway ECB monitoring each of their transactions.
- Potential users could mistrust the reliability of the technical system and its resilience in the face of crises or catastrophic events.
- Potential users could mistrust the fungibility of the digital euro, fearing for example that their funds could be frozen more easily (also for political reasons) if they are managed directly by the central bank.

Each of these fears should be unjustified in the final digital euro system, for example due to an appropriate technical design as well as strong oversight and auditing processes.

However, negative mental models might still prevail or be encouraged by media campaigns. To promote long-lasting trust, the design of the digital euro should be transparent, avoid complexity and be reviewed and approved by renowned independent institutions, such as academic institutions. To ensure that education campaigns about the qualities and benefits of the digital euro strike fertile ground, the general technical literacy of EU citizens should be furthered.

There are two approaches we can take to make a digital euro work, one that requires intermediaries to process the payment and one that doesn't. […] From your perspective, which of the following do you find most appealing? (select one):

Potential replies:

a) *a digital euro focused on privacy and the protection of personal data, which can be used offline;*
b) *a digital euro with broader potential for additional services, allowing innovative features and other benefits for citizens and businesses;*
c) *a combination of both.*

Choice and comments:

We favor option a). We do not see the necessity to focus explicitly on innovative features for digital cash. Such are in development already for other means of digital payment. Automation, conditional withdrawals and other smart features can well be built around the medium-of-exchange but do not necessarily need to be part of its own design. We see this happening in many shades already for credit money (f.e. in the services of Paypal or the cooperation of Stripe and Calendly).

The features of today's cash, on the other hand, are harder to replicate by the private sector. A lack of focus on privacy might leave the niche of digital, anonymous payments to cryptocurrency projects like Monero or Zcash. A cash-like digital euro with will improve the choice-set for citizens by offering a payment method that is private but also trusted, digital and accepted by merchants.

A digital euro may allow banks and other entities to offer additional services, on top of simple payments, which could benefit citizens and businesses. What services, functionalities or use cases do you think are feasible and should be considered when developing a digital euro?

While feature-rich currency proposals are tempting, we would vote for a simple design. Richness in features might lead to complexity which in turn increases the probability of undetected weaknesses. The main feature of a medium-of-exchange offered by the ECB is to be trustworthy which requires safety, robustness and predictability in operation.

Which solutions are best suited to avoiding counterfeiting and technical mistakes, including by possible intermediaries, to ensure that the amount of digital euro held by users in their digital wallets matches the amount that has been issued by the central bank?

Cryptographically secured ledgers, as popularized in the context of blockchain systems, enable the implementation of a global transaction log that can be easily audited. Privacy requirements, as well as the ECB's stated desire to retain control of the digital euro system, suggest that the full transaction log (and resulting account system) should be visible and extendable only through the ECB itself. In order to promote trust in the system, mechanisms for end-users to (cryptographically) verify the correct maintenance of the ledger and their accounts could be implemented.

While a plethora of technical solutions from academia and practice are plausibly relevant in the context of this question, a thorough technical investigation based on specific requirements and priorities must be conducted in order to arrive at specific technology recommendations.

What technical solutions (back-end infrastructure and/or at device level) could best facilitate cash-like features (e.g. privacy, offline use and usability for vulnerable groups)?

Secure offline payments can plausibly be realized only using trusted hardware devices, such as smart cards or devices resembling cryptocurrency hardware wallets. "Double spend" frauds involving a malicious payer using a compromised payment device are generally undetectable by a payment recipient that is offline.

Different technological solutions exist that could enable anonymous offline payments between trusted devices - see for example the literature on anonymous digital credentials. It is completely within the state of the art to ensure that the privacy of transaction partners is preserved even if a participating device is compromised. On a side note, digital euro wallets could also be equipped with credential- and identity-attestation functions, enabling even more innovative applications.

For realizing a back-end ledger data structure with cash-like privacy guarantees, cryptographic solutions from the cryptocurrency world might be investigated, such as ring signatures (used, e.g., in the cryptocurrency Monero) or non-interactive zero-knowledge proofs. Similarly to state of the art technologies for the offline case, these approaches maintain privacy guarantees even in the face of strong adversaries with full access to the ledger data structure.

What should be done to ensure an appropriate degree of privacy and protection of personal data in the use of a digital euro, taking into account anti-money laundering requirements, and combating the financing of terrorism and tax evasion?

Extreme care must be taken to ensure that the digital euro cannot be branded as surveillance infrastructure, or as potential surveillance infrastructure conditional on changes in the political climate. This is especially relevant considering the larger centralization of citizens' financial data implied by an ECB-managed digital euro ledger. Surveillance fears are also highly relevant when extrapolating that the digital euro might become a standard payment system in the euro area, implying a strong economic pressure for individual citizens to use it.

To sustainably preserve core liberties and promote trust in the privacy offered by the digital euro system, it might be insufficient to rely only on organizational protection measures and safeguards. As stated in a previous answer, a variety of technological solutions such as anonymous credentials and ring signature-based ledger data structures exist that provide very strong privacy guarantees in digital currency settings. However, strong privacy guarantees also impede criminal investigations and the regulation of financial flows. There is some hope that this tension can be eased through advances in the state of the art. Current academic projects that explore the space between complete anonymity and complete institutional trust in the context of digital currencies include PRCash and Collaborative Deanonymization. To the best of our knowledge, current investigations in this space are still at an early stage and not necessarily conducted with the specific requirements of a digital euro in mind. An intensification of investigations might yield new solutions that preserve the goals of current AML/CFT regulation while reducing privacy threats.

The central bank could use several instruments to manage the quantity of digital euro in circulation (such as quantity limits or tiered remuneration), ensuring that the transmission of monetary policy would not be affected by shifts of large amounts of commercial bank money to holdings of digital euro. What is your assessment of these and other alternatives from an economic perspective?

Limiting the risk of high-powered central bank money flowing out of the system into digital cash wallets might be first priority to avoid a destabilization of the financial system. Quantity limits, in this context, seem like the stronger and thus preferable way to mitigate the above risk. While monetary punishment for holding large amounts of digital cash might be a potential solution as well, this might be politically more difficult. Nowadays, holding large balances of non-digital cash naturally holds increased cost-of-storage. This is hard to replicate for digital cash.

Furthermore, depending on the exact implementation, tiered remuneration might be perceived as "helicopter money" by citizens and threaten their trust in the currency's value. A remedy might be measures to credibly communicate the ECB's primary goal of providing stable currency also in this new context.

If a digital euro were subject to holding balance limits, what would be the best way to allow incoming payments above that limit to be shifted automatically into the user's private money account (for example, a commercial bank account) without affecting the ease of making and receiving payments?

An automatic shifting of payments to a user's private money account might undermine privacy expectations on part of the payer and should therefore be avoided. For improving the ease of receiving payments, users could be notified once their holding balance limits are close to being reached. Additionally, open programming interfaces to digital euro holdings should be offered so that users (or organizations working on their behalf) can implement their own systems and rules for the automatic shifting of funds.

Should the use of the digital euro outside the euro area be limited and, if so, how?

Keeping to the "digital cash" metaphor, it is unclear why the use of the digital euro outside the euro area should be limited. Moreover, such a limit will likely harm only ordinary citizens, as given cash-like privacy features (which we consider highly desirable) a black market for digital euro wallets and accounts will likely emerge quickly. Opening up the digital euro to users outside of the euro area is arguably also more in tune with European values, demonstrating a culture of openness and welcoming, and would underline the EU's ambition to be an important pillar to the global economic system.

Which software and hardware solutions (e.g. mobile phones, computers, smartcards, wearables) could be adapted for a digital euro?

As stated in a previous answer, purely software-based solutions (i.e., not leveraging trusted hardware) will be insufficient to enable the offline payments use-case.

An integration into current consumer electronic devices with trusted enclaves or similar technology is problematic due to the large complexity of these systems, which leads to a significantly larger potential for accidental bugs and vulnerabilities. This concern is exaggerated by the fact that security is rarely a top requirement in current consumer electronics. Also, the globe-spanning manufacturing chains of modern consumer devices imply extensive possibilities for targeted attacks, for example the covert insertion of backdoors. The digital euro system must be able to monitor current security advisories for all supported wallet devices, provide support and retain the possibility to remotely disable wallets on compromised hardware models.

For gaining the trust of more cautious users, the offering of at least one single-purpose digital euro wallet device, ideally of predominantly European design and manufacturing, appears prudent.

What role can you or your organisation play in facilitating the appropriate design and uptake of a digital euro as an effective means of payment?

The Weizenbaum Institute for Networked Society is the German Internet Institute, a place of excellent research on the transformation and design processes of digital change. In the spirit of Joseph Weizenbaum, we research the necessary framework conditions, means and processes for individual and social self-determination in a networked society. We understand self-determination as a design principle that is central to the preservation of human dignity and democracy.

As an independent, publicly financed, basic research-oriented, interdisciplinary research institute, we will accompany the digital euro discussion and design process focusing on the merits and implications of core technical decisions. Once the design of the digital euro and its embedding in existing social, economic and legal contexts becomes more clear, we will likely also investigate the impact of the digital euro on these systems, mapping challenges and opportunities for consumers and European society.