EUROPEAN CENTRAL BANK

EUROSYSTEM

Appendix

The Eurosystem's analysis of privacy-enhancing techniques in central bank digital currencies

The Eurosystem had already started to explore privacy-enhancing techniques (PETs) in central bank digital currencies before preliminary work on a digital euro began.

In 2019 Eurosystem experts developed a proof of concept (PoC) for enhancing privacy in a central bank digital currency payment system.[1] The PoC showed that it is possible to monitor for illicit activities while still allowing users to make a small number of low-risk, low-value payments with limited sharing of information. In the use case analysed, any user's intermediary would only know that a payment of a small amount has been made or received, but without knowing the identity of the counterparty involved in the transaction. It would therefore be impossible for any intermediary to know the purpose of a low-value payment made or received.

The PoC set a maximum overall amount of private small payments each user can make in a given time period. This would be established in line with the regulatory framework to stop large payments being split into several small payments to circumvent the regulation. The solution was based on assigning a number of time-limited "digital vouchers" to each user, who could use them to privately transfer central bank digital currency. The impossibility of tracking past payment activity would preserve the privacy of users.

In 2020 experts from the ECB and the Bank of Japan analysed a broad range of PETs aimed at balancing the confidentiality and auditability of payments in a distributed ledger environment.[2] The project identified a number of PETs that can be used alone or in combination, such as (i) segregating information on payments made and received by individual users; (ii) sharing such information in hidden form through cryptographic techniques that make transaction details uninterpretable; and (iii) creating "noise" in the data exchanged by users and intermediaries so that it would be difficult or even computationally unfeasible to link information on the transaction to information on the participants.

1 ECB (2019), "Exploring anonymity in central bank digital currencies", *In Focus*, No 4, December.
2 ECB and Bank of Japan (2020), "Balancing confidentiality and auditability in a distributed ledger environment", *Project Stella*, February.

European Central Bank
Directorate General Communications, Global Media Relations Division
Sonnemannstrasse 20, 60314 Frankfurt am Main, Germany
Tel.: +49 69 1344 7455, email: media@ecb.europa.eu, website: www.ecb.europa.eu

The experience gained from these projects will help us respond to the demand for privacy that was expressed in our public consultation on a digital euro.

The issue of privacy is being further explored as part of the experimental work on a digital euro.[3]

One work stream is examining options for minimising the amount of personal information stored in the ledger of a centralised infrastructure. This includes the possibility of segregating data to prevent participants from knowing what transactions are taking place between any pair of users.[4] Such information could be aggregated on a "need to know" basis only for the purpose of detecting illicit activities and at the request of the competent authorities. We are also experimenting with the use of one-off cryptographic public keys and end-to-end encryption to ensure that payment operators are unable to infer private information by looking at transaction data.

In another experiment, we are assessing the effectiveness of tools aimed at unlinking the identities of users from their transactions in a decentralised ledger. We are also testing the implications of off-ledger payment channel networks in which the payment details would be known only to the payer and the payee, and hidden from any other third party (including the central bank). Furthermore, we are testing how to shape different elements of a blockchain prototype (e.g. ledger, wallets, identity service) to allow for different levels of privacy.

In addition, we are looking at possibilities for local storage, in collaboration with developers of bearer payment instruments that could be used in offline transactions. Testing the reliability of trusted elements used in hardware devices plays a crucial role in this work stream, since privacy cannot come at the expense of security. The possibility of paying using a bearer instrument (where the payer and the payee would be responsible for verifying any transfer of value between them without the involvement of third parties) would make bearer solutions very similar to cash, which is distributed by intermediaries and then transacted between users in line with their sole responsibilities.

For each work stream, privacy is analysed taking into account anti-money laundering requirements. If a digital euro project is launched, we will carry out further work, which will have to strike the right balance between privacy, security, efficiency and compliance with applicable regulations.

---

[3] The work streams established for the preliminary phase of the digital euro project are described in Panetta, F. (2020), "From the payments revolution to the reinvention of money", speech at the Deutsche Bundesbank conference on the "Future of Payments in Europe", Frankfurt am Main, 27 November.

[4] For example, data can be segregated in a such a way that allows the operator of the infrastructure to record private transactions between cryptographic public keys of the users without knowing their identities, while the intermediary of the payer and the payee would only be aware of the link between its customers' identities and the public keys.