Eesti Pank
EUROSÜSTEEM

BANK OF GREECE
EUROSYSTEM

DEUTSCHE BUNDESBANK
EUROSYSTEM

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

BANCO DE ESPAÑA
Eurosistema

LATVIJAS BANKA
EIROSISTĒMA

EUROPEAN CENTRAL BANK
EUROSYSTEM

BANCA D'ITALIA
EUROSISTEMA

DeNederlandscheBank
EUROSYSTEEM

Work stream 3: A New Solution – Blockchain & eID

July 2021

July 2021

CONTENTS

EXECUTIVE SUMMARY AND CONCLUSIONS

In September 2020, the Eurosystem's High-Level Task Force on Central Bank Digital Currency launched experimental work on a digital euro to assess and gain further insights into the technological feasibility of the design choices identified in the report on a digital euro[1]. The experiments[2] were conducted in a multidisciplinary environment and also involved participants from academia and the private sector, but did not endorse any particular solution.

This report covers the experiment conducted in Work stream 3 *A new solution* and has been written jointly by Eesti Pank, Banco de España, Banca d'Italia, Deutsche Bundesbank, Latvijas Banka, De Nederlandsche Bank, Central Bank of Ireland, Bank of Greece and the European Central Bank.

A question that has accompanied the entire debate since contemporary discussions about issuing a retail CBDC first began is whether blockchain or DLT technology could and should be the basis for central bank money. These technologies open up the possibility of disruptive innovation in payments through programmable money, micropayments, machine-to-machine payments and more. Questions remain however about their security, privacy, and compliance properties, and particularly about whether blockchain and DLT platforms can scale to meet the performance requirements of a modern payments and money system over the coming decades.

To address these questions, Work stream 3 assessed a blockchain-based system for issuing, redeeming and distributing the digital euro. The CBDC system evaluated combined an existing blockchain-based platform with novel architecture for money and payments, instantiating value in digital bills, which are fixed-value tokenised representations of banknotes that represent the liabilities of the central bank.

The investigation focused on three areas:

Scalability. The primary focus was on investigating and demonstrating the potential scalability of this blockchain-based platform and of digital bills as a possible infrastructure for a digital euro. It was hypothesised that bill-based architecture would be able to support the parallel processing of transactions, scale linearly and handle a very large number of accounts settling exceptionally large numbers of transactions simultaneously. Performance testing concluded that the system was able to exceed the KPIs of the Eurosystem and validated the hypothesis that bill-based systems are linearly scalable.

Performance test results:

- A load-testing programme simulated 100 million wallets performing payments on a deployment of the CBDC system, optimised to meet the Eurosystem's KPIs (see page 9). This end-to-end setup supported 15 thousand transactions per second, exceeding the KPI by 50%, with a 2s median transaction time.
- Further testing of the core infrastructure demonstrated scalability to at least 325 thousand retail payments per second, equivalent to 2 million bill transactions per second, with a 0.6s median end-to-end transaction time per payment.

Identity. The work stream also explored whether and how this blockchain solution could be combined with existing digital identity (e-ID) and digital signature components[3] for user authentication and authorisation in remote transactions.

The experiment involved integrating the Estonian and Spanish eID systems and certificates with the CBDC system and exchanging €-CBDC tokens in peer-to-peer transactions both within one single jurisdiction and across two EU countries. This exercise showed that eIDAS-compliant eID solutions and certificates could support the core principles and key requirements of a digital euro like privacy,

[1] https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

[2] https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf

[3] eSignature solutions were only explored from a conceptual point of view.

safety, accessibility and market neutrality; positively contribute to meeting several policy goals like limits, tiered remuneration or direct allowances to the general public; and streamline the onboarding process.

Conceptual analysis of identity included a review of the current status of how eIDAS is implemented in the EU and highlighted potential interoperability constraints. The use of waterfall, remuneration options and programmable money scenarios was studied as an analytical exercise. The analysis concluded that alongside the potential benefits of using eID for CBDC, several important obstacles remain. The European Commission's proposed update to the eIDAS regulation may help address some of these obstacles.

Privacy. Work stream 3 further looked into how different degrees of privacy could be afforded to different parties such as counterparties, core ledgers, operators, and account or wallet operators under different deployment models, and assessed the implications of these models for compliance with regulations on AML and combating the financing of terrorism (CFT).

While it appears technically possible to offer a fully anonymous CBDC, this would come with unacceptable trade-offs in terms of control over money-laundering, terrorist financing and other criminal activities. The benefit of a value instrument such as the digital bill-based system tested here lies in the large range of deployment models that could offer greater privacy than existing payment rails or accounts held at the central bank, but still make it possible to carry out AML and compliance functions. A conclusion of this experiment is that the choice of privacy configuration is primarily a question of policy and regulatory requirements.

Different privacy scenarios and configuration options for this CBDC system were analysed, with the aim of exploring different privacy scenarios that could represent use-cases for this technology, and to assess whether AML could be conducted while still preserving privacy. The privacy and auditability analysis concluded that this CBDC system enables a particularly broad range of privacy deployments, with AML possible even in relatively decentralised ecosystems where users hold their own wallets.

MAIN OBJECTIVES OF THE EXPERIMENT

The goal of the research project is to evaluate the feasibility of a digital euro issued and operated on a blockchain-based architecture. A CBDC system based on an existing blockchain platform and using digital bills was used to answer questions about CBDC functionality, scalability, privacy and compliance, and the use of electronic identity (eID) with it. The context for the experiment is the blockchain technology used by the Estonian government since 2012 and a research project launched In October 2020 to investigate how it could be used to support retail CBDCs.

The project is organised around answering three main questions:

i) Can the CBDC system evaluated deliver the functionality and scalability required for the digital euro?

ii) Can existing eIDAS-compliant national eID and eSignature solutions be integrated with this system to address the needs of a digital euro?

iii) What are the privacy configuration options for the system and their implications for users and AML?

An instance of this CBDC system was deployed for the purposes of the experiment alongside dedicated performance testing infrastructure, several end-user applications running on existing external e-ID services, and a consolidated custody layer facilitating interoperability between end-user applications. This setup simulated an end-to-end central bank money system covering payment, store of value, intermediaries, and end-users identified using eIDAS-compliant electronic IDs or certificates.

Scalability and settlement time are key considerations for a digital euro platform. Users expect final settlement of their payment to be instantaneous. Retail payment infrastructures must today support thousands of transactions per second, but this number may grow significantly as micropayments, and automated and machine-to-machine payments become more common. The project aimed to assess the current and potential scalability of this novel blockchain-based architecture for CBDC.

When issuing the digital euro, central banks need to take account of the strong public interest in privacy while complying with applicable regulatory frameworks on money laundering and terrorist financing. With this goal in mind, the project aimed to analyse different possible levels of privacy offered by the technology, with particular reference to its ability to perform AML functions.

Many of the policy choices being considered for a digital euro will require access to user identities or attributes, imposing additional friction and overhead. Successfully integrating a digital euro with existing and future eID and eSignature schemes may help smooth the adoption of a digital euro. The project aimed to investigate how feasible this integration could be.

A NEW SOLUTION FOR CBDC

The solution tested is a purpose-built infrastructure for operating a CBDC. It uses a bill-based or value-based CBDC money scheme on top of an existing blockchain architecture.

The system is built on two design choices:

Scalable and provable blockchain. The system operates a standalone instance of an existing blockchain technology that allows it to achieve security and resilience. The system claims strong security and cryptographic properties as the correct operation of the system as a whole is provable in real-time, which makes it secure against both internal and external attacks on the integrity of the system and allows continuous mathematical verification of the total money supply. The system is designed to be resistant to potential attacks by quantum computers.

Digital bills. The system instantiates value in “digital bills”, which are data structures that contain a nominal value, serial number, ownership information and a cryptographic proof verifiable against the blockchain. Each bill has its own ledger that tracks its history of ownership and is cryptographically anchored in a publicly available blockchain ledger.

Digital bill with basic properties:

- Fixed nominal value
- Serial number
- Cryptographic proof

Each bill is its own ledger which tracks ownership over time

Digital bills can be issued in an arbitrary range of denominations. In the experiment they were issued in a range from 1 cent to 200 euros.

Digital bills contribute to the creation of a highly scalable money system. Payments can be conducted in parallel on each bill ledger without the need for coordination between ledgers. This should allow the system to scale linearly, meaning it can maintain a consistent throughput rate proportionally as resources are added to the system, and so cover high transaction volumes.

The system consists of a blockchain machine that updates the ledgers for individual bills and commits payments to the blockchain ledger; input and output components that process payment orders and return cryptographic proofs of bill ownership; and a control unit that manages money supply and controls the correct operation of the CBDC system.

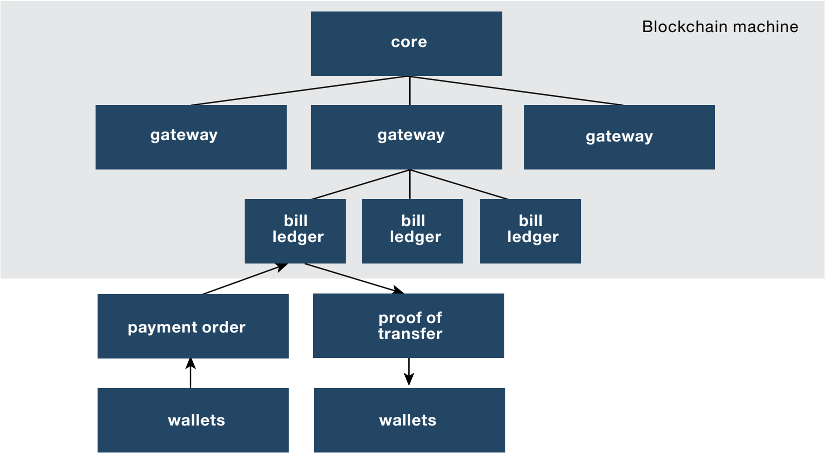
Bill ledgers are grouped together in partitions known as gateways. A gateway is a logical machine that maintains the current state of its bills and verifies payment orders before executing them. A gateway produces new blocks and proofs that are added to the bill ledger.

New bills are emitted in batches by the central bank following a pre-defined process, which includes the creation of an emission record. Newly emitted bills are initially moved to a wallet controlled by the central bank, from which they can be distributed. Removal from circulation follows a similar logic, as bills are moved to a write-only wallet held by the central bank, from which they cannot be spent.

Payment. A payment is a transaction that changes the ownership of one or more bills.

Upon receiving a valid and properly signed payment order for an individual bill, the gateway updates the ledger for that bill. A cryptographic hash of the bill is committed to the core, which is updated in discrete time periods called rounds.

Figure 1. The Blockchain machine processing a payment



All transactions processed by the system are settled with finality to the core blockchain within the timeframe of the transaction. Settlement occurs on one tier and to a single ledger, so there are no payment channels, or layer-two or lightning networks, nor is there any need to validate settlement against specific nodes or shards. After each round, cryptographic proofs of updated bill ownership can be verified by any party. Bills contain proofs of payment of 2.4kB that are locally verifiable in under one millisecond.

The system settles transactions with finality at the level of the individual bill. For a multi-bill transaction, a check for completeness can be performed at one of multiple possible points in the process: by the payer, if they are forwarding bill proofs to the recipient; by the recipient; or by a notification module in the output component, as part of a specific transaction schema layered on top of the core ledger. During the pilot, checks of completeness were conducted by the custodial layer (described below).

Transactions, interfaces between back-end infrastructure and intermediaries

Possessors of digital bills interact with the system through an API. Users are required, either directly or through a custodian, to maintain a private key or similar identity attribute that allows them to generate valid payment orders.

End-users do not need to interact with or even be aware of the bill structure. They can see their overall holdings and payments categorised in an account-like view. An exchange service at the level of back-end infrastructure ensures that a correct payment is made when users do not have the appropriate combination of bills in their wallet, by enabling wallets to change the denominations of bills so that wallets can transact in arbitrary sums.[4]

A CBDC system using digital bills resembles cash in a number of ways:

- There is a clear separation of roles between issuing money and holding wallets or accounts. End-users can have a direct claim against the central bank without necessarily having a customer relationship with the central bank.
- Control over the asset is a function of controlling cryptographic keys, and not of identity. There is no functional need for the operator of the core ledger to identify asset holders. This allows for a functional separation between issuance and settlement of CBDC claims and supervisory functions like AML and KYC.
- A bill deterministically can belong to only one owner at any given point in time, meaning that double-spending is impossible by design.
- The money supply is strictly controlled by the central bank as no money is created or destroyed during the processing of a transaction. New bills can only be issued by the operator of the system, which is the central bank.[5]

PERFORMANCE TESTING

During the project, the system was subjected to a set of tests to assess whether it meets the KPIs for the digital euro, and to further tests to assess its scalability and performance and to validate the theoretical properties of the bill systems described above.

The CBDC system was tested against the following KPIs. The deployment was optimised for the effective resource usage needed to meet the KPIs:

[4] The impact of the exchange service on system performance was assessed during the experiment. The optimal usage of the exchange service depends on the use-case. Unlike physical wallets, a digital wallet can actively manage its contents and be ready for anticipated payments.

[5] Verification of the proof for a bill includes steps verifying that the bill belongs to an emission of money carried out by the central bank.

Throughput and scalability: the PoC is able to process the equivalent of 10,000 payment orders per second (1B per day) assuming 100 million wallets

Settlement latency (processing time per transaction): a KPI of 95% of transactions processed within 5 seconds and 99% of transactions processed within 10 seconds

Resource and carbon footprint: a qualitative assessment demonstrating that the ledger technology could be resource and environmentally efficient

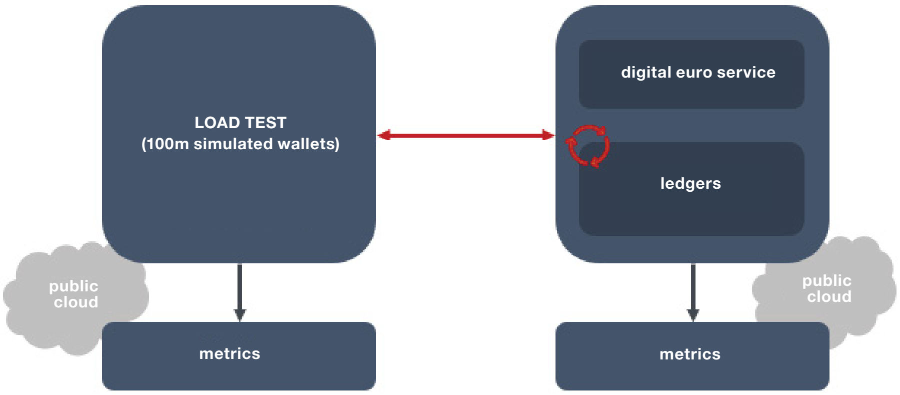
Availability: The system is able to perform 24/7 (no maintenance window, is updated live). Failure scenarios of one of multiple components are tested and recovery time is measured below 2 hours

A dedicated performance testing programme was deployed to generate load. The load generator simulated 100 million wallets, each consisting of a cryptographic key pair used to sign bill payment orders and a list of bills held by that key pair. Wallets selected the appropriate bills for each specific payment, interacting with the exchange machine that is part of the CBDC system if necessary. After payment was made with a specific bill, the recipient's wallet requested the corresponding bill proofs from the system and upon receipt verified these proofs.

Payment orders were generated following the characteristics of Eurosystem payments data. Payments were distributed along a log-normal curve between 0.01 and 200 euros, and generally consisted of multiple bills, with an average of 5.6 bills per payment. A load of 10,000 transactions per second entailed approximately 56,000 bill payment orders per second.

The CBDC system and the testing programme were both run on a cloud service. The load generation programme was run in the same region as the CBDC system but as a separate deployment, with communication between the two over https (secure hypertext transfer protocol). Network traffic between the two components was around 1900 megabits per second during load testing at 10,000 transactions per second.

Figure 2. Schema representing the performance testing deployment



Real-world testing. The test deployment comprised a number of elements that were designed to make testing as close to real-world conditions as possible. Inputs to the system were in the form the system would process in real-world use:

- The footprint of the system deployed comprised the elements of a CBDC system, with store of value, end-to-end transactions from user to user, and security elements including management of the amount of money in circulation.
- Security elements as payment orders were signed and verified. Payees were issued with cryptographically verified and verifiable proofs of their ownership of funds.

- Payment orders consisted of real-world amounts.
- Payment duration was measured from generation of the payment order in the wallet of the sender to the verification of ownership of bills by the wallet of the recipient, including network traffic between the load testing programme and the CBDC system.[6]

Scalability. The system was tested to a throughput of up to 15,000 transactions per second in a number of scenarios. Lengthier performance tests of up to one hour in duration were conducted at 10,000 transactions per second, or approximately 56,000 bill transactions per second.

Stress, scaling and variable load tests were used to assess the performance and resource usage of individual components and identify performance bottlenecks within the system. These tests confirm the hypothesis that the system scales to transaction volumes with a linear increase in the system resources required. Furthermore, no bottlenecks were evident in system components that would prevent scaling to significantly higher volumes.

Further testing of core components demonstrated the linear scalability of the bill-based architecture. Deployments of 25, 50 and 100 gateways allowed throughputs respectively of 250,000, 500,000 and 1 million bill payments per second. A maximum throughput of 1,960,000 bill payments per second was achieved.

No constraints to further scaling emerged at any volume of transactions. Throughout these tests, the core blockchain components operated at low load, and there is no practical limit to the number of bill ledger gateways in operation.

Figure 3. The system processing a load of 10–15 000 retail payment orders per second in the full testing setup

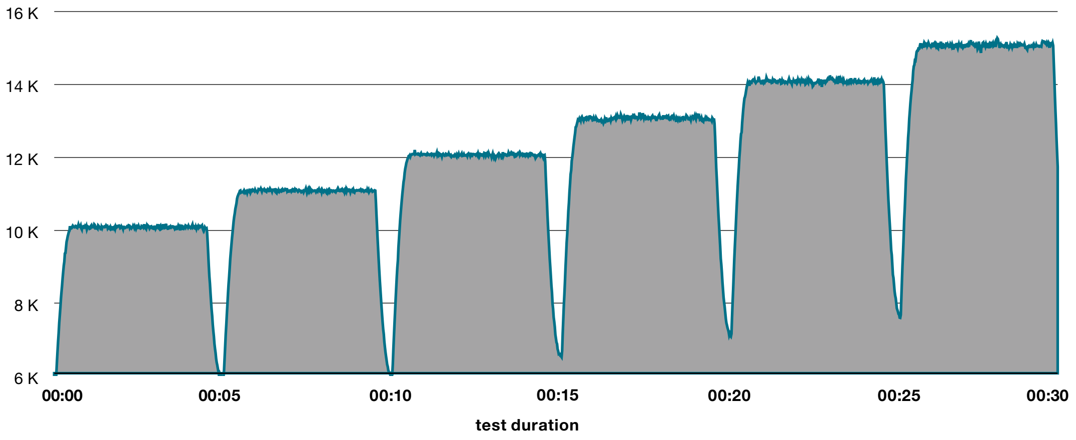
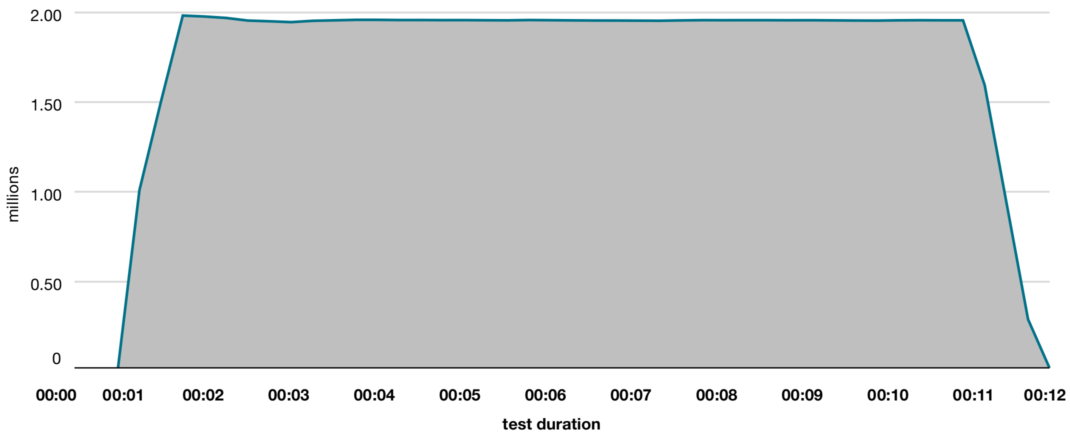


Figure 4. Core components operating 200 gateways at a volume of 1.96 million bill payments per second



[6] These were both deployed in the same public cloud, so network traffic had to travel a relatively short distance.

User numbers. Testing was in general conducted with 100 million wallets. Tests with smaller numbers of wallets at 1 million and 10 million confirmed that the number of users did not have a noticeable impact on settlement time or throughput.

Transaction time. During load testing at 10,000 TPS, transactions were completed in a median time of 2.4s. In tests at lower volumes, this time was 1.8s. The baseline time for guaranteed processing of a payment order in the present configuration was 1.441s.

In subsequent experimentation, the system was further optimised, with the duration of rounds of the core blockchain lowered from 1s to 200ms. Load tests were re-run, achieving a result of 0.6s median transaction time, with 99.65% of payments conducted in under 2 seconds.

NOTE: The results for payment duration reported are for the end-to-end transaction time from payer wallet to payee wallet and include network latency between the performance testing and CBDC infrastructures. Settlement time to the blockchain is not reported separately, but by design occurs within this timeframe. The system is unable to generate new proofs of bill ownership for the payee before the transaction has been settled to the blockchain.

Resilience. The testing protocol called for one of several components to be taken offline and then restored. During testing, a gateway component was taken offline and then restored. Restoring the gateway took between 6 and 12 minutes depending on the size of the gateway. The system was also run for an extended period of 24 hours at a load of 575 transactions per second without incident.

Footprint. An indirect assessment of the carbon footprint of the system under test yields emissions of 31 tonnes of CO_2e per year.[7] At a rate of 10,000 transactions per second, the carbon emissions per transaction are approximately 0.0001 g/CO_2. Per-bill transactions costs are about one fifth of this amount.

Analysis:

As a whole, the performance tests prove the technical feasibility of using this particular blockchain-based system as the infrastructure for a hypothetical digital euro. Such a system is able to scale to meet the performance requirements of a Eurosystem-wide payments platform and can do so in a manner that is resilient and environmentally efficient, and that requires modest computational resources.

PRIVACY

The project conducted a conceptual and empirical analysis of how the CBDC system being evaluated could support a variety of approaches to privacy and AML. A general conclusion of the analysis is that the system supports the separation of transactions from identity, which allows for significantly greater granularity and flexibility in designing privacy protections into the CBDC system.

The system supports the deployment of a CBDC in a layered architecture that allows knowledge of the end user's identity and transactions to be separated between different parties or layers in the system. A variety of privacy-enhancing techniques can be used to protect the identity of the user from the counterparty, ledger operator and wallet operators.

Bill ledgers, like UTXO[8] based schemes, also have some unique characteristics such as being able to cluster seemingly unlinked pseudonyms to the same owner. The pilot deployment used a split custodial wallet, with user identification and payment origination handled in the user wallet and keys held in a custodial layer that is separated from the wallet provider. In this set-up, due diligence and suspicious transaction reporting should be performed by the custodial end-user wallet provider and payment operator together. The pilot deployment ensures a high degree of privacy against all parties except the end-user's wallet provider of choice, who is the account operator.

[7] Assuming a 14kW power requirement and a carbon mix intensity factor of 255 g CO_2e/kWh (the 2019 EU average, source: https://www.eea.europa.eu/data-and-maps/indicators/overview-of-the-electricity-production-3/assessment).

[8] Unspent Transaction Output or UTXO is the token exchange in multiple blockchains, such as Bitcoin.

The different privacy configuration scenarios provide a mosaic of different degrees of data access for the different entities involved, who are the public, the recipient, the payment operator, and the account operator. The analysis considered possible AML-obliged entities in each of the scenarios and how customer due diligence and suspicious transaction reporting could take place. In addition to the conceptual analysis, an empirical analysis also tested some of the proposed approaches using common machine-learning based AML techniques against test data. Simulation testing confirmed that AML procedures aligned with current regulations can be performed in a variety of configurations.

The privacy analysis was structured around two main questions:

- What are the possible privacy configurations in this system?
- What are the implications of those configurations from an AML perspective?

The answer to the first question required the privacy options that could be allowed within the constraints of this CBDC system to be analysed, together with their potential implications for the portability of accounts from one intermediary to another.

The privacy configurations depend on choices that could be taken for three different components:

- **Blockchain:** the ledger can be divided into different independent gateways that could be distributed. Only the party operating a gateway has access to bill ledger data. Gateway distribution could be used as a means of increasing privacy, as no agent will then hold all the information on all transactions.
- **Wallets:** there are two main configurations for the wallets. Either the wallet provider has the private keys of the user in the Custodial Wallet, which allows the wallet provider access to identity, balance and transactions, or the wallet provider does not have the keys, in the Personal Wallet, but can ask the user to identify themselves if they want to use the wallet.
- **Identity:** identification could be a requirement for using the wallets. The onboarding process could require that government-issued identities be used or could require no identification.

Another dimension to explore would be the behaviour of the parties involved in the CBDC ecosystem. These have been clustered under three scenarios:

- **Default:** users have one pseudonym and each bill stores the complete list of its owners.
- **Bill ledger pruning:** users have one pseudonym and only the information on the pseudonyms of the last two owners of a bill is stored in the ledger.
- **One-time address:** users have a different pseudonym for each transaction in which they act as a receiver, but each bill stores the complete list of previous owners as their pseudonyms.

Answering the question regarding the AML implications requires a broader conception of the obliged entities and the activities of customer due diligence and suspicious transaction reporting. AML procedures would largely depend on the wallet configuration and how it is integrated with user identification. There are three options for this:

- **Custodial wallet:** the wallet provider has access to the identity, the balances and the transactions of their customers. AML could be conducted in a similar manner to how it is currently. The wallet providers would be the obliged entities.
- **Personal wallet:** the wallet provider identifies users to allow them access to their wallet. However, it has no access to the ledger and has no information on user balances or transactions. The payment operator has access to the ledger and can perform analysis on anonymised data. Customer due diligence could be conducted by wallet providers, while suspicious transactions could be identified by payment operators. Suspicious transaction reporting would require wallet providers and payment operators to collaborate to file suspicious transactions reports. Wallet providers and payment operators would need to be obliged entities.

- **Wallet with no ID:** the wallet provider has no information on the user identity. The payment operator can run analysis on anonymised data but cannot link behaviour in the ledger to real identities. AML could not be conducted as user identification would not be feasible.

We present as a summary the main results in the following table.

Tabel 1. Summary of possible privacy levels and AML implications

Privacy Scenario	Wallet configuration	Public	Recipient	Payment operators	Wallet providers	AML
Electronic transfer	n/a	🟩	🟨	🟥	🟥	✅
Default	Custodial	🟩	🟨	🟥/🟨	🟥	✅
	Personal	🟩	🟨	🟥/🟨	🟨	☑️
	No ID	🟩	🟨	🟥/🟨	🟩	❌
Bill-ledger pruning	Custodial	🟩	🟨	🟥/🟨	🟥	✅
	Personal	🟩	🟨	🟥/🟨	🟨	☑️
	No ID	🟩	🟨	🟥/🟨	🟩	❌
One-time address	Custodial	🟩	🟩	🟨/🟩	🟥	✅
	Personal	🟩	🟩	🟨/🟩	🟨	☑️
	No ID	🟩	🟩	🟨/🟩	🟩	❌

Table 1: Summary of possible privacy levels and AML implications. [Privacy: Green: Information is held confidential from this party. Yellow: Information is partially confidential, so personal information cannot be retrieved but user transactions could be tracked from anonymous data, or personal information is known but data on transactions or balances are not for example. Red: Information is not held confidential from this party. The payment operator has two colours, as the result depends on the distribution of the gateways. AML implications: Green Tick: AML is possible. Blue Tick: AML is possible under some circumstances, depending on how gateways are distributed for example. Red cross: AML is not possible or not viable]

Recommendations in favour of a specific approach are beyond the scope of this analysis and depend on which policy considerations are followed and a detailed analysis of regulatory compliance.

The empirical and conceptual analysis shows that a personal wallet deployed with this CBDC system provides a good balance between privacy and auditability, but that the wallet provider would need to work in collaboration with the payment operator in order to be able to file a suspicious transaction report. AML processes would be more complicated and potentially not in line with current regulations. If custodial wallets linked to an identity service are used, the privacy level is similar to those of other electronic forms of payment and current AML procedures could be followed. The highest level of privacy would be achieved with wallets that do not register or validate the end user’s identity, but in this case, AML compliance would not be possible.

eID

This portion of the experiment tested the use of various digital ID solutions in end-to-end peer-to-peer retail transactions, identifying several operational, cost and compliance benefits to using eID. Further analysis identified some practical limitations that may be eased by an updated eIDAS regulation and the greater use of verifiable credentials or self-sovereign identity.

End-to-end user testing was conducted on the CBDC system, with peer-to-peer payments conducted between identified individuals employing different end-user solutions. The experimental setup made the following assumptions:

- **Users** are physical persons, authenticated using eIDAS-compliant[9] **eID** credentials or certificates issued by public authorities.
- **Intermediaries** hold a customer relationship with the user, operate a user interface or wallet, and are responsible for AML and KYC. Their role is similar to a PSD2 Third Party Service Provider, as they display balance and payment history, instruct payments, and conduct strong customer authentication.
- Assets, which are digital bills, are held in a **custodial layer** that links the identity of users to the cryptographic key or keys for their bills. The custodial layer presents an account-like view of assets accessible to end-users via intermediary end-user solutions.
- The **CBDC system** executes and settles digital euro payments in the relevant ledgers.

Estonian users were authenticated using a private app-based solution that combines eID and eSignature functionalities and can be integrated into any digital or mobile wallet. Credentials are issued by the Estonian Police and Border Guard, though the solution is also widely used in Latvia and Lithuania.

Spain used X.509 eIDAS-compliant certificates issued by a Spanish public body whose underlying credentials were loaded onto a self-sovereign decentralised global private identity solution accessed via a mobile application. This application allows users to manage these credentials themselves and exercise control over how they are shared with third parties.

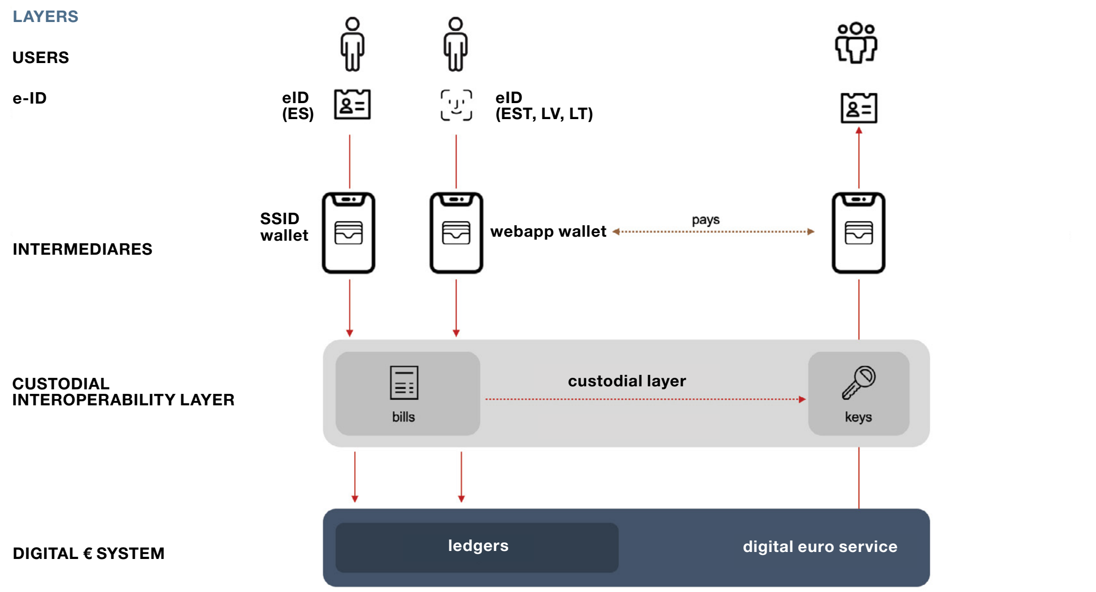
In the experimental setup, a custodial layer was deployed on top of the CBDC core ledger. This custodial layer keeps the cryptographic keys linked to individual digital euro bills, maintaining a link between these keys and the identity of their owner, and forwards payment notifications between wallets. In the experiment, OpenID Connect was used as a protocol to pass credentials from identity providers to intermediaries and the custodial layer.

End-users accessed their holdings by authenticating themselves to local end-user wallets, which passed those authentications on to the custodial layer. Users saw account balances and payment history, and could make payment orders through their mobile wallets, as is the case with current e-money and commercial bank money solutions. The ability of users to access their holdings was tied to their identity and was independent of the end-user application they were using.

[9] Regulation (EU) No 910/2014 on electronic identification (eID) and trust services (eSignature for natural persons and eSeal for legal persons) for electronic transactions in the internal market. eIDAS also regulates other trust services such as timestamping.

Although the case for P2B, B2B and B2P digital euro payments is strong, the workstream was aware of the additional complexities associated with identifying legal persons like the choice of applicable identifiers and their relevant attributes, and of the limited time for experimentation. It consequently decided to focus its efforts on the P2P sphere.

Figure 5. High-level end-to-end transaction flow in the experimental deployment of the PoC



Using eIDs can reduce the total friction and cost of deploying a digital euro. The benefits of linking claims on digital euros to digital identity include:

- Less onerous and expensive remote customer onboarding, with some elements of remote KYC analysis, as an eID may contain attributes used in KYC analysis that would otherwise need to be determined independently.
- Facilitation of customer switching across PSPs without the link being lost between a person's identity and their digital euro bills[10].
- Strengthening of the direct, cash-like nature of the claim against the central bank as it is independent of intermediary default or insolvency.
- Support for more effective operational and policy controls on the use of the digital euro.
- Direct use of certificates issued by public authorities, which introduces a high degree of legal certainty and confidence in the identification of end-users.

Private and public eID solutions at national level work well for Strong Customer Authentication (SCA). Where eIDAS-compliant eID or eSignature solutions exist and are widely used, no new SCA solutions would be needed, as the existing solutions could be used for both customer authentication and payment authorisation. This could then lower the cost of a CBDC rollout and remove a barrier to entry for intermediaries, who would no longer need to set up their own SCA infrastructure.

The current setup of the experiment and the use of existing eID and eSignature solutions facilitated strong customer authentication for login and access to cryptographic keys, which were used thereafter for authorising payments. Payment order information is stored, and can be timestamped, together with cryptographic keys linked with eIDs.

For the authorisation of digital euro payment transactions, conceptual analysis showed that advanced and qualified electronic signatures as regulated under the eIDAS regulation can, in principle, meet the expectations of the legal framework. However, the CBDC system would need to use the eSignature

[10] Since the identification elements used are independent of a single PSP; in the experiment setup the custody layer links a person's identity to bills by issuing a unique identifier that allows the user to be onboarded into another end-user solution, authenticates towards the custody layer with its eID solution, and gets access via the new end-user solution.

solutions in a way that ensures they comply with the practical requirements derived from the PSD2 and its accompanying Regulatory Technical Standards (RTS).[11] This means that payment orders would be sealed and timestamped, as this would prevent changes being made to the original payment order authorised by the payer.

The experimental deployment reflected a relatively centralised approach to managing cryptographic keys for value-based CBDC, which was functionally equivalent to holding individual CBDC accounts on the central bank's ledger. However, keys could also be held in custody by intermediaries or by the end-user. The potential benefits and drawbacks of this setup remain to be explored.

In any case, the centralised approach tested offers several benefits: it maintains a high degree of central bank oversight; it facilitates interoperability between end-user wallets for making and receiving payments across the EU; it allows switching of end-user wallet providers if the intermediary becomes unavailable as eID can be used with another wallet provider to access the custodial layer and the cryptographic keys to the bills; and it is in theory open to legal persons and non-EU residents, as the custodial layer uses unique identifiers based on the onboarding process of the end-user wallet provider.

In this setup, licensed intermediary end-user solution providers remain responsible both for AML and KYC activities and for providing payment services. This means they can compete for clients upstream without compromising interoperability downstream.

The experiment identified challenges that require further consideration:

Seamless user experience. Multi-factor authentication can impede a fast and seamless user experience. In the current experiment, users were required to go through an extra step for two-factor authentication before completing a transaction. The experiment identified perspectives for further work on this, particularly for machine-to-machine payments.

Identities accredited using the current **eIDAS standard** alone do not contain sufficient information to automate all the AML and KYC checks.[12] It may be necessary to access additional information, either for reasons of AML or KYC or because of specific policy rules such as holding limits. A national eID may for instance not be sufficient for determining whether a given person is a euro-area resident, as it may not provide incontestable evidence of the current address of the individual, since the address shown in a national ID may not be up to date. Other potential alternatives such as population registers, electoral registers or tax rolls might help address these shortcomings, but a lack of standardisation or the potential exclusion of certain groups like foreign students may prove important limitations.

One practical approach to this issue could be to require an updated proof of address as part of the authentication process every time a payment transaction with the digital euro is initiated. The choice of accreditation that is considered valid evidence of address may vary by jurisdiction. The cost and operational implications of this approach need to be explored further.

Moreover, **pan-European uptake of national eID schemes notified under the eIDAS regulation appears to be very limited** in practice because the interoperability of national eIDAS nodes is only partial[13], national eIDs have a modest footprint[14], and there is quite a narrow range of public and private services that these nodes connect to.

[11] Due to time constraints, the experiment could not address alternative configurations such as using eIDAS eSignatures for PSD2 SCA at the level of end-user wallets or applying eSignatures for payment authorisation at the level of the back-end infrastructures.

[12] For example checks to determine whether a client is a politically exposed person or to determine the origin of the funds.

[13] Full coverage would imply a matrix of 27 x 26 / 2 connections. According to a report by Eurosmart, in June 2020, the extent of operational connections was limited due to legislative and technical obstacles. A review of the state of the connections shows 8 Nodes are still not operative, while the working Nodes have connections with few or no other Nodes or with a maximum of 18 (see https://www.eurosmart.com/recommendations-for-an-improved-application-of-eidas).

[14] Only 15 of the 27 Member States have so far notified the EC about national eID schemes under the eIDAS regulation.

Another notable shortcoming is the **exclusion of non-EU citizens because there is no mutual recognition of eID schemes outside Europe**. As a result, existing eIDAS-compliant eID solutions could potentially fall short in meeting the Eurosystem's policies and objectives, in particular the core principle that the digital euro be widely accessible.

The newly proposed European Digital Identity Regulation may help address some of these issues.[15] Member States are to be required to offer their citizens identity wallets that enable the user to request, store and share identification data and electronic attestations of attributes. These identity wallets, which could be provided by the private sector, will operate on a set of common standards that will be defined by the European Commission.

This approach could move in the direction of self-sovereign identity (SSID) solutions, which permit a user to present multiple attributes and credentials that have been verified by a trusted third party. SSID solutions exhibit a potential that could partly address some of the challenges identified. In addition, deploying decentralised identity (DID) services in combination with SSID may allow for greater efficiencies, as multiple attributes and identity claims issued by trusted institutions could be aggregated to potentially satisfy more rigorous AML and KYC checks. This may help address the current lack of harmonisation and uptake of national eID schemes and provide a means for users to make adequate information or attributes easily available for purposes like AML checks.

[15] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663