EUROPEAN CENTRAL BANK
EUROSYSTEM

Market Research Outcome Report

Background and participation

As part of the digital euro project investigation phase, the Eurosystem has conducted a market research exercise[1] to inform the ongoing investigative work on the design of a possible digital euro and to show a possible way forward should it be decided to continue the project in autumn 2023. On 6 February 2023 the Eurosystem published a supplementary document[2] providing answers to participants' questions to facilitate a good reciprocal understanding of concepts in the final submissions.

A digital euro[3] would allow end users of retail payment instruments to access and transfer central bank money in electronic form. Every digital euro will always be a central bank liability, enabling end users to make and receive payments throughout the euro area in a similar way to what they are used to doing with cash. Digital money issued by the central bank would provide a monetary anchor of stability for the euro area, strengthening its monetary sovereignty and fostering innovation, competition and efficiency in the European payments landscape.

The aim of the market research exercise was to obtain feedback from relevant interested parties and to gain non-binding information on potential technical solutions for a digital euro. The feedback received has helped the Eurosystem to better understand the current level of knowledge in the market and the existing experience in building solutions and identifying suitable technologies to potentially implement a digital euro. Participation in this market research exercise was entirely voluntary and has no impact on eligibility for future procurement procedures related to a digital euro or any other procurement. Nor does it imply pre-selection for a potential subsequent tender.

The market research covered 12 different components[4] that may be needed to support a digital euro, addressing ways to deal with their development, maintenance and operation. These components would enable the issuance and redemption of digital euro, the initiation, processing and settlement of transactions, the management and protection of user access and user data, and all necessary interfaces between digital euro components and with digital euro users. Each component could be developed and operated either by market actors or in-house by one or more Eurosystem central banks.

---

1 Market research on possible technical solutions for a digital euro took place between 13 January and 17 February 2023.

2 See "Digital euro market research – Answers to questions received.", ECB, February 2023.

3 The digital euro glossary provides a resource for terms and definitions that apply to a digital euro environment.

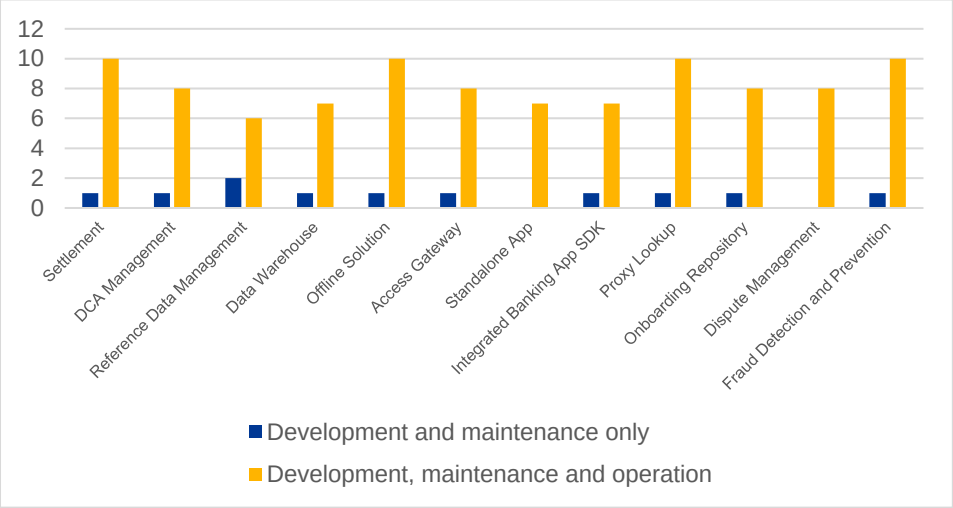
4 Components included in the market research: Settlement, Dedicated Cash Account (DCA) Management, Reference Data Management, Data Warehouse, Offline Solution, Access Gateway, Standalone App, Integrated Banking App Software Development Kit (SDK), Proxy Lookup, Onboarding Repository, Dispute Management, and Fraud Detection and Prevention.

The market research also added to the Eurosystem's understanding of the options for a digital euro technical architecture.

Overall, 29 responses were received. Figure 1 provides an overview of the number of responses received per component. Respondents selected the components to which their feedback applies and specified whether their submission covered development, maintenance and operation or development and maintenance only[5].

Chart 1

Overview of number of responses received per component



The Eurosystem reviewed all proposed approaches for individual components and, where further clarity was needed, followed up bilaterally with selected respondents to clarify open questions and better understand the feedback received.

It should be noted that since the information was collected through an open consultation, the responses do not constitute a representative sample in any statistical sense. This report summarises the responses using various descriptive metrics but does not intend to imply that any of the solutions presented by the respondents are necessarily optimal or best-fit solutions for a digital euro.

Main lessons from the market research exercise

The Eurosystem wishes to thank all respondents and express its appreciation for their valuable input on the possible technical solutions for a digital euro and remains committed to taking into account the views of market participants in the potential development of a digital euro.

Through an analysis of the responses, the Eurosystem has been able to broaden its understanding of the wide range of approaches and potential technical solutions to

[5] "Development and maintenance only" covers the first five years of maintenance, after which this is viewed as an operational task.

the challenges of developing a digital euro successfully should the ECB Governing Council decide to continue the work on the project.

The Eurosystem is reassured that there is a sufficient pool of European providers able to tackle the challenge of developing digital euro solutions. Apart from questions on the functional solutions for a digital euro, the market research exercise has also been informative in terms of non-functional aspects and questions related to intellectual property and contractual arrangements for developing or operating the different components of a potential digital euro solution.

At a **cross-component** level, the results of the market research revealed that most functional and non-functional requirements can be addressed in multiple ways. The technical designs of the proposed approaches vary in terms of architecture, technology and level of integration or interoperability among digital euro components, with the existing Eurosystem financial market infrastructures and, where relevant, with other existing market infrastructures.

Most respondents proposed unit-based[6] solutions concerning the structure of the ledger, while also confirming the feasibility of balance-based approaches within the privacy requirements laid down in the market research. There was broad consensus that a digital euro design should be optimised for waterfall[7] and reverse waterfall[8] functionalities, as these were depicted as essential scenarios in a potential digital euro solution.

Requirements related to data privacy, scalability and security were also covered in a comprehensive manner. In particular, a high level of privacy could be met for the purpose of settlement. The Eurosystem will not see or store users' private information. When supporting other potential functionalities, like fraud detection, more data might need to be processed by the relevant service provider. Concerning development approaches, respondents considered solutions based on a software architecture distributed across multiple regions and sites. With regard to the deployment model of the digital euro infrastructure, most respondents proposed cloud-based solutions, while a few respondents offered both cloud-based and on-premises solutions.

For the **Settlement** component, most respondents confirmed there are solutions able to fulfil the market research requirements. Only few respondents indicated approaches based on existing products or prototypes, whereas others considered custom-made approaches necessary to cater for the Eurosystem requirements.

Some respondents mentioned the relevance for performance purposes of combined transactions, i.e. transactions combining funding and payment, as would be the case in a reverse waterfall scenario. Other approaches considered relying on two

6 Unit-based solutions also include unspent transaction output (UTXO)-based and digital bill-based solutions.

7 A waterfall is a method for facilitating the use of a digital euro by automatically converting the amount of digital euro that exceeds a defined holding threshold into private money in a linked liquidity source chosen by the end user, such as a commercial bank account.

8 A reverse waterfall is a method for facilitating the use of a digital euro in which private money from a linked liquidity source chosen by an end user (e.g. a commercial bank account) is automatically converted into digital euro when the end user's digital euro holdings are not sufficient to make a payment.

sequential transactions, i.e. a funding transaction and a payment transaction, to reduce the complexity of the solution. Meeting the performance requirements, especially in waterfall and reverse waterfall scenarios, was considered challenging by some respondents, mainly owing to the geographically distributed nature of the envisaged transactions. Other respondents regarded the performance requirements as feasible.

Some respondents acknowledged the importance of low-latency queries by intermediaries, on digital euro entries or transactions, for information or payment status purposes. However, they stressed that such queries would only be used occasionally, as they expected intermediaries to mirror all relevant data in their own internal IT systems.

In terms of structure of the ledger, respondents saw different pros and cons in both unit-based and balance-based approaches[9]. Respondents stressed that unit-based approaches would more easily enable the required level of privacy, as obfuscation of end users' payment patterns can be addressed in a variety of ways, although privacy-enhancing techniques could also be applied to balance-based approaches. It was noted, however, that obfuscation of end users' payment patterns could hinder fraud monitoring.

For the **DCA Management** component, the feedback received on the feasibility of meeting the requirements exemplified in the market research was reassuring. Respondents suggested approaches that align the DCA management with well-established features in other TARGET Services. Regardless of the structure of the ledger, i.e. balance-based or unit-based, the interaction with the other components and the Central Liquidity Management (CLM)[10] of TARGET Services by means of application-to-application (A2A) interfaces must be guaranteed. Concerning maintenance and operation, almost all respondents concurred that a high degree of automation is essential to minimise downtime and increase availability when performing routine tasks, like software updates or backups. Many respondents also envisaged the use of liquidity monitoring and alerting tools.

Regarding the **Reference Data Management (RDM)** component, it contains system and intermediaries' reference data, without processing personal data. Respondents communicated competencies to meet the exemplificatory requirements defined by the Eurosystem. Respondents flagged that leveraging the existing Common Reference Data Management (CRDM)[11] could facilitate data consistency between a digital euro solution and current TARGET Services where data and participants could overlap.[12] Respondents largely concurred that the use of the CRDM could offer some synergies not available under a greenfield approach.

---

9 Unit-based approaches refer to a digital representation of an asset that can only be spent once in its entirety in one payment, similar to banknotes in the physical world. Balance-based refers to the typical accounting recording process of increasing or decreasing a holding balance.

10 CLM provides information on central bank liquidity, managing credit lines and central bank operations.

11 CRDM is the TARGET Services common component for the management of reference data.

12 Technical and governance interdependencies with other services will need to be analysed.

Other respondents considered an approach where the architecture of the RDM incorporates an event-driven replication element to ensure data consistency with the CRDM in real time and an element to manage data access from other components.

As to the **Data Warehouse (DWH)** component, it collects data from other components and provides data and tools for historical, statistical and regulatory reporting. Respondents broadly indicated that the exemplificatory requirements defined in the market research can be met. Some respondents proposed approaches that foresee reporting functionalities and specific analytical tools. Others suggested low-latency business storage with pre-processed data to allow real-time analysis and reporting. In this context, many respondents highlighted the need for a data quality gate to ensure the completeness, accuracy and reliability of the data.

Several respondents also considered appropriate security measures for data protection, such as encryption, access controls and network security. The responses also included approaches to monitoring, backup, recovery and support mechanisms to ensure high availability.

Concerning the **Offline Solution** component, most of the respondents indicated their compliance with the requirements defined by the Eurosystem.[13] However, further exploration will be needed into how the required security, integrity and privacy goals can be reached. The responses to the market research indicated that solutions compliant with the Eurosystem requirements would be novel and might create uncertainty when an offline solution might be ready to be rolled out. The proposed functional implementations vary, with most respondents claiming it would be possible to complete transactions via near-field communication (NFC) or Bluetooth interfaces. As an alternative approach, some respondents highlighted the possibility of relying on quick response (QR) codes for the exchange of information. In terms of access to the technical specifications, none of the respondents followed the approach of providing open specifications. The feedback also confirmed the readiness of European market providers to participate in the development of an offline solution.

Regarding the **Access Gateway** component, respondents indicated that meeting the requirements stated in the market research was feasible. Some respondents considered that the deployment model of the digital euro infrastructure, i.e. whether it would be on-premises or cloud-based, could influence its development. Most respondents further specified approaches in which the access gateway could rely on a combination of already existing commercial solutions. A few respondents also provided further details on the distinction between direct internet connectivity and connectivity via network service providers (NSPs), for example in terms of different user types and the services that need to be provided, like endpoint protection.

All respondents addressing the **Standalone App** component, confirmed the feasibility of developing it and meeting the exemplificatory requirements defined by the Eurosystem. From a methodological point of view, an agile development

[13] Some respondents proposed a delayed settlement approach, which refers to an online ledger to which the offline transaction is sent, but this is not in line with the exemplificatory requirements defined by the Eurosystem. Other responses explicitly referred to the ability to settle locally with finality and allowing consecutive offline payments. However, all these approaches relied on a systematic transfer of transaction information to an online back-end, which has privacy implications.

approach was widely supported among respondents. In terms of technology, most respondents recommended using the native languages of the relevant operating systems for the development in order to enhance the user experience. Most respondents further suggested providing a single app for both online and offline functionality to enhance the user experience and leverage synergies.

Concerning the **Integrated Banking App SDK** component, the majority of respondents indicated existing competences to meet the requirements included in the market research. They advocated connecting the development of the standalone app and the SDK. Concerning the underlying technology, the responses were similar to those for the standalone app with regard to the suggested technical implementation and use of native languages.

With regard to the **Proxy Lookup** component, respondents acknowledged that there is sufficient market knowledge and experience to meet the exemplificatory Eurosystem requirements. Respondents differentiated between two main approaches to development: a greenfield approach and one relying on existing market solutions. Relying on existing market solutions would mostly correspond to a decentralised approach owing to the absence of a widely used pan-European solution. Some respondents advised that all repositories should ideally adhere to the same technical, messaging and data processing standards.

Respondents largely concurred that both approaches would be compliant with relevant data processing standards and the additional Eurosystem requirements for safeguarding end user data. While some respondents mentioned that relying on existing market solutions could allow further integration of the digital euro into the existing payments landscape, others mentioned that the development of a dedicated proxy lookup could offer greater flexibility. Multiple respondents emphasised that non-functional requirements, particularly related to latency, may be more challenging in a decentralised set-up, especially when existing repositories are reused. On the other hand, several respondents considered the main advantage of the decentralised set-up to be data segregation, which might better mitigate the impact of system failures on end user data.

With regard to the **Onboarding Repository** component, the responses indicated that no widely available service is currently used in the market. The reason is that the main purpose of such a repository is to verify whether end users already have an existing digital euro account relationship with an intermediary, but such a centralised check is only rarely performed for private money accounts (such as savings accounts) and only in some euro area jurisdictions. Nonetheless, respondents considered that existing national databases could provide support to the functioning of an onboarding repository and that there is sufficient knowledge to develop such a repository.

Concerning the **Dispute Management** component, most of the respondents indicated their compliance with the exemplificatory requirements defined by the Eurosystem. Other respondents proposed different set-ups, such as an end-to-end solution covering dispute management or linking it to fraud detection and prevention. Several respondents reflected on approaches that would foster automation to reduce

the number of manual interventions across the stakeholders involved, for instance based on questionnaires and without the need for an exchange of dedicated documents. Multiple respondents also offered ways to store underlying documentation in an encrypted way and indicated competencies to cope with a flexible set of functionalities.

Finally, regarding the **Fraud Detection and Prevention** component, the majority of respondents confirmed that they could meet the market research requirements and that both approaches – real-time and ex post fraud detection – are feasible, provided sufficient information is available to the fraud detection engine. Several respondents confirmed the technical possibility of performing real-time assessments of fraud risk within milliseconds. For ex post fraud detection, considerations also included how to benefit from machine learning. Some respondents mentioned the challenges of designing a potential fraud detection and prevention solution balancing privacy considerations and effective fraud prevention.