EUROPEAN CENTRAL BANK

EUROSYSTEM

IN FOCUS I Issue no 4 I December 2019

Exploring anonymity in central bank digital currencies

EUROPEAN CENTRAL BANK

EUROSYSTEM

Exploring anonymity in central bank digital currencies

Executive summary

The ongoing digitalisation of the economy represents a major challenge for the payments ecosystem, requiring that a balance be struck between allowing a certain degree of privacy in electronic payments and ensuring compliance with regulations aimed at tackling money laundering and the financing of terrorism (AML/CFT regulations). Under the coordination of the ECB, the European System of Central Banks (ESCB) has established a proof of concept for anonymity in digital cash – referred to here as "central bank digital currency" (CBDC).

That proof of concept is part of the ESCB's ongoing technical research on CBDC and the aim is to contribute to the broader discussion on the topic. The work carried out is not geared towards practical implementation and does not imply any decision to proceed with CBDC. The ECB will continue to analyse CBDC with a view to exploring the benefits of new technologies for European citizens and in order to be ready to act should the need arise in future. The prospect of central bank initiatives, however, should neither discourage nor crowd out private market-led solutions for fast and efficient retail payments in the euro area.

The proof of concept drawn up by the ESCB demonstrates that it is possible to construct a simplified CBDC payment system that allows users some degree of privacy for lower-value transactions, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks.

That proof of concept boasts several novel features developed by the ESCB's EUROchain research network (with the support of Accenture and R3) using distributed ledger technology (DLT). It provides a digitalisation solution for AML/CFT compliance procedures whereby a user's identity and transaction history cannot be seen by the central bank or intermediaries other than that chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional checks are delegated to an AML authority. This is achieved using "anonymity vouchers", which allow users to anonymously transfer a limited amount of CBDC over a defined period of time.

Although there is no immediate need to take concrete steps towards the issuance of CBDC in the euro area, the proof of concept will be instrumental in any assessment of (i) how CBDC could work in practice and (ii) how the specific technical features of such an initiative will affect its potential implications for the economy.

EUROPEAN CENTRAL BANK
EUROSYSTEM

EUROchain

Research Network.
A network of
knowledge and exploration

The world's first DLT research network between a large group of central banks.

WHAT WE FOCUS ON

DLT solutions in the field of market infrastructure and payments, leveraging existing central bank services

Securities settlement

Retail payments

WHO WE ARE

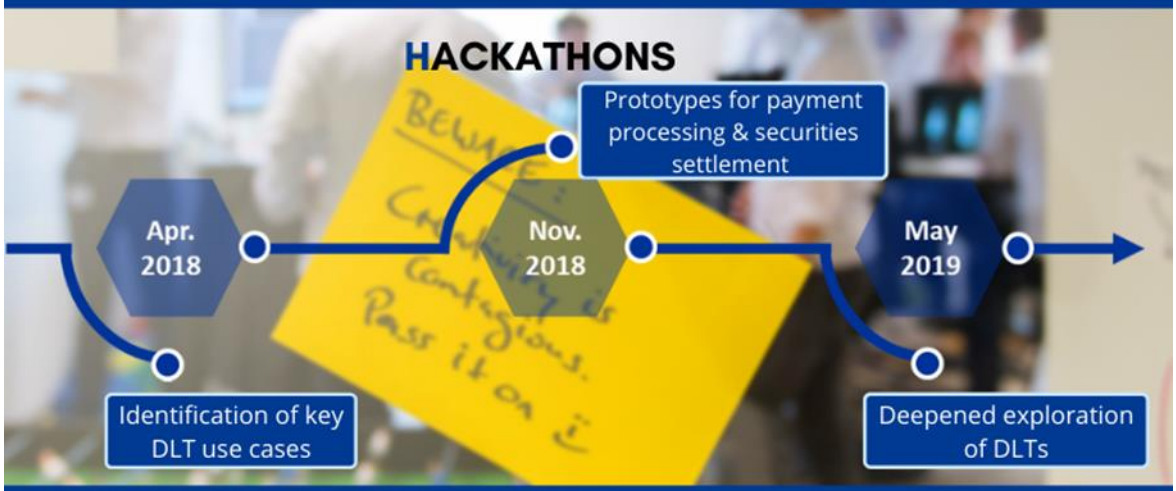
ECB Innovation Lab: a cross-functional team of payments specialists and IT colleagues at the ECB.

Expert network: colleagues from 18 national central banks with knowledge of financial market infrastructure who are involved in local market networks

HOW WE WORK

Research → **Explore** → **Test** → **Validate**

HACKATHONS



1 Introduction

Against the background of the ongoing digitalisation of the economy, the payments ecosystem needs to find an answer to an issue that concerns all citizens: the question of how to allow some degree of privacy in electronic payments, while still ensuring compliance with AML/CFT regulations. The proof of concept that has been developed by the ESCB's EUROchain research network proposes an answer to that question for CBDC.[1] The EUROchain research network seeks to foster a common understanding of DLT and gain practical experience of such technology.[2]

The main thing that this prototype shows is that, in a simplified environment typical of a proof of concept, DLT can be used to balance an individual's right to privacy with the public's interest in the enforcement of AML/CFT regulations.[3] It provides a digitalisation solution for AML/CFT compliance procedures whereby a user's identity and transaction history are nevertheless hidden from the central bank and intermediaries other than that chosen by the user.

This finding is particularly relevant in the context of central banks' ongoing analysis of the economic and societal impact of issuing CBDC. Indeed, while the question of whether or not to issue CBDC is still primarily a policy matter, that question cannot be answered without a deep understanding of the various specific design features that a CBDC could have. This report seeks to contribute to wider discussions on the potential use of DLT in the issuance of CBDC. It should be noted that the work carried out is part of the ESCB's wider technical research on CBDC, is not geared towards practical implementation and does not imply any decision to proceed with CBDC.

The IT architecture supporting the proof of concept has been developed in cooperation with R3 and Accenture, building on the functionalities of the Corda platform. Other proofs of concept have been developed by EUROchain in the past, and that work will continue in the future.

This report describes the use case that is addressed by this initiative (see Section 2), as well as the proof of concept (see Section 3), before going on to describe the

1 For the purposes of this report, "CBDC" is a central bank liability that is made available to individual citizens in digital form. Some authors use the term "general-purpose CBDC" in order to distinguish such digital currency from "wholesale CBDC", which is only available to specific types of entity, such as banks (see, for example: BIS, "Central bank digital currencies", March 2018).

2 EUROchain was set up by the ECB as a learning tool for Europe's central banking community. There are currently 18 national central banks taking part in this voluntary initiative (those of the Austria, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Portugal, Slovenia, Spain and Sweden). Cooperation within EUROchain takes various forms, including hackathons where business and IT experts work together to establish proofs of concept.

3 A distributed ledger is a record of information or database that is shared across a network. It can be used to record transactions, with no need for a central party to validate them. One type of DLT technology is "blockchain", which stores all transactions in groups, or blocks, which are attached to one another in chronological order using cryptography to ensure the security and integrity of data. This chain forms a register of transactions that users consider to be the official record (see Pinna, A. and Ruttenberg, W., "Distributed ledger technologies in securities post-trading: Revolution or evolution?", *Occasional Paper Series*, No 172, ECB, April 2016).

various lessons that have been learned in this regard and a possible way forward (see Section 4).

2 Use case

The proof of concept is based on four main principles:

- First, it is assumed that CBDC has **cash-like features**. There is strong emphasis on users' privacy for lower-value transactions, and balances are not remunerated.
- Second, the design is **built around intermediaries** in a two-tier model. Rather than on-boarding and servicing CBDC users directly, the central bank relies on intermediaries that have access to central bank accounts and can draw on reserve balances held at the central bank to provide CBDC to users. Intermediaries process transactions on behalf of their clients and offer them custodial services.
- Third, the **central bank** is the only entity that is allowed to issue CBDC units and remove them from circulation.
- Fourth, a **dedicated "AML authority"** performs AML/CFT checks. That authority checks the identities of users involved in large-value transactions and prevents CBDC from being transferred to embargoed users.

3 Description of the proof of concept

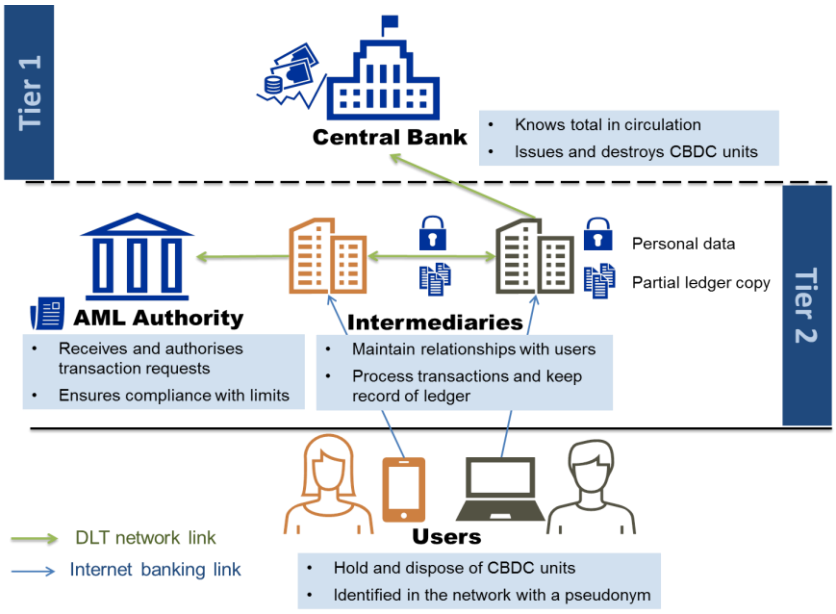
The proof of concept has been developed using Corda. Corda is a DLT platform which is designed to ensure that the information that is held locally by two users, which store details of their bilateral transactions, is consistent with the overall information stored in the system (without that information being shared with other users).[4] The proof of concept features four entities (two intermediaries, one central bank and an AML authority – each represented in the network by a node that operates a CorDapp[5]), an intuitive web application allowing interaction between users, and a set of application programming interfaces (APIs) allowing communication and interaction between different parties (see Figure 1).

[4] Thus, a user cannot, for example, spend the same CBDC unit in two different transactions with two different payees

[5] This logic enables assets to be transferred between entities.

Figure 1

Two-tier model and relationship between entities



Source: ECB

CBDC units in Corda and usage model

CBDC units are represented in the ledger by Corda "states".[6] Every state contains information on its value, details of its past and current owners, and cryptographic proof of its validity – i.e. proof that, since its issuance, it has always been transferred in accordance with the rules laid down by the central bank.

States in Corda follow the unspent transaction output (UTXO) model, whereby every transaction consumes one version of a state and triggers, in the same ledger, the creation of a new version that can be used in a subsequent transaction. At any given time, only state versions that are unspent, and whose previous versions have been spent in accordance with the rules of the system, can be accepted by payees. In the proof of concept, it is ultimately the responsibility of the payee's intermediary to ensure that the states which are received by its client are valid and can be redeemed with the central bank on demand.

In the proof of concept, a special node called a "non-validating notary" allows intermediaries to check the validity of states by maintaining a registry of all currently valid UTXOs. To protect users' privacy, the notary has no access to data such as transaction values, users' addresses or states' histories.

Rules governing transfers of states between parties are kept to the minimum that is necessary to avoid double-spending and implement AML constraints set by the system. At the same time, all entities are able to apply additional rules of their own

[6] A state template (the "Token SDK" – with SDK standing for "software development kit") provides standard definitions and patterns for the representation of assets in a Corda ledger.

choosing (while maintaining adherence to those core rules) and can, in essence, turn CBDC units into "programmable money".

Users' addresses

Each user is on-boarded by an intermediary, which provides its clients with pseudonymous identities that are used as network addresses for CBDC payments.

Anonymity vouchers

In order to enforce AML/CTF limits on the amount that a user can spend without the AML authority seeing transaction data, a novel new concept – "anonymity vouchers" – has been devised. The AML authority issues these additional, time-limited states to every CBDC user at regular intervals.[7] If users want to transfer CBDC without revealing information to the AML authority, they need to spend these vouchers (at a ratio of one voucher per CBDC unit transferred). Thus, the amount of CBDC that can be spent anonymously is limited by the number of vouchers that the AML authority provides to each user.

Although vouchers are technically "spent", they are issued free of charge and are not transferrable among users. They are simply a technical tool used to limit the amount of CBDC that can be transferred anonymously. This means that limits on anonymous CBDC transfers can be enforced without recording the amount of CBDC that a user has spent, thereby protecting users' privacy.

Issuance and distribution mechanisms

When an intermediary receives a CBDC issuance request from a client, it checks that the client's post-transaction CBDC balance will remain below any wallet cap that it may have set. If that is the case, the intermediary requests CBDC units from the central bank on behalf of its client.[8] This means that the issuing central bank does not limit the supply of CBDC in a way that could lead to excess demand from its users, since limits are only applied at the level of each individual wallet. Conversion to and from CBDC always occurs at a ratio of one-to-one, to ensure that CBDC has the same value as alternative forms of the same currency.[9] The central bank debits the intermediary's reserve balance[10] and authorises the creation of new CBDC units by approving (thus "signing") the issuance request through its node. The new units

[7] The current prototype suggests that a limited amount of vouchers should be distributed each month, regardless of account balances.

[8] In exchange, the intermediary will draw down its reserve balance held at the central bank by the face value of the CBDC units.

[9] This is similar to what happens with commercial bank money, electronic money and physical cash.

[10] The link between the CBDC system and the real time gross settlement (RTGS) system where intermediaries hold their reserves of central bank money is simulated by a local service where information on the balances of commercial banks' accounts with the central bank is stored.

are then added to the original client's CBDC account, and that client's account with the intermediary in private money is debited by the same amount.[11]

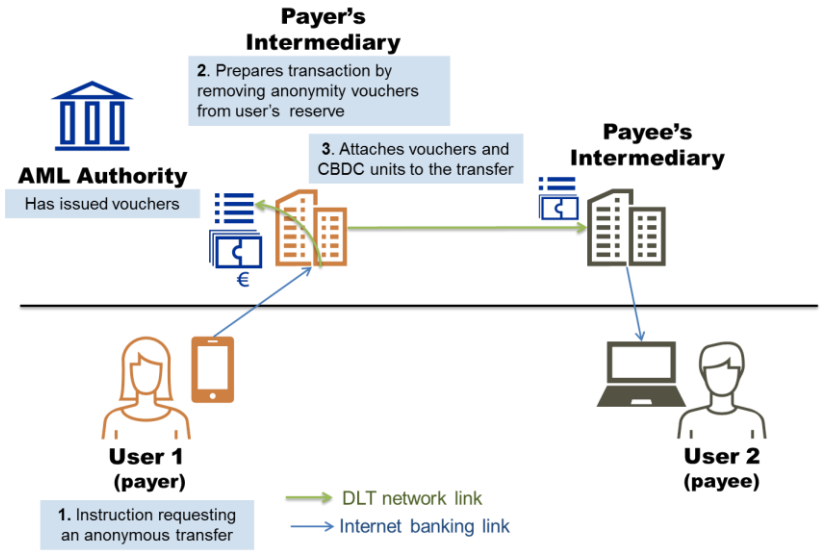
Transfers

Transfers of CBDC units take place without any involvement on the part of the central bank. A payer sends a CBDC transfer instruction indicating the amount, the pseudonym of the payee (account identifier and intermediary identifier) and whether or not the payment should be made anonymously. If this is the first time that the payee has received CBDC units from the payer's intermediary, the transfer starts with a look-up request by the payer's intermediary in order to obtain the payee's address from its intermediary.[12] The intermediary's node then initiates the transfer by following a process that varies depending on whether the AML authority is involved in the transaction. The transfer mechanism allows for AML checks by intermediaries, but it largely safeguards confidentiality.

The transaction can be accepted by the payee's intermediary with no need for approval from the AML authority if the payer has a sufficient number of anonymity vouchers and asks to use them (see Figure 2). In that case, the payer's intermediary removes the necessary vouchers from the user's reserves and attaches them to the transfer of CBDC, to prove to the payee's intermediary that the transaction can be validated without checks being carried out by the AML authority.

Figure 2

Transfer with anonymity vouchers



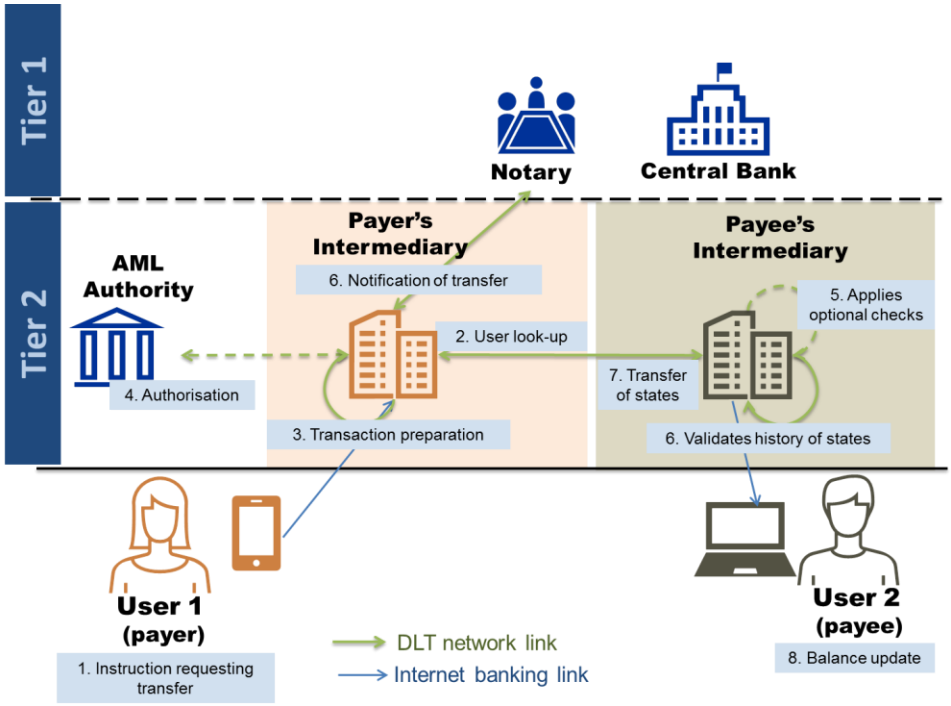
Source: ECB

11 "Private money" refers to money that is held in an account with the intermediary, constituting a claim on that intermediary, rather than the central bank.

12 This process is based on Corda's "confidential party" mode, which enables states to be assigned to an end user by using a one-time key that does not reveal directly the user's pseudonymous identity, thereby reducing privacy concerns

If a payer chooses not to use vouchers or does not have enough vouchers available (see Figure 3), its intermediary will prepare the transfer and route it via the AML authority, sending additional information on the payer for the necessary AML checks. On the basis of the information provided, the AML authority will either approve or reject the transfer.[13] The payee's intermediary will only accept the payment if it is approved by the AML authority.[14]

Figure 3
Transfer with AML checks



Source: ECB

Limits on the amount of CBDC that can be transferred in a given period of time and caps on the CBDC holdings of individual users are enforced at the level of individual intermediaries, which will be driven to reject transactions that infringe AML/CFT requirements by (i) respect for the rule of law and (ii) financial incentives (since they will not be able to redeem CBDC units at the central bank if those units have been transferred illicitly at any point in time). It should in this context be noted that limiting the amount of CBDC at the level of individual wallets would indirectly allow the overall CBDC volume to be controlled if for example the number of wallets per citizen and the usage by non-citizens were restricted.

13 Rejection is automatic in the proof of concept and is based on text-matching rules.

14 If the CBDC transfer were to be accepted without approval from the AML authority, the payee would be unable to reuse those CBDC units, since it would be clear from their history that they had been transferred in breach of system rules, and the central bank would not recognise them as being valid.

Redemption

Users are able to convert their CBDC units back into other forms of currency by initiating a process through their respective intermediaries. When an intermediary receives such a request, it takes the requested amount of CBDC units from its client's wallet and marks them as spent. The intermediary then sends a request to the central bank to reclaim funds in the RTGS system and updates the balance of its user's account in private money.

4 Lessons learned and way forward

The proof of concept shows that it is possible, using the Corda platform, to build a simplified CBDC payment system that safeguards users' privacy for lower-value transactions, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks. However, that proof of concept also highlights a number of areas where there is room for improvement.

Reducing the amount of information visible to parties not involved in the transaction: one challenge that would need to be addressed is the impact of the transaction validation mechanism on confidentiality. In the proof of concept, intermediaries validating a CBDC transaction need to look at information on past transactions of the CBDC units being transferred, all the way back to the moment when they were first issued. Notwithstanding the data segregation model of Corda, a participant can therefore build a knowledge graph based on information collected from the CBDC units it receives over time. This means that details of past transactions can be seen by new holders' intermediaries that were not involved in those transactions. Nevertheless, no intermediary has a full overview of all network activities at any given point in time. The central bank knows the amount that is currently in circulation, but only obtains information on individual CBDC units and the pseudonyms of their holders when those units are redeemed. To some extent, this challenge can be addressed through the process of trimming the history of a state – referred to as "chain snipping". This is a technical procedure whereby an intermediary initiates the redemption of all CBDC units held in the accounts of its users and triggers the issuance of the relevant amount of CBDC for each user. By resetting the history of a user's units, an intermediary reduces the amount of information that is visible to other participants. However, that has no impact on the user's privacy vis-à-vis the central bank, which still receives all information carried by redeemed units.

Users' ability to access or spend CBDC balances when the intermediary is unavailable: the proof of concept could be enhanced to include an option allowing users to hold CBDC units and initiate transactions independently of their original intermediary. In the present version of the prototype, a technical failure on the part of the original intermediary will result in its users being unable to access their CBDC balance or spend (and, in some cases, receive) units. This issue could be mitigated by allowing users to sign transactions through keys stored in their own device (such as a mobile phone wallet) and enabling other intermediaries than the original one to

access the user's "back-up" CBDC units. Shorn of its custodial services, an intermediary would, in such a situation, be more akin to a transaction gateway, conducting services like "know your customer" processes.

Limiting the number of accounts per intermediary: the current prototype does not include a mechanism ensuring that users can only have one account with one intermediary. The decentralised implementation of such a solution is another possible area for investigation.

Adding privacy-enhancing techniques: privacy could be further enhanced by using mechanisms such as rotating public keys, zero-knowledge proof and enclave computing. Using rotating keys, which would involve users generating new pseudonyms on a regular basis, would limit nodes' ability to link transactions to individual users, since users would be using various different pseudonyms over time. At the same time, intermediaries would still be aware of all transactions initiated and received by their respective clients, and the AML authority would know the real identities of the payer and the payee whenever transactions without anonymity vouchers were sent for approval.

Interoperability with an RTGS system: moreover, the current proof of concept does not cover the link between the present prototype and the RTGS system. A validation procedure at that juncture would involve several additional steps. For instance, the payment would need to be confirmed before the central bank issued or redeemed CBDC units.

Practical functioning of the prototype: finally, the proof of concept focuses on concept and design rather than the functioning of the prototype and the efficiency of the prototype. Scalability of the prototype was for example not analysed.