EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital euro experimentation scope and key learnings

1 Scope of the experiments

In September 2020 the Eurosystem's High-Level Task Force on Central Bank Digital Currency launched experimental work on a digital euro with a view to assessing, and gaining further insights into, the technological feasibility of design choices identified in the Report on a digital euro (hereinafter referred to as "the Report").

Experts from the euro area national central banks and the ECB participated in the experiments, which were grouped into four work streams. These work streams assessed different design features covering four main areas: the digital euro ledger, privacy and anti-money laundering (AML), limits on digital euro in circulation, and end-user access. The objective was to address the key design questions that had been left open by the Report and that warranted analysis in terms of their technical feasibility, and to acquire a broad understanding of the compliance of the different design possibilities with the principles stated in the Report. The experiments were conducted in a multidisciplinary environment and also involved participants from academia and the private sector, without endorsing any specific solution.

Work stream 1: "Scale the existing"

The experiments of this work stream focused on an account-based system and tested the issuance, redemption and distribution of a digital euro using a network architecture built on the existing, centrally managed architecture of the TARGET Instant Payment Settlement (TIPS) system, which is operated by the Eurosystem.

The primary focus was to investigate and demonstrate the scalability of the TIPS system as a potential infrastructure for a digital euro. This work drew on equivalent key performance indicators (KPIs) that were also used in work stream 3.

In addition, the work stream conducted experiments on how an infrastructure based on the TIPS system could be integrated into the existing payments ecosystem via three different interfaces based on i) the Single Euro Payments Area (SEPA), ii) point-of-interaction, and iii) the revised Payments Services Directive (PSD2)[1]. It also explored how using pseudonymous identities could afford enhanced privacy on a "need to know basis" in this digital euro model.

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p.35).

Work stream 2: “Combined feasibility”

The experiments of this work stream focused on how to combine a centralised ledger and (one or more) decentralised platform(s) based on distributed ledger technology (DLT). They were divided into two sub-streams (a “flat” approach and a “tiered” approach) that tested and demonstrated two alternative ways in which cross-ledger transactions could be settled. The objective of this work stream was to test the interaction between centralised and decentralised technologies, allowing for innovative functionalities, while also relying on existing infrastructures. The experiments were designed to gain a better understanding of how different features (e.g. programmability, enhanced privacy) could be added to a digital euro.

The flat approach proposed a liquidity exchange model that relied on central bank accounts acting as a bridge for liquidity transfer between digital euro platforms. The aim was to test how an account-based digital euro and a DLT-based digital euro could complement each other in accommodating user needs that could be typically met with either of the two platforms. The experiment combined an upgraded version of the TIPS system (the centralised ledger) with two different DLTs: the first enabled the creation of an online digital euro with enhanced privacy, via a so-called payment channel network, and the second enabled programmable features. In the payment channel network, retail users open payment channels with intermediaries, so that payments between users can take place off ledger, instantly and privately, while being routed via financial intermediaries and possibly via central banks. Using the programmable DLT solution, financial intermediaries can automate use cases in the form of smart contracts, which are deployed and executed directly on the ledger, while retail users can send and/or receive funds to/from the smart contracts, for example as a result of their execution.

The tiered approach proposed a hierarchical structure in which a centralised ledger (the TIPS system), known as the first tier and operated by the central bank, is used to issue digital euro and exchange liquidity between different digital euro platforms in a second tier. Supervised intermediaries have access to dedicated accounts in the first tier where they can exchange the digital euro issued and distribute them via a variety of platforms (DLT and non-DLT) to end users. This experiment demonstrated that it was possible to interface multiple platforms and transfer liquidity between them relying on existing technology and business processes (based on XML message exchanges, such as those used in SEPA). By combining existing and new technologies in a hierarchical model, the tiered approach facilitated innovative features such as programmability and privacy, while leveraging existing infrastructures. It clearly distinguished the issuance process and the distribution process, assigning the former to central banks and the latter to the private sector.

Work stream 3: “A new solution”

The experiments of this work stream aimed at assessing a solution for the issuance, redemption and distribution of digital euro using a blockchain-based platform and

fixed value tokens ("digital bills").[2] The primary focus was to investigate and demonstrate the scalability potential of this blockchain-based platform and digital bills as a possible infrastructure for a digital euro.

In addition, the work stream explored the possibility of combining this blockchain solution with existing digital identity (e-ID) and digital signature components. Furthermore, it looked into how different degrees of privacy could be afforded to different parties (e.g. counterparty, core ledger, operator, account/wallet operator) under different deployment models, and assessed their implications for compliance with regulations on AML and combating the financing of terrorism (CFT).

The experimental set-up simulated an end-to-end digital euro proposal that implemented a solution covering the issuance of digital euro in the form of electronic bills by the central bank and a payment infrastructure based on a new blockchain technology. Under that solution, the issuance of a central bank digital currency (CBDC) is still controlled by the central bank, and whenever a payment is made between users, the units of digital euro simply change ownership. This value-based digital euro ledger can support a range of decentralised and centralised payment ecosystems in parallel. The system simulated an environment in which users were onboarded by the end-user wallet provider, using e-IDAS[3]-compliant e-IDs/certificates. The end-user wallet providers acted in a similar way to a third-party service provider under PSD2, operating the user interface (wallets) and having responsibility for AML and know your customer (KYC) procedures. Within the scope of the experiment, the digital euro were held in wallets that linked users' identity to the cryptographic key(s) for their units of digital euro. These cryptographic keys allow users to sign transactions and are stored in a custodial service separate from the wallets, enabling customer portability.

Work stream 4: "Bearer instrument"

Together with six companies selected via a procurement process,[4] the research conducted by this work stream focused on offline payment solutions (i.e. hardware-based bearer instruments) that were already on the market or under development, and that could facilitate the use of a digital euro as a bearer instrument. The selected companies were tasked with delivering a proof of concept and a comprehensive research report that addressed a list of open questions on the design of a digital euro and specific questions relating to hardware-based bearer instruments.

The assessments covered a number of aspects: i) the feasibility of offline solutions for both peer-to-peer (P2P) and person-to-business (P2B) transactions, ii) ways to establish different levels of privacy, iii) geographical limits for holdings of digital euro and remuneration in the context of offline transactions, iv) security and resilience

---

2 The blockchain-based platform used consisted of a log of transactions, in which the assets were represented as units of digital euro (that can be thought of as virtual "bills" with a given value), with a separate ledger containing the transaction history maintained for each bill.

3 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

4 For further information, see https://www.ecb.europa.eu/euro/banknotes/research/html/index.en.html#call.

against integrity attacks, v) ease of use and inclusiveness, and vi) cost per unit of production.

2 Key learnings from the experiments

The work streams assessed a range of design features that complemented each other (rather than being mutually exclusive or vying to be the “best” solution). While some were tested by more than one work stream (e.g. privacy was assessed by all work streams, KPIs and the ecological footprint by two work streams, and the combination of centralised and decentralised infrastructures with intermediation roles by two work streams), other advanced functionalities (e.g. e-IDs) were tested by only one work stream. The key learnings are summarised below.

The results of the experiments provide input on design questions, thereby supporting policy discussions and design decisions on a possible digital euro, and do not pre-empt decisions or commit the Eurosystem to providing a digital euro. The results are grouped into four categories, which do not correspond to the four work streams presented in the previous section but combine their findings under common categories.

2.1 Digital euro ledger

One of the key questions addressed by the experiments was the extent to which the digital euro ledger could be limited by the technological choices in terms of performance and flexibility. The work streams that conducted experiments with the TIPS system and a blockchain-based digital euro provided some answers in that regard. The prototypes were able to exceed the threshold of 10,000 transactions settled per second.[5] Testing of end-to-end payments using the blockchain-based solution achieved the equivalent of 15,000 retail payments per second, with additional testing of core components alone showing that this could be scaled up to 325,000 retail payments per second. The solution based on the TIPS system comprised only the settlement system behind a transaction injector simulating instructions sent by intermediaries and showed that it could process up to 40,000 transactions per second. Regarding the latency in transaction settlement, with the blockchain-based solution, 95% of the transactions could be signed by the payer, settled and cryptographically verified by the payee in fewer than three seconds, while with the TIPS-based solution, 95% of the transactions could be settled in fewer than 0.8 seconds.[6] Further scalability assessments could be carried out to evaluate the impact on the throughput of other design choices (such as privacy techniques, remuneration, etc.).

To estimate the potential environmental impact of a digital euro, the power consumption of the core settlement systems was measured and assessed to be in

5 This estimate is based on the total number of cash and card retail transactions in the euro area per year (around 300 billion), assuming a uniform distribution of transactions along all seconds of the year.

6 In further testing, the blockchain-based solution demonstrated a reduced payment time of 1.3 seconds.

the order of a few kilowatts to run thousands of transactions per second. This measurement was also used to extrapolate the carbon footprint of the core settlement system and this was found to equate to the carbon footprint of a few European households. Although this is only one element of the total environmental impact, the latter can be considered to be relatively low, as the power needed to run these systems equates to that used by a single electric car on a motorway.

To complement the comparison of the different types of ledger, two sub-work streams explored ways of creating a multi-ledger environment. The experiments revealed that there are various solutions for implementing an architecture that combines centralised and decentralised infrastructures, but they did not cover either throughput or latency considerations, which is a precondition for a multi-ledger environment to be considered a viable option. However, given the results of other experiments encompassing the centralised ledger and a blockchain, it is plausible that multi-ledger environments could also meet the expected KPIs.

One experiment also found that payment channel networks could be used to enhance scalability and privacy. However, some legal questions would need to be clarified before they could be considered for implementation. For example, could digital euro exchanged in the payment channel network be viewed as a direct claim on the central bank (i.e. a CBDC) or a claim on the channel counterparty to deliver digital euro (i.e. not a CBDC)? For this, it would be necessary to determine the role of each node in the payment channel network from a legal point of view, as well as the implications of those roles, e.g. is a node acting as a settlement agent when forwarding a transaction within the payment channel network?

The potential addition of programmability features to a digital euro was also investigated because the provision of additional logical conditions linked to the payment instructions (that could be defined by third parties) could support innovative business processes and help central banks to define the properties of central bank money and control the conditions of its allocation and use. The ledgers tested demonstrated that various types of automation could be programmed into DLTs by i) deploying different blockchain protocols built either on token-based standards or not, ii) through comprehensive functionalities, or iii) as a restricted set of instructions. Automation in case of a centralised ledger (e.g. by third parties deploying automation relying on external services and instructing payment processing on a central ledger) was not tested at this occasion.

With regard to offline payments, the experiments confirmed their feasibility from a technical point of view. However, they did not answer all the questions on how to fully control the risk of double spending. One of the key elements in ensuring the integrity of the system over time is that transactions cannot be offline indefinitely, i.e. offline devices will at some point need to resynchronise with the online ledger.

2.2 Privacy and AML

The baseline for all experiments was to investigate from a technological perspective, either directly or indirectly, different privacy models for a digital euro. To consider

some of those privacy models as a viable option, their compatibility with AML/CTF legislation, as well as their impact on throughput, would need to be further verified.

The experiments based on the TIPS system focused on the segregation of information between the intermediaries and the settlement system operator. With this approach, intermediaries would either use pseudonyms to relay information to the TIPS system (which could be linked with real identities if necessary) or rely on the "anonymity card", which is a limited version of a TIPS account that could be topped up with cash, thereby eliminating the need for KYC procedures.

The experiments that explored blockchain ledgers identified a large pool of possibilities that could be used to enhance the privacy options for end users and showed that blockchains could be easily adjusted to accommodate various levels of privacy.[7] Some examples of the techniques explored include:

- one-time pseudonyms: a different pseudonym is used for each transaction that users participate in, making it difficult for the receivers to link the numerous pseudonyms to the identity of the sender;
- transaction mixing: a protocol or a service enables multiple users to mix their transactions in order to prevent pseudonym linkage and traceability, i.e. linking the sender and receiver;
- payment channel network: a network of bilateral channels in which the privacy level could vary, depending on the agents who are allowed to participate in the network.

When multiple privacy techniques were combined to investigate different privacy levels for the end users, a number of technological solutions were identified that would provide a basis for a payment solution with a very high degree of privacy. Nonetheless, while some solutions could provide legally compliant alternatives, for instance with traceability solutions (ex post), others would require further analysis to verify that the high level of privacy did not violate AML/CFT regulatory requirements.

In offline solutions, complete untraceability was possible provided that the assets (i.e. digital euro) exchanged remained offline. However, if an offline solution is designed to pass on the transaction information as the assets are transferred, there is a possibility of ex post traceability in offline transactions.

2.3 Limits on digital euro in circulation

The experiments found that it is possible to introduce limits on balances and transaction amounts regardless of the underlying technology. In addition, they identified a potential way of automatically transferring the excess amount (e.g. if an incoming transaction sends a digital euro balance above a certain limit) to an

[7] It is important to note that although the ledgers experimented with showed a larger range of options for blockchain-based technologies, a newly designed centralised system could include some of these options if they were taken into consideration from the start of the design process.

account/wallet in private money that is paired with the digital euro account/wallet. The impact of this on transaction latency would need to be further verified for this to be considered a viable option.

The implementation of a remuneration scheme could have some limitations, although remuneration was successfully implemented on different types of ledger. However, end users could perceive this as an arbitrary rate applied to transactions.[8] One solution, as proposed in one of the blockchain-based experiments, is to hold value instruments in custodial wallets that allow remuneration schemes to be implemented in a manner equivalent to account-based schemes.

The investigations into offline bearer instruments confirmed that imposing limits on transactions in terms of time and remuneration would present significant challenges for the offline use of digital euro, but it would be possible to have a capped amount for individual transactions or the balance held offline. If the secure hardware device is designed to perform internal validation checks when processing the payments, this could also facilitate the setting of other rules to cap transfer amounts and/or register high value transactions. Nonetheless, it remains a challenge to design and enforce time-sensitive rules, such as setting a transaction limit over a certain time frame, as these would require a connection with the online ledger from time to time to ensure that the rules were not breached.

The experiments were based on the underlying assumption of each citizen only having one digital euro account/wallet, which would need to be ensured during the process of onboarding new account/wallet holders, or that all accounts/wallets could be identified for the purpose of applying the right remuneration (the latter was not part of the experiments).

2.4 End-user access

The experiments conducted with several end-user solutions (mobile applications, web apps and cards, point-of-interaction/point-of-sale integrations) revealed numerous options for making digital euro available to a wide variety of users. The possibility of using the existing infrastructures and technologies will make it easier to adopt digital euro as a means of payment. The solutions provided via near field communication (NFC) and Bluetooth to enable contactless payment were promising in terms of their ability to support fast transactions, but also had limitations in terms of practicality when required to transfer large quantities of information. For instance, in certain cases, the designs of bearer instruments for processing transactions offline, as well as sensitivities in phones and card antennas, ended up preventing the transfer of the record of transactions of a particular unit of digital euro. In addition, practical usage demonstrated other limitations in accessing certain components in cases where manufacturers had limited the reach and usability of certain devices and applications.

[8] Units of digital euro should keep their value irrespective of the payment rails used.

The experiment that tested state-issued e-IDs for user authentication involved the Baltic SmartID, which is based on existing e-ID services, and a Spanish e-IDAS-compliant certificate alongside an e-ID solution that is more akin to the self-sovereign identity model, as developed by the World Wide Web Consortium. Irrespective of the model tested, the findings show that it is possible to implement a user authentication process that accommodates both centralised (Baltic) and federated (Spanish) e-ID systems for the same account/wallet provider. Although further investigation is required (e.g. to test other e-ID systems, such as fully decentralised ones or with different account/wallet providers), the existing e-IDAs-compliant national e-ID systems/certificates along with other identity provision services could be used as a basis for user authentication in the case of a digital euro. Nevertheless, linking a person's e-ID to digital euro holdings would enable the application of limits and tiered remuneration in a relatively smooth way, and e-IDs could also make it easier to switch between digital euro account/wallet services providers and possibly reduce KYC and AML costs. Unfortunately, however, in many countries the provision/use of government-issued e-IDs is still relatively low, although the proposed update to the e-IDAS regulation aims to change this with the introduction of national identity wallets. Even though this experiment showed that e-ID solutions could be very helpful in providing digital euro services, the above-mentioned lack of coverage may require the widespread adoption of an e-ID solution.

3 Conclusion

The results of the experiments show that there were no major technological restrictions for any of the topics assessed and indicate that there is the wherewithal to accommodate the design requirements discussed in the Report. The findings will need to be weighed up by a number of related areas, ranging from policy to legal. For some solutions, it would also still need to be confirmed whether or not they could already be implemented in a way that is suitable for a retail digital euro aimed at the general public, taking into account, for example, safety, reliability, speed, convenience and cost efficiency.

Overall, the practical findings provide initial input into policy discussions and further experiments during the investigation phase of the digital euro project. They also provide guidance for decisions, assessments and future work on how to combine the different models in the upcoming digital euro investigations and possible digital euro use cases (e.g. how could a digital euro be integrated into the current payments landscape? To what extent should current standards be used? What services could a digital euro offer?). In turn, the sooner the scope of possible use cases can be narrowed down, the easier it will be to set up focused and specific technical investigations in the future.

Such practical and conceptual investigations during the investigation phase would build on the insights gained in this experimentation phase and contribute to the development of a minimum viable product that should/could be available for live experimentation in the future.

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).