EUROPEAN CENTRAL BANK

EUROSYSTEM

Summary of collected inputs from MAG members

Three foundational design options for a digital euro

06/07/2022

Digital euro project team

Disclaimer

The following presentation summarises findings of the answers made individually or jointly by some digital euro MAG members; these findings need not necessarily reflect design decisions for the digital euro

1. 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)?

MAG members supported the analysis done on the foundational design options for the digital euro and endorsed the orientation taken by the HLTF-CBDC.

Particularly, MAG members noted:

Option 1. Recognised as close complement to cash, addressing specific needs and use cases, especially the low-value proximity payments. Members noted that highest privacy for the users could be enabled by this option.

Option 2. Strongly endorsed, as:

- Similar digital payment solutions are already familiar to the consumers and merchants
- Possibility for the intermediaries to offer value added services

Option 3. Members acknowledged the significant risks associated with this option, noting also that the unfamiliarity to the consumers and merchants would hinder the adoption.

2. 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?

MAG members supported Eurosytem considerations on privacy options for digital euro payments.

In particular, MAG members:

- Supported that **full anonymity is not feasible;**
- Agreed with **focusing on currently applicable baseline scenario** (transaction data transparent to intermediary) as being capable of providing the best balance and an effective division of responsibilities, while minimising the Eurosystem involvement into the processing of users' data;
- Supported the **exploration of options beyond the baseline** that would allow higher degree of privacy for relatively low-value/low-risk payments.

MAG members agreed on the importance to differentiate between

- **data** that would be required (from technical and legal perspectives) **to perform the payments**, and
- (extended) data, on the basis of **specific opt-in** granted by the users, **to provide value added services.**

3. 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?

- The MAG members supported that the toolkit to avoid an excessive use of digital euro should include **holding limit** at user's level. To avoid additional payment friction, linking a digital euro wallet to the user's current account would allow amounts of digital euro in excess to be automatically transferred to that account in commercial bank money.
- From the perspective of user experience, consumers are accustomed to the limits to holding or maximum spending for a given period, to which most retail payment instruments are subject. Furthermore, there are no technical issues in implementing such limits. Ensuring that a user cannot have many digital euro wallet/account would reduce the complexity significantly.
- Regarding **tiered remuneration** the opinions of the MAG members were more nuanced. Members tend to agree that a tiered remuneration system does not protect against outflows of bank deposits in times of increased uncertainty/crisis.
- Whatever tool the Eurosystem is considering, it is important that its i**mplementation is easy and understandable** for end users. Introducing holding limits appears to be an appropriate solution. Tools and related policies must ensure independence from political pressure and robustness across economic cycles.

Thank you!

Annex

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

	Offline	Online
Third-party validated	Impossible by design	**Option 2**
Peer-to-peer validated	**Option 1**	**Option 3**

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

Closer to cash

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

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

Closer to digital age

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

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

Experimental

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