Foundational design options for a digital euro

Euro Retail Payments Board technical session on digital euro

4 May 2022
Digital euro project timeline

Project team on-boarding
Governance set-up

July 2021
Governing Council decision to launch investigation phase

Q4-2021
Q1-2022
Q2-2022
Q3-2022
Q4-2022
Q1-2023
Q2-2023
Q3-2023

Use case prioritisation
Report on focus groups with citizens and merchants

Design options to moderate take-up
Distribution model

Compensation model
Access to ecosystem
Value added services
Advanced functionalities

Prototyping results

Selection of service provider(s) for possible project realization phase

Decision making document including advice on potential issuance digital euro, its design and implementation plan

July 2021
Governing Council decision to launch investigation phase

Project team on-boarding
Governance set-up

Q4-2021
Q1-2022
Q2-2022
Q3-2022
Q4-2022
Q1-2023
Q2-2023
Q3-2023

On-line/off-line availability
Data privacy level
Transfer mechanism

Settlement model
Amount in circulation
Role of intermediaries
Integration and form factor
Prototype development

User requirements
Preparation for possible project realisation phase decision making

September 2023
Governing Council decision to possibly launch realisation phase

Tentative - timing subject to change
Objective of today’s exchange

Present Eurosystem’s analysis of foundational design options for a digital euro

Invite your feedback on design options identified by Eurosystem (followed by written procedure) as input for Eurosystem preparations of final decisions on these options by Governing Council in autumn 2022
Foundational design options for a digital euro
Foundational design options for a digital euro

1. Transfer mechanism to settle transactions
   - **Third party** would determine, on behalf of the payer and payee, whether a transaction is valid
   - **Peer-to-peer** where the payer and the payee would be responsible for verifying any transfer of value between them

2. Connectivity
   - **Online payment**: the settlement of which requires that either the payer or the payee (or both) connect to a network
   - **Offline payment**: that is settled with no need for network connectivity.

3. Privacy options enabled by the data elements transferred among actors in digital euro payments

4. Tools to avoid the excessive use of the digital euro as a form of investment

<table>
<thead>
<tr>
<th></th>
<th>Offline</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party validated</td>
<td>Impossible by design</td>
<td>Option 2</td>
</tr>
<tr>
<td>Peer-to-peer validated</td>
<td>Option 1</td>
<td>Option 3</td>
</tr>
</tbody>
</table>

Levels of privacy compatible with legislation

Set of tools for remuneration- and quantity-based limits
Core elements of the three options

**OPTION 1**
With peer-to-peer validation of offline transaction

- Peer-to-peer validation of offline transactions via secure hardware devices
- Privacy of low-value proximity payments within limits set by legislation

**OPTION 2**
Available online and validated by a third-party

- Third-party validation of online transactions
- Transparency of transaction data to intermediaries for AML/CTF purposes

**OPTION 3**
With peer-to-peer validation of online payments

- Peer-to-peer validation of online transactions via secure devices
- Allows remote payments but transactions cannot be checked ex-ante

*Its technical feasibility and associated legislative framework need to be further assessed*

*Solutions to increase its resilience to connectivity outages need to be further investigated*

*Experimental solutions, unlikely to be ready for the first release. Thus, not further analysed in this phase*
Outstanding questions in the programme on the options

How to ensure that the offline option is sufficiently secure? Within which timeframe is developing such an offline solution feasible?

What tools, taken individually and/or collectively, would be effective to avoid the excessive use of a digital euro as a form of investment under different circumstances? Which ones should instead be discarded?

What leeway is available to improve users' privacy under the current legislation? How could payments that can only take place in proximity [like cash] fit within it?
Feasibility & preliminary conclusions
Criteria to evaluate the three foundational options

**Desirability criteria**
- Coverage of high-priority use cases
- End-user value perception / focus group
- Policy considerations
- Possibility to enable design features (privacy, remuneration tools and quantitative limits)
- Implications for future design decisions
- Dependencies on external stakeholders

**Feasibility criteria**
- Technical considerations
- Legal feasibility
A digital euro available online and validated by a third-party is desirable and appears to be the most feasible option in the near future: it covers the broadest set of high-level use cases, appears able to support Eurosystem policy objectives, leaves room for flexibility in other design decisions related to the digital euro, and its launch would have relatively little dependency on external stakeholders.

A digital euro with peer-to-peer validation of offline transactions could be pursued as part of the first digital euro release because of its policy relevance, but it has strong dependencies on the technological innovation, regulatory framework and the readiness of secure elements to support a digital euro solution.

Eurosystem will monitor market developments on peer-to-peer validated online payments. This option shall not be considered for the first release of the digital euro due to technical and legal challenges. The Eurosystem will assess the possibility of its development at a later stage.
Options for privacy
Privacy is a **fundamental right** and a certain baseline option for a digital euro is mandated by legislation.

Digital euro **public consultation** highlighted **privacy as a key concern of future users**.

**Focus group research** on new digital payment methods & digital euro showed more nuanced views around privacy in payments.
Full anonymity of users is not a desirable feature – it would otherwise be impossible to control amount in circulation and avoid money laundering.

**Eurosystem shall only be able to see the minimum amount of necessary transaction data** – ranging from no data at all to the strict minimum necessary for validation of digital euro payments if it decides to perform such function.

Anonymised and/or aggregated data on the use of the digital euro should be available to the Eurosystem under any privacy option – for statistical, research, supervisory and oversight purposes.

**Supervised intermediaries shall be responsible for customer onboarding and AML/CFT checks** – building on existing customer relations to be retained.

**Key role of European co-legislators** – decision on privacy options.
Privacy options (from user perspective)

- **Anonymity**
  - Identity of users is unknown when they access services; no KYC during onboarding.

- **Non-transparent to third party**
  - KYC during onboarding; holdings/balances and transaction amounts are not known to intermediary and central bank.

- **Transparency to intermediary**
  - KYC during onboarding; transaction data and users’ profiling data transparent to intermediary for AML/CFT purposes.

- **Selective privacy**
  - KYC during onboarding; higher degree of privacy for low-value transactions; large-value transactions are subject to standard CDD checks.

- **Fully transparent to central bank**
  - KYC during onboarding; all transaction data and users’ profiling data fully transparent to central bank.

---

**Preliminary view:** not to be pursued, only minimum info.

**Preliminary view:** beyond the baseline, technical and legal dependencies to be investigated.

**Preliminary view:** beyond the baseline, dependencies with legislation to be investigated.

Currently applicable baseline scenario.
Exploring options beyond the baseline scenario

**Online**
- Customer checks during onboarding
- Higher degree of privacy for low-value / low risk transactions
- Implies simplified checks (e.g. specific wallet with lower requirements during onboarding)

**Offline**
- Customer checks during onboarding
- Fully private offline transactions and holdings, no transparency to intermediary or central bank
- Only for proximity payments of lower value

Higher-value transactions would remain subject to standard controls
Options for tools to avoid excessive use as a form of investment
Excessive use to be avoided by design

• The digital euro will be designed so as to avoid potential undesirable consequences of its issuance. Limiting any adverse effects on:
  • monetary policy
  • financial stability
  • provision of services by the financial industry

• That does not imply the status quo should be maintained, but that any potential risks should be mitigated in both normal times and financial stress
Ongoing work on the impact of digital euro issuance

- The analysis has been focusing on many dimensions, for example:
  - Liquidity risk
  - Impact on different banking business models
  - Balance sheet adjustments
  - Collateral availability
  - Central bank liquidity provision
  - Policy scenarios
  - Impact on usability and attractiveness
  - Impact on provision of services
Remuneration- and quantity-based tools

- Tools merit **further analysis** in view of **limiting the use of digital euro as a form of investment** while supporting its payment function.

- Current agreement is to deploy the **widest set of effective tools**.

- Aiming at simplicity, in terms of technical implementation and understanding from the public, to **avoid negative user experience/public perception**.

- Decision on parametrisation of tools will be taken **only close to possible introduction** of digital euro.
Way forward and discussion
Further investigation on the possibility for greater privacy of low-risk low-value digital euro transactions and offline functionality

Consultation of Eurosysten committees

Outreach to external stakeholders on the identified design options

Confirmation of Eurosysten views on first set of design options in summer 2022 based on the outcome of Eurosysten committees’ consultation, discussions with external stakeholders and additional internal analysis

Review of combined design decisions (“Bringing it all together”) in Q2 2023 and feedback by stakeholders on overall design prior to Governing Council decision making in autumn 2023
For feedback

We invite reflections on all aspects of the analysis, including the following questions:

- What are your views on the three foundational design options for a digital euro (i.e. offline peer-to-peer validated, online third-party validated, online peer-to-peer validated)?

- What are you views on privacy options for digital euro payments?
  - How do you assess greater privacy for low-risk low-value digital euro transactions and offline functionality?
  - How do you assess the role of intermediaries in the processing of users' transaction data?

- What are you views on tools to avoid excessive use of digital euro as a form of investment?
  - How do you assess the impact of remuneration and holding limits on the usability of a digital euro?
THANK YOU!