DEUTSCHE
BUNDESBANK
EUROSYSTEM

Eurosystem experimentation regarding a digital euro

Research workstream on hardware bearer instrument

Content

Dieser Bericht wird von der Deutschen Bundesbank zu Informationszwecken veröffentlicht. Es setzt Schwerpunkte und erhebt deswegen keinen Anspruch auf Vollständigkeit.
Bei Fragen zum Bericht wenden Sie sich bitte an Frau Inga Schultze, inga.schultze@bundesbank.de oder Herr Marcus Härtel, marcus.haertel@bundesbank.de

Motivation

In the Eurosystem's Report on a digital euro[1] from October 2020, the High-Level Task Force on Central Bank Digital Currency (HLTF-CBDC) raised a number of questions about the design and features of possible implementations of a digital euro, and postulated a number of scenario-specific requirements and design possibilities. To investigate these topics, the HLTF-CBDC created various workstreams to experiment with different dimensions of a potential implementation of a digital euro.[2] One of these workstreams focused on the potential implementation of a hardware bearer instrument (HBI). This relates directly to two of the topics raised in the Report on a digital euro: (i) whether existing hardware solutions could be adapted for a digital euro or new specific solutions and standards are required and (ii) how could cash-like features could be made available and usable offline. The workstream included the Banco de Espańa, the Banque de France, the Banca d'Italia, the Deutsche Bundesbank, the European Central Bank, the Nederlandsche Bank and Suomen Pankki – Finlands Bank.

Project Scope

While work on ledger systems with different degrees of centralisation has been ongoing in the Eurosystem for many years now, a hardware bearer instrument (HBI) is a challenging technology that combines hardware and software expertise for the development of a physical device to load, transfer and make payments with digital euros. Despite early attempts, like cash preloaded cards, an HBI holding Central Bank Digital Currency (CBDC) can be considered a new technology. To obtain the best possible picture of the state-of-the-art of these physical devices, the Eurosystem reached out to the industry and academia. This allowed the broad knowledge of the participants in this field to be leveraged, giving the Eurosystem a detailed initial view of the possibilities and limitations of existing hardware devices. In contrast to other projects, this workstream had a discovery rather than an experimentation angle. To select the partners, the ECB initiated a procurement process[3], and as a result chose six participants with a wide range of expertise to ensure a broad view of the topic from different angles (e.g. well-established players as well as smaller, highly-specialised companies). The task of each of the participants was to independently deliver a proof of concept (POC) together with a comprehensive report. In these reports, the participants described their proposed solution and addressed a list of research questions regarding the technologically feasible possibilities of HBIs. The role of the workstream was to guide the companies throughout the development of the POCs and the drafting of the reports.

With this project, the Eurosystem did not aim to select any specific solution or provider or make any decisions on the design of the digital euro. Its only purpose was to objectively assess the technically feasible possibilities of a potential HBI implementation

[1] European Central Bank (2020), Report on a digital euro, October.

[2] The digital euro experimentation project is described in the document European Central Bank (2021a), "Digital euro experimentation scope and key learnings".

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

for a digital euro. This project was hence aimed at assisting the Eurosystem, including the ECB Governing Council, in making informed decisions about the convenience of conducting further investigations on the matter.

Unique characteristics of a hardware bearer instrument (HBI)

The unique features of an HBI can be easily confused with functionalities offered by other implementations of the digital euro or even electronic money. The key difference is that the **HBI entitles the holder of a hardware device the ownership and full custody of the currency stored in the device.** This is in stark contrast, for example, with a debit card linked to a bank account, where the cardholder uses funds previously deposited in a financial institution. In addition, the transfer of funds using an HBI settles the payment from one holder (citizen or business) to another, without the need for third-party intermediation. As the HBI is hence a device whose possession suffices to hold money and carry out transactions with it, the most intuitive (non-digital) equivalent is cash. A banknote is a bearer instrument, which represents value in itself, and a transfer of the banknote corresponds with the transfer of funds.

An HBI's resemblance to cash also extends to the possibility of enabling **offline** (no internet) payments and it also shares actions equivalent to the withdrawal and deposit of funds. This takes the form of loading and unloading of digital euros onto the device, where **loading** is understood as the process in which valid funds (e.g. cash, funds from a bank account or even digital euros) are converted into or transferred to the HBI native digital euro form and made available for transacting. Once the digital euros are loaded, the HBI can make transactions even without internet access. The cycle is closed by the **unloading** (equivalent to a cash deposit) of the HBI digital euros into other forms of funds.

The POCs and the market research showed a number of different design options with regards to the **form factor.** The HBI generally has a portable form factor, such as a smart phone, a smartcard, a dongle or a wristband. To ensure secure implementation, the common element to all solutions investigated in the project was the **support of a secure element (SE).** While the SE is the only essential element of the different form factors, access to form factor should ideally enable the user to verify, at minimum, the following functionalities: (i) setting the amount to be transferred, (ii) checking the balance and (iii) authorising the transaction. These functionalities require access to keypads and screens or the use of a mobile phone as a graphical user interface proxy.

A **notable distinction is whether the hardware device used is active** (powered) or **passive** (such as common credit or debit card devices). There are the two common implementations seen in the POCs: mobile phones or smartcards (bank card-like form). A powered device, in especiall a phone, could offer compatibility for users with multiple payment scenarios, such as person-to-person (P2P), point-of-sale and remote payments. As for smartcards, the POCs covered both passive and active card implementations. The latter carry their own battery to support self-executed actions, such as establishing an NFC connection with another card and performing P2P transactions. For any online functionalities they nevertheless rely on an additional online device as none of the cards tested can yet establish their own internet connection.

Finally, the workstream found **three basic approaches which could 'digitalise' euros in an HBI.** The design decision regarding these three approaches would have a deep impact on the functionalities andlimitations of the HBI:

1) Indivisible tokens: a piece of digital information representing a certain value and digitally signed by a central bank. It is the closest analogy with euro banknotes and coins, as they also have fixed denominations.

2) Divisible tokens: similar to the previous approach, but each token can be broken up by the HBI into parts to make up the exact amount of a transaction (i.e. there would be no need for the counterparty to provide change).

3) Balance: each digital wallet has a balance of euros that increases when money is received and decreases when payments are made.

Challenges of an HBI from a CBDC perspective

From the different aspects analysed by the workstream, a summary of the ones considered especially relevant from a central bank perspective is presented in the following sections. This has a broad scope and covers technical and security aspects, from the double spending prob-lem to policy aspects like remuneration or fitting with AML regulation.

System security and the use of an SE

Execution and storage of the cryptographic information inside an SE has been unanimously identified as an essential safeguard to **prevent counterfeiting (minting) or double expenditure.** The SE provides isolated storage and execution as well as protection against physical tampering. The software running on the SE or in adjacent secured sectors would allow the implementation of different control elements, for example to establish limits (e.g. amount of euros allowed in the hardware wallet), implement restrictions (e.g. a possible number of offline transactions, maximum value of single transactions) and store AML-related and KYC-related data. As a complement to the use of SEs, when enabling offline transactions, regular online reconciliation has been appointed as essential in detecting fraudulent use in an offline environment.

The supply chain of an HBI, in particular the SEs, poses additional challenges. For example, some mobile phone manufacturers include SEs in their phones, but they keep tight control of fabrication and external software access. The mobile phone is a very convenient and universal form factor but the implementation of HBI solutions in a phone environment, may depend on the existing policies of phone manufacturers for the use of SEs, communication interfaces (like Near Field Communication – NFC) or the lower-security Trusted Execution Environment (TEE).

Offline payments

The Report on a digital euro[4] established a scenario-specific requirement (i.e. in case of decreasing demand for cash) that a digital euro should enable offline payments. Additionally, respondents in the Eurosystem report on the public consultation on a digital euro[5] ranked offline capability as the fifth most desirable feature of a digital euro, which shows that many citizens would likely demand this feature in a potential digital euro. The research was therefore focused on enabling a number of consecutive offline payments.

An important conclusion is that the state-of-the-art technology is not able to perform an indefinitely long chain of consecutive offline payments in a secure way (i.e. ensuring that no double spending of funds occurs). This reinforces the current stance of the Eurosystem that a digital euro should not replace, but rather complement, euro cash.

However, an equally relevant conclusion is that it is possible to perform a limited number of offline transactions without severe security concerns. Although it is impossible to avoid a device eventually being compromised, all measures should be taken to compel potentially compromised devices to interact with other devices that go online frequently. Pure offline operation raises concerns derived from the risk of total system collapse when a first wallet is compromised, which could be mitigated by going online regularly.

The research has shown that if more than one offline payment in a row is supported, divisible tokens or balance account solutions are preferred. The issue with divisible tokens is the need to carry a history of previous offline transactions, which increases the processing times during the transfer of funds and hence degrades the user experience. Similarly, the data storage capacity of hardware devices would eventually limit the number of offline transactions.

Different levels of privacy and user identification

The privacy aspect has two clearly distinct angles: (i) the traceability of the financial transactions executed with an HBI, and (ii) the identification of an individual using an HBI. These two aspects overlap in some of the POCs, and privacy and security needs in an offline environment often clash.

The research showed that there are technical solutions for achieving a certain level of privacy, even some sort of tiered privacy. In some cases, the identification of the individual is only enabled by a third-party entity as a response to suspicious activities. Besides, as most of the solutions did not implement specific privacy features other than the functional POC design, more research were needed if guaranteeing the non-traceability of the transactions would be a prime goal.

Most implementations distinguish between HBI for citizens going through a full KYC process[6] and tourists or other persons with a limited KYC check. Some POCs also illustrated the technical possibility of issuing dedicated devices with full anonymity. To allow for a certain amount of anonymity, measures such as a balance upper limit, a limit in the value or number of offline transactions or specific transaction fees could be implemented.

To obtain access to the device and execute a transaction, the POCs relied on the identification measures

[4] European Central Bank (2020), op. cit.

[5] European Central Bank (2021b), Eurosystem report on the public consultation on a digital euro, April.

[6] The question of which entity should perform the KYC check was not part of the research, but the general assumption was that it was either the hardware on-boarding entity (e.g. the bank which provides the card or links the phone to a digital euro solution) or a dedicated KYC authority.

implemented in the specific HBI devices. In these instances, PINs or biometrics were often used to authenticate the user. These could be implemented in a smart phone or card environment.

Remuneration and geo-limits[7]

Remuneration implementation in an HBI poses many challenges. It is necessary to differentiate between an infrastructure where offline operation is possible and one where online connectivity is permanent. In the latter, remuneration implementation is possible as a timely update or every time a transaction happens. If HBIs can be offline for long periods of time, implementation is far more complicated. It would be possible to set a rule that it has to go online e.g. once a month and retrieve the new rates but this would limit the flexibility of rate adjustments and cannot be enforced in practice. On the hardware side, this method would require a "secure" clock inside the device to prevent any manipulation. Based on the outcome of the research, a clock of this kind is not currently available as standard.

Any implementation of **geo-limits** requires some sort of location identification. The research has shown that it is not currently possible to fully guarantee a geo-limit in an offline-supporting environment.[8] In a smartphone, the implementation of probabilistic methods would be possible (e.g. last known location half an hour ago) but even GPS location information can be simulated. In a card-based implementation this is even more complicated to achieve as they have no GPS receiver. However, restrictions based on citizenship or residence are possible and can be linked to a KYC on-boarding process. These restrictions would be implemented on a policy level and not on a hardware level.

AML/CFT legal aspects

In essence, AML-CFT checks are possible if HBIs go online regularly and reconcile against a ledger (this would e.g. enable pattern recognition and uploading of up-to-date sanction lists). There seems to be no convincing way to prform such checks in a pure offline solution.

We did not study the AML/KYC requirements in depth, but there is strong evidence that the current AML-CFT framework would be very limiting for an offline HBI digital euro, considering that the limits and thresholds for anonymous payments with prepaid instruments are currently very low.[9]

Key takeaways

Two important questions resulting from the Eurosystem's Report on a digital euro were whether existing hardware solutions could be adapted for a digital euro and whether cash-like features could be made available and usable offline. The research work conducted by the workstream confirm that the implementation of a digital euro as an HBI is feasible. However, the extent to which cash-like features can be incorporated into an HBI is limited by technology, security and legal considerations. In addition, a set of technical and legal challenges will need to be addressed by central banks, industry and academia to ensure that hardware solutions are implemented safely and in compliance with the regulations.

[7] European Central Bank (2020), Report on a digital euro, October. Requirement 13

[8] For example, in case of a smartphone this would mean that the device is in flight mode and transactions are still possible.

[9] Directive (EU) 2018/843 on money laundering and terrorist financing sets a limit of EUR 50 for remote payments for general-purpose anonymous prepaid cards.

The key takeaways of the research work can be summarised as follows:

- **Technical feasibility.** The first and most important conclusion from the research is that, from a technical perspective, the digital euro could be implemented as an HBI. This instrument could even support consecutive offline payments, although this possibility would come with a set of limitations which would prevent it from being fully comparable to euro cash.

- **Security.** The initial analytical work showed that offline transactions can be sufficiently secure. However, it is impossible to discount an attack vector via physical tampering or via software weaknesses. The former risk should be mitigated by independent assessment and tests and the latter via rigorous audits. However, even if successful, the potential damage would be limited as it would force an attacker to remain offline in all further transactions as an online connection would reveal the compromising of the system. Possible solutions might incentivise users to reconcile often as a way of protecting the network.

- **Form factors.** There are no limitations regarding possible form factors of an HBI as long as it can host an SE and has certain standard communication interfaces like Blue-tooth or NFC. In some cases, a phone can act as a user interface of a card. The most common embodiments are therefore a smart phone or a smartcard. Given that these are well established systems, a user-friendly implementation in a known infrastructure is not a problem from a technical standpoint.

- **Supply chain.** SEs are the cornerstone of to a secure implementation of an HBI and, at the same time, one of the elements whose supply control will be more complicated for the Eurosystem. Especially in a phone implementation, the access policy of the manufacturer might be a risk factor in terms of flexible implementation by the Eurosystem. The limited presence of semiconductor manufacturers in the EU means a potential dependency on a non-European provider. However, we can currently see encouraging developments towards an increase in semiconductor production, design and expertise in the EU.

- **AML and KYC compliance.** Even with offline capabilities, any implementation must comply with AML and KYC rules. The POCs have shown that this is only possible by implementing rules directly on the card and rely on the initial HBI attestation[10] to ensure compliance with those rules, additionally supported by a background ledger against which reconciliation occurs from time to time.

- **Back-up system.** The need for security and compliance with regulations (e.g. through solutions establishing a maximum number of offline transactions, amount limits for offline transfers, or limits on holdings), together with the technical limitations of the offline functionality, restrict the length an HBI digital euro could function as a back-up system[11] as it would require a regular check against the ledger.

- **Remuneration and geo-limits.** The support of a chain of consecutive offline payments, though possibly desirable, limits to a great extent the implementation of policies like remuneration or geo-limits. Remuneration might be realisable but only with restrictions both on the user as well as the central bank side. An effective implementation of geo-limits is unrealistic given the current status

[10] Attestation is the process in which the HBI is initialized with its cryptographic keys and that information is optional link to the owner.
[11] European Central Bank (2020), Report on a digital euro, October. Requirement 5

of technology. What is possible, however, is a distinction within the KYC process between residents and tourists and a corresponding differentiation on a wallet level (e.g. different limits or offline restrictions).

Deutsche Bundesbank
Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main

Postfach 10 06 02
60006 Frankfurt am Main

Telefon 069 9566-0
Telefax 069 5601071
Internet http://www.bundesbank.de