EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital euro – Prototype summary and lessons learned

Executive summary

From July 2022 to February 2023 the European Central Bank (ECB) conducted a prototyping exercise to test how design choices for the digital euro could be technically implemented and integrated into the existing European payments landscape. The tests showed that it is possible to smoothly integrate them, while leaving ample scope for innovative features and technologies. The findings also confirmed that a digital euro could in principle work both online and offline, using independent designs. This would also increase the resilience of the digital euro.

The prototyping exercise is an important part of the investigation phase of the digital euro project. This project was launched by the ECB and the euro area national central banks to ensure that central bank money remains accessible in the digital age. The investigation phase commenced in October 2021 and will be concluded in autumn 2023. It aims to address key issues relating to the design and distribution of a digital euro.

The prototyping exercise included the development of a single back end – i.e. a settlement engine – designed by the Eurosystem, and five different front-end prototypes – i.e. user interfaces. The back-end prototype was not intended to be the final design, but was an experimental version to test and to learn from. The front-end prototypes were presented by private companies selected following a public call for expressions of interest. Each proposed user interface was tailored to one of the five prioritised use cases for the digital euro, namely person-to-person payments conducted (i) online and (ii) offline; payments initiated in shops (iii) by the payer and (iv) by the payee; and (v) e-commerce payments. The ECB thanks the companies for their valuable contributions to our ongoing investigative work.

For the back-end prototype, the Eurosystem developed a centralised settlement engine (N€XT), based on an unspent transaction output (UTXO) data model commonly used for transactions with digital currencies. The tests showed that this model allows for fast and efficient validation of transactions. This system proved capable of supporting different types of transaction, while protecting users' privacy by not revealing their payment patterns or account balances to the Eurosystem. In parallel, market participants successfully implemented and tested all five payment scenarios, while also experimenting with innovative approaches, such as self-custody wallets, which could potentially allow for more privacy – pending legislative developments. The exercise was also useful to technically test the interface between the front-end and back-end layers, and the results showed a smooth interaction. Nevertheless, as all the prototypes were entirely developed from scratch, the

exercise did not consider the potential effort that would be required to adapt existing payment service provider (PSP) systems.

The prototyping exercise included offline payments, which operate with no need for network connectivity or the availability of any third party when the payer and payee interact, even for consecutive payments. In line with the Eurosystem's objectives, it was possible to deepen the understanding of the technical characteristics of offline payment systems, building on the knowledge already gained from the previous experiments conducted by the Eurosystem in 2021. However, questions remain as to whether the existing technology is capable of delivering, in the short to medium term (five to seven years), a production-ready and secure offline solution in line with the Eurosystem's requirements and on the scale foreseen for the digital euro.

As the purpose of the exercise was to learn, the resulting prototypes were used as research tools and not as a basis for developing future payment solutions. The API specifications do not prejudge possible alternative designs, nor will the specific choices made for the prototypes affect any decision relating to a specific technology or functionality for the final digital euro design. Therefore, the actual prototypes presented will be discarded and not used further. Moreover, no personal data were processed in the prototyping exercise either by the ECB nor by the front-end prototype participants.

This report provides suggestions for further exploratory work, such as evaluating performance optimisation options and alternative technologies. Additional prototyping work could explore technical alternatives for later design decisions that could not be included in the scope of this exercise, such as the set-up for cross-currency payments, dispute management and fraud management.

1 Background, set-up, prototype scope and objectives

1.1 Background

The Governing Council decided to include prototyping activities in the context of the digital euro investigation phase. The main reason cited for the prototyping exercise was to gain reassurance that the combination of requirements emerging from the design decisions taken during the investigation phase could be met in practice. Furthermore, the exercise proved to be a useful means (i) to evaluate a possible technical implementation in advance of a potential realisation phase; (ii) to test the ability to integrate the digital euro into the existing European payments landscape by involving market actors; and (iii) to offer practical demonstrations to stakeholders. No personal data were processed in the prototyping exercise either by the ECB or by the front-end prototype participants. **The prototyping activity was intended to be a learning exercise; therefore, there was no goal of developing the core of a later production solution: the resulting prototypes were merely used as research tools.**

1.2 Set-up

The prototype is split between the front end and back end. The front-end components were developed in collaboration with five market participants selected via a public call for expressions of interest, while the back-end component was developed in collaboration with eight national central banks of the Eurosystem, coordinated by the ECB. These were the central banks of Belgium, Germany, Spain, France, Italy, Austria, Portugal and Finland. The prototyping exercise was conducted within a limited time frame of seven months between July 2022 and February 2023.

1.3 Prototype scope

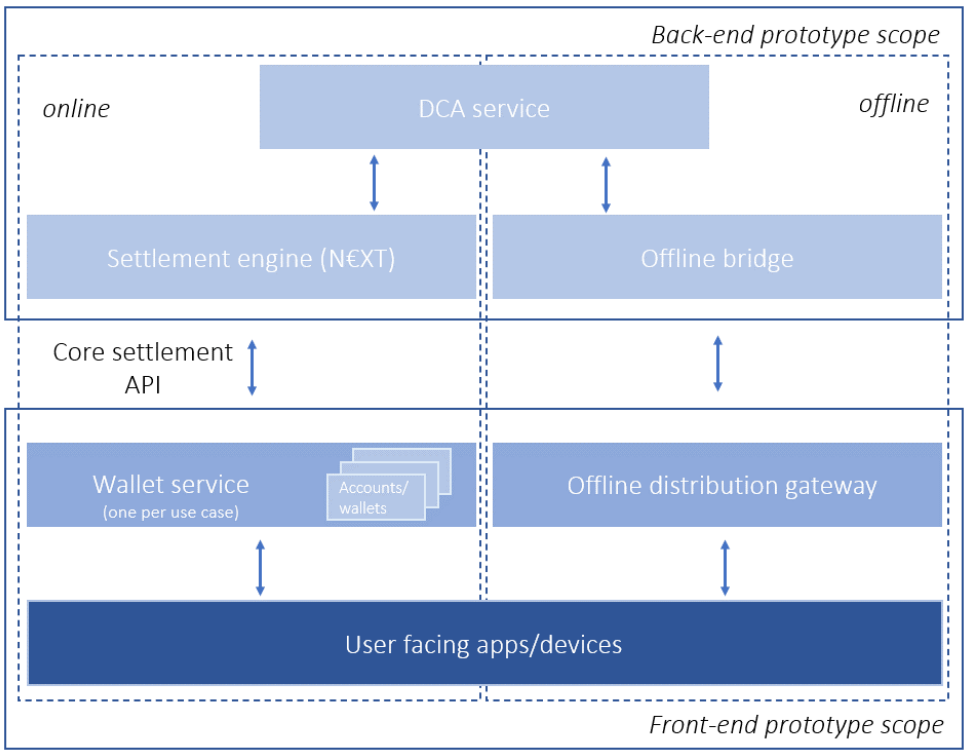
The **prototypes supporting online use cases** are conceptually structured in three layers:

1. **Settlement engine (called N€XT):** a settlement engine which processes digital euro payment and funding/defunding transactions, based on a UTXO data model, and which provides its services via a web application programming interface (API).

2. **Wallet service:** a service (provided by each digital euro intermediary in a real-world scenario) responsible for (i) managing user wallets; (ii) receiving payment instructions from user-facing applications; and (iii) converting payment instructions into UTXO-based transaction messages and sending them to the settlement engine for settlement.

3. **User-facing apps/devices:** devices or applications which interact with the user.

Figure 1
Front- and back-end prototype scope



The scope of the **back-end prototype, developed by the Eurosystem, comprised the settlement layer,** while the scope of the **front-end prototypes, developed by selected market participants, included both a wallet service and user-facing apps/devices.**

Slightly different scopes applied to the **offline payments use case.** The back-end prototype included a so-called offline bridge which provided an interface to be used by the front end for funding and defunding operations, as well as the necessary connection to central bank liquidity sources (the digital euro Dedicated Cash Accounts – DCAs – of the intermediaries, which were shared with the back end for the online use cases). The scope of the offline front-end prototype developed by the selected participant included all functionalities required at the intermediary level for the distribution of offline digital euro to end users (including a mock payment account system to enable funding/defunding tests), and user-facing apps/devices with the additional requirement that they should be based on Secure Elements.[1]

[1] From the digital euro glossary: a Secure Element is a tamper-proof chip with pre-installed software that can store confidential and cryptographic data and run secure applications.

1.4 Research objectives

The research objectives for the prototyping exercise included both quantitative and qualitative aspects. In some cases, the objectives involved benchmarking against specific indicators, while in others they were exploratory in nature. The aspects researched for the online back-end prototype included performance, scalability, resilience, security, privacy and feasibility of conditional payments. For the offline prototype they included settlement finality, technical interoperability between different offline solutions and with the online solution, transaction performance and modular design. Finally, for the front-end prototypes they comprised end-to-end integration aspects. Most of the objectives have been achieved and many valuable insights have emerged from the activities.

2 Back-end prototype

The digital euro back-end prototype for online payments, called N€XT, is a bespoke design developed from scratch by the Eurosystem. **The architecture of N€XT is not that of a distributed ledger, rather it is based on a UTXO data model**[2] which has been made popular by distributed ledger technologies (DLTs). This model was chosen as it presented the greatest potential for learning for the Eurosystem, also taking account of previous experiments[3].

2.1 Architecture

The N€XT settlement engine is the central building block of the back-end prototype. The main challenge was to implement and validate a horizontally scalable[4] settlement engine that ensures low latency of transaction processing. At the same time, the architecture should enable multi-region hosting and redundancy for resilience and to permit 24/7 operations. In the case of the N€XT settlement engine, two different large data sets need to be stored: the transactions and the UTXOs. Considering all these requirements, a scalable solution needs to rely on sharding[5]. To enable a low latency of the end-to-end process despite the expected high volumes of transactions, an event-driven streaming architecture based on microservices that communicate asynchronously was designed, as shown in Figure 2.

---

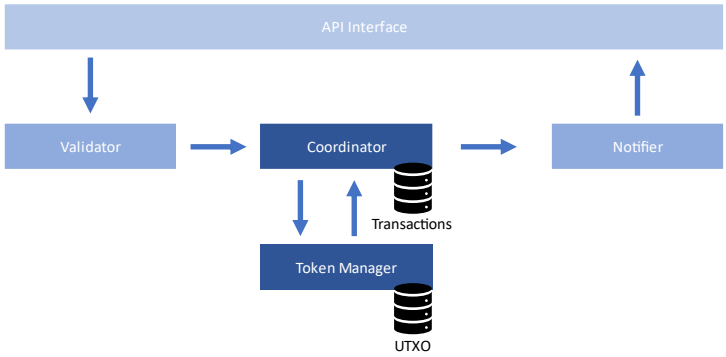
2 In the UTXO model, holdings are recorded as discrete units with immutable value. Each UTXO participates only in two transactions, one in which it is generated and one in which it is consumed (potentially destroyed). Multiple UTXOs can be combined and spent together in a single transaction. Should the total value of the input UTXOs exceed the transaction amount then for the difference a new UTXO is created and handed back as change.

3 See the document entitled “Digital euro experimentation scope and key learnings”, at https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

4 Horizontal scaling refers to designing the engine in a way such that if additional nodes/machines were added to the system this would effectively provide an increased system workload capacity.

5 Sharding refers to a process of distributing the storage (and sometimes processing) of a larger set of information across multiple nodes based on a certain key derived from the data themselves. Each node only keeps a part of the overall data and each set of data is stored on only one node.

Figure 2
Overview of the settlement architecture



Kafka, an open-source messaging technology, serves both as the inter-service communication platform and as a multi-site sharded data store for transactions and UTXOs. The allocation of responsibilities to the different microservices is as follows:

The **Validator** serves as the entrance to the settlement engine. It validates all input data coming from the web API by checking:

- syntax, i.e. the correct formatting of the message and the presence of all mandatory fields;
- semantics, i.e. correct values for fields – for instance no negative amount and the sum of all inputs should be equal to the sum of all outputs;
- cryptographic signatures;
- and authorisation, i.e. whether the sender is allowed to make use of the money.

As the Validator operates in a stateless fashion, several instances can independently process the stream of input data.

- The **Coordinator** is a scalable component that creates a sharded storage for transactions and checks for duplicates. This component coordinates the atomic swap of old into new UTXOs via a two-phase-commit involving the Token Manager and, if needed, handles rollbacks owing to failed transactions.
- The **Token Manager** is a scalable component that creates a sharded storage for UTXOs and handles all related operations based on requests from the Coordinator. These operations include checks for the existence of specific UTXOs and their validity/availability for transactions, as well as the related reservation/release. The Token Manager also invalidates spent tokens and creates new UTXOs as requested.
- The **Notifier** prepares the final settlement result based on events received from the Validator or Coordinator and forwards them to the web API layer for communication of the result to the parties involved. As the Notifier operates in a stateless manner, several instances can independently process the stream of settlement results.

2.2 Key results and learnings

Future-proofing. The UTXO transaction format of the back-end prototype natively supports many types of transaction with a single, common message format, and can easily be extended to support more transaction types. This makes it very beneficial for supporting both core and advanced features in a future-proof manner. The transaction types implemented for the prototype were payment, funding/defunding and reservation/unreservation of funds. The only parameter that distinguishes these types of transaction and allows the different validations and input data requirements to be catered for is the so-called witness-type. Witness-types are a cryptographic construct which essentially allows different authorisation schemes to run simultaneously. Each witness-type can also employ different cryptographic algorithms. The abstraction provided by UTXO witness-types not only allows the system to be extended, but also supports crypto-agility, as it is possible to change cryptographic primitives without extensive development efforts and in a modular way.

Conditional payments. The reservation of funds transaction type is particularly interesting, as it allows conditional payments[6] to be implemented without any reliance on smart contracts (user-defined programs stored and executed directly on the settlement layer), but rather based on APIs, with comparable functionalities and guarantees. In the case of a conditional payment, the payer authorises the payment together with the related condition. To ensure successful execution once the condition is met, a certain (maximum) amount of funds is reserved and then later used to fulfil the payment obligations. Compared with smart contracts, this approach allows a clear distinction between the payment leg of a transaction and the related triggering event. The payment leg remains in the secure environment of the market infrastructure, while the trigger can be monitored and detected outside the platform, allowing third parties to provide innovative business services.

Issuance and redemption. In the back-end prototype there are two alternative approaches for the creation/destruction of UTXOs (i.e. issuance/redemption of digital euro in circulation). In the first approach, the DCAs of intermediaries use the traditional balance-based data model[7], and UTXOs are created “on the fly” upon the debiting/crediting of DCAs when end users fund/defund their wallets. In the second approach, UTXOs are pre-emptively created upon the funding/defunding of intermediaries’ DCAs, which natively support the UTXO data model.

Both approaches have advantages and disadvantages. Creating UTXOs on the fly during end-user funding will lead to a very high number of issuance/redemption transactions, as each funding/reverse waterfall and defunding/waterfall operation will result in an issuance transaction and a redemption transaction. On the other hand, the amount of digital euro in circulation is easy to determine, as it is the sum of the

6 From the digital euro glossary: conditional payments are payments that are instructed automatically when predefined conditions are met.

7 Balance-based refers to the typical accounting recording process of increasing or decreasing a holding balance, in contrast to unit-based approaches (such as UTXOs) which 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.

balances of DCAs, and the Eurosystem has a great deal of experience in handling DCAs in a balance-based manner.

The alternative of generating the additional UTXO value during the funding/defunding of an intermediary's DCA substantially reduces the number of issuance/redemption transactions. The funding/defunding of end-user wallets then technically becomes a UTXO-based transfer between the wallet representing the intermediary's DCA and the end user's wallet. On the other hand, however, the DCA service needs to maintain a wallet for each DCA and manage the respective UTXOs in a transparent way.

The prototype has shown that both approaches do work. From a technical perspective, the second alternative of representing DCAs as UTXO wallets clearly demonstrated its advantages, although a scenario with high throughput on such a DCA as a result of high volumes of end-user funding and defunding operations has not been tested owing to time constraints.

Scalability and performance. One of the main challenges identified for the digital euro back-end prototype was how to design a scalable architecture that supports high throughput and low latency. Scalability is obvious for stateless components; however, the N€XT architecture relies on stateful components too, i.e. the Coordinator and Token Manager. The tests on the N€XT prototype gave good initial results for horizontal linear scalability, showing that increasing computational resources results in a proportional increase in throughput. Some issues emerged in relation to high processing latency when the system was flooded with transaction requests. Further investigation will be necessary to gain a better insight into the cause of these issues.

Privacy. Among the key research objectives of the back-end prototype was the investigation of a design that would ensure the privacy of end users vis-à-vis the Eurosystem. One of the advantages of a UTXO-based data model is in fact the ease of implementing a centralised ledger that does not allow balances to be associated with any given individual. The N€XT prototype natively supports one-time UTXO addresses and does not need to know which wallet holds the UTXOs, nor the identity or pseudonym of their owner, in order to process UTXO transactions. Thus, the prototype showed that the Eurosystem would be able to perform the settlement tasks without being able to know the balance or to infer the payment patterns of any user. However, this approach will require intermediaries to manage one-time addresses and to implement certain features such as checks on holding limits. Furthermore, it would require the incorporation of procedures to ensure that end users can recover their funds if their intermediary suddenly ceased to operate.

3 Front-end prototypes

To identify suitable companies that could develop a front-end prototype, a call for expressions of interest was published on the ECB's website on 28 April 20228. The call for expressions of interest included a set of minimum capabilities that companies needed to fulfil to be eligible to participate. Additionally, it included qualitative capabilities that were used as selection criteria to identify the five most suitable participants for the specific use cases. A total of 56 entities expressed their interest in participating and five of these – all established actors for their respective use cases – were ultimately selected based on their compliance with the criteria.

3.1 Prioritised use cases for the front-end prototypes

The prioritised use cases and the selected participants were decided as follows:

- Person-to-person online payments – CaixaBank;
- Person-to-person offline payments – Worldline;
- Point-of-sale payments initiated by the payer – EPI;
- Point-of-sale payments initiated by the payee – Nexi;
- E-commerce payments – Amazon.

3.2 Guidance given to the participants and information-sharing

At the start of the prototyping exercise, the participants received the technical onboarding package[9], in which background information on the prototype layers and expected scope were defined. The Eurosystem defined the essential functions for the front-end prototypes and participants could voluntarily expand their scope by adding optional functions. So that selected participants would not gain a competitive advantage over other market actors and in order to ensure a level playing field, the Eurosystem has published all information that was provided to the participants, namely the abovementioned onboarding package and the final version of the prototype API[10].

8 See the call for expressions of interest at https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews220428.en.html

9 See the onboarding package at https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221207_annex1_front_end_prototype_providers_technical_onboarding_package.en.pdf

10 The prototype API can be downloaded at https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.prototype_summary20230526_annex~7767a2b1dd.en.zip

3.3 Delivered front-end prototypes

Five front-end prototypes, each covering one of the use cases, were successfully delivered as part of the exercise. The deliverables ranged from mobile phone applications, to implementations in a SmartPOS payment terminal and an online shopping interface. Payments could be simulated contactless (via near-field communication), through QR-codes, in an e-commerce checkout process and through request-to-pay. All of the front-end prototypes have been integrated with the Eurosystem back end and tested end-to-end.

Two additional, innovative functions were delivered as part of the exercise. First, self-custody wallets that store the private key used to authorise transactions locally on an end-user device were included. In the custodial model, the private key is stored with the intermediary. The storage of the private key and its use to cryptographically sign transactions were the only functionalities included in the self-custody wallet, respecting the intermediation role of banks and other digital euro intermediaries.

Second, simplified customer due diligence checks depending on the risk profile of the transaction were prototyped. Such a risk profile, or "tier", would either depend on the individual transaction amount, or on the cumulative value of transactions in a wallet in a given time window, or on both criteria. For each tier, a different amount of personal information would need to be available to intermediaries to perform the due diligence checks, which could reduce the amount of personal data to be transmitted between intermediaries, especially for low-value payments, should this come to be permitted by legislation.

3.4 Key results and learnings

All participants were able to successfully deliver a front-end prototype and integrate it with the N€XT back-end prototype, thus confirming that a potential digital euro could be smoothly integrated into the existing European payments landscape while leaving room for innovative features and non-traditional technology choices.

UTXO data model and API interface. The prototype interface between the front end and the back end was validated during the integration exercise with the front-end participants. All front-end prototypes were successfully integrated with the back end, and the adoption of the UTXO data model was smooth and successful on both the back and the front end. This finding, however, does not consider the potential effort required to adapt existing PSP systems, as all participants developed their prototypes from scratch. The integration with a settlement system based on such a data model may entail extra costs and effort for intermediaries, as existing PSP systems and messaging standards would have to be adapted to support it. This is because traditional PSP systems are balance-based rather than cryptography-based and unit-based.

Self-custody wallets. Custodial wallets are the current standard in payment instruments, whereas self-custody is a novel approach that aims to be more cash-like and give the end user full control over their digital euro – more closely mirroring

an end user's control of euro banknotes in their physical wallet. One conclusion from the experimentation was that the implications of key custody at the end-user level did not have any impact on the user experience for customers or on the role of intermediaries vis-à-vis the digital euro and could allow for greater innovation and enable new service offerings.

Tiered due diligence checks. The main learning with regard to these checks was that it is technically feasible and potentially advantageous to unbundle checks that are dependent on the user's identity (such as AML/CFT[11] checks) from the payment flow, so that they can be either skipped for low-value payments – if permitted by legislation – or potentially performed by different entities. In such a set-up, the use of the digital euro would come closer to the use of cash from a privacy perspective, and benefits could be achieved by relying on specialised identity verification service providers who would ideally adhere to harmonised pan-European standards, rather than relying on intermediary-specific identity solutions.

Shared services for intermediaries. While working with the participants, it emerged that it might be more efficient to provide certain functions centrally as shared services, rather than having each intermediary implement and operate their own services. This would be beneficial for interoperability and standardisation, and would result in economies of scale. Examples of such functions and services are:

- Cross-intermediary communication, through a message routing service;
- Alias lookup, e.g. a service that maps aliases such as mobile telephone numbers or email addresses to digital euro addresses for payment initiation;
- Identity verification services, to facilitate digital identity proofing and customer onboarding in a technically standardised manner.

4 Offline prototype

The offline person-to-person payment use case warranted particular focus owing to its unique characteristics. This use case foresees the possibility of consecutive payments in the absence of network connectivity, with final settlement without the validation of a third party beyond the payer and payee. Previous experiments conducted by the Eurosystem[12] and subsequent analysis indicated that an offline payment solution of this kind must rely on secure hardware (Secure Elements) to be sufficiently secure. The focus of the prototyping activity for this use case was on gaining more in-depth knowledge of how the combination of hardware and software protocol could avoid double spending and ensure settlement finality and non-repudiation. An additional line of investigation looked at achieving interoperability (i) between different technical solutions provided by different vendors based on (open) standards; and (ii) between offline and online digital euro prototypes.

11 AML stands for anti-money laundering. CFT stands for countering the financing of terrorism.

12 See the document entitled "Digital euro experimentation scope and key learnings" at https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

4.1 Architecture

The offline prototype was built as a secure JavaCard applet running in smartphones' Secure Elements, and a mobile phone application running as the end-user interface leveraging the secure applet and using near-field communication antennas for data exchange between offline devices. Funding and defunding operations are supported when the device is online to contact an "offline digital euro gateway" available at the user's intermediary. This component in turn relies on interfaces with a mock payment account and with the "offline bridge" component of the Eurosystem's back-end prototype to process funding/defunding requests. The prototype data model is balance-based, as opposed to the UTXO-based data model used for the online back-end prototype; different versions of the offline settlement protocol were analysed, including some which used cryptographic techniques to validate the integrity of the transaction history.

4.2 Key results and learnings

The prototyping activities provided the Eurosystem with a deeper understanding of how offline solutions can be technically designed and highlighted that the risks can only be effectively mitigated by means of regular online reconciliation of data **–** i.e. transferring the data stored in the secure device to a central database for security checks **–** which would be the only sure way to detect anomalies. The prototyping exercise showed that an offline peer-to-peer solution could potentially be balance-based and does not necessarily need to be unit-based (i.e. based on UTXO or bills), leveraging cryptographic signatures applied to transaction history to mitigate the risks of typical attacks. Furthermore, it showed that online and offline digital euro prototypes can be interoperable even if based on different data models and technical designs. In the prototype, the number of shared components was minimal, being limited to the DCA service. Such a set-up can increase the overall resilience of the digital euro. With regard to interoperability between offline solutions based on different technologies, the offline prototype was based on a single platform (JavaCard) that is a standard that can be used on hardware from different manufacturers and the prototype was tested on devices with different chipsets from different manufacturers. The possibility of working with an alternative platform was identified but not pursued owing to time constraints. The limitations imposed by certain mobile phone vendors on the use of near-field communication antennas and Secure Elements on their devices was identified as a remaining challenge. Further challenges are expected to emerge with regard to the delivery of a production-grade solution that fulfils the Eurosystem's requirements in the short to medium term (five to seven years), owing to (i) the novelty of the required solution; (ii) the low level of readiness of existing technology; (iii) the absence of security standards that encompass both hardware and software aspects of a possible solution; and (iv) the

need to roll out offline support to a large variety of user devices and payment terminals.

5 Further work

The prototyping exercise has delivered valuable insights into the technical choices for a potential digital euro system. Nevertheless, owing to the short time frame, open questions remain. Directions for potential further work include:

- Further investigation of the specific challenges of a geographically distributed system and the aspects to consider for ensuring resilience, availability, throughput and latency;
- Further analysis of the architecture and technology stack used to ensure that the most suitable technology/product is applied for each component, as well as testing and comparison of possible alternatives;
- Further investigation of the origin of the latency issues detected during the scalability tests.

In addition, the following additional prototyping activities could help to better prepare for the next phase of the digital euro project or to anticipate some crucial tasks:

- Further work on the API layer, with the goal of specifying the principles and general design considerations for the production API;
- The design and potential implementation of a second prototype with a completely diverging technology stack to validate current design choices and investigate options if a non-similar facility[13] were to be required;
- Prototyping cross-currency functionality to gain further insights into technical aspects of linking different central bank digital currency systems;
- Prototyping additional requirements stemming from design decisions that were not included in the prototype scope owing to planning constraints.

With reference to the front-end prototyping, the topic of wallet portability and recovery could be explored further. This would address the use case in which an intermediary suddenly ceased to operate, or the user lost the wallet in a self-custody model. In any case, further work on front-end topics could be carried out independently of the already developed front-end prototypes.

[13] According to the Bank for International Settlements, a non-similar facility "seeks to replicate the core functionality of an FMI [financial market infrastructure] but using technology different from that used by the primary facility. Accordingly, in the event of a cyber intrusion that has managed to compromise the core systems of the primary facility, an FMI could recommence operations using the non-similar facility, assuming the NSF itself is not compromised".

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary (available in English only).