The digital euro in the digital age: Can we really digitise cash?

Received (in revised form): 3rd September, 2023

Maja Schwarz
Managing Consultant, NTT Data DACH, Germany

Maja Schwarz

***Maja Schwarz** is a managing consultant at NTT Data DACH. As a member of the CTO Team, she works on technology innovation and explores how emerging technologies can lead to product and service innovation. She holds a PhD in computer science from the Polytechnic University of Catalonia and an MBA degree from the Mannheim Business School.*

*NTT Data Deutschland SE,
Königsberger Str. 1,
60487
Frankfurt am Main,
Germany*

E-mail: maja.schwarz@nttdata.com

Journal of Payments Strategy & Systems
Vol. 17, No. 4 2023, pp. 398–407
© Henry Stewart Publications,
1750-1806

Abstract

Central banks around the world are considering the introduction of retail central bank digital currency. The European Central Bank, for example, has made considerable progress in this respect, and its research into the viability of a digital euro is at an advanced stage. Given, however, that people living in the euro area have been using various forms of digital payments for a number of years, a key question is what the benefits of such an innovation would be, aside from a reduced dependence on payment processors from outside the EU. A digital euro that retained the properties of physical cash, such as anonymity, offline payments and high inclusion, could provide added value compared with existing digital payment solutions. This paper explores whether and how fast-developing technology might be used to implement a cash-like digital euro. This type of resemblance to cash could eventually be more important for wide adoption than the difference in liability between central and commercial bank money.

Keywords: central bank digital currency (CBDC), retail CBDC, privacy, offline payments, digital euro, cash-like

INTRODUCTION

Central banks worldwide are considering the introduction of central bank digital currency (CBDC). CBDC projects in different countries are in various phases, ranging from initial research, proofs of concept and pilots, up to the launched digital currency. CBDC has already been launched in the Bahamas and Jamaica, while some other countries, like China, are using pilots for real-world testing of their solutions.[1] Most other countries are in earlier stages of research and the development of proofs of concept. The European Central Bank (ECB) is also actively exploring the possibility of introducing a digital currency. The current investigation phase should be finished in October 2023, after which it will be decided whether to start the process of developing a digital euro.[2]

The digital euro investigation phase targets the retail euro, which is used for payments by citizens and businesses. The ECB is also involved in projects related to wholesale CBDC, which is used by financial institutions for settlements in central bank money. As the wholesale CBDC as a means of digital interbank settlement in central bank money has existed for decades, and the retail CBDC represents a new digitisation concept, the motivation for retail and wholesale CBDCs projects differ.

The wholesale CBDC projects explore how a new technology — blockchain/distributed ledger technology (DLT) — could improve the current process for digital payments in central bank money, notably with respect to inefficiencies such as those associated with cross-border payments due to the use of correspondent banks. Furthermore, central banks also need to be prepared for the potentially wide-scale adoption of DLT, such as in security trading, where the payment leg is currently settled in central bank money. In such a case, the absence of wholesale DLT-ready CBDC could lead to the use of other means of payment from the private sector. The Bank of International Settlements (BIS) and its Innovation Hub lead many international collaborations in this area.[3]

In contrast to the wholesale CBDC, the retail version is a genuinely new concept under development. Physical cash in the form of banknotes and coins is a liability of the central bank and is currently without a digital counterpart. Citizens can, however, make digital payments using commercial bank money or e-money, or since more recently, crypto currencies and stablecoins.

The present paper focuses on the digitisation of the retail euro and investigates the characteristics of physical cash that, if retained in the digital form, would present added value compared with the existing forms of digital payments. Important properties of physical cash are high inclusion, full privacy and the ability to make offline payments. These characteristics distinguish cash from existing digital payment solutions. Cash supports high inclusion as anyone can hold it, without needing a bank account. Furthermore, cash payment provides the best way to maintain transaction privacy. Finally, payments with physical cash are offline and do not require an internet connection. The ECB is working to design a digital euro that considers these cash-like properties.[4,5]

Although the final design of the digital euro will be also driven by policy-related decisions, this paper shows how technology can enable cash-like properties. Results from recent technical CBDC projects are used to evaluate the extent to which cash-like properties can be translated from the physical to the digital world.

MOTIVATION FOR A CASH-LIKE DIGITAL EURO

As citizens have been able to make digital payments using commercial bank money for many years, the argument for the introduction of retail CBDC requires clarification. According to the ECB, a digital euro will ensure access to central bank money in the digital age.[6] The ECB thus sees the digital euro as both a complement to, and an equivalent of, physical cash.[7]

At present, central bank money (as a direct liability of the central bank) is available to citizens only in the physical form of banknotes and coins. In terms of liability, a retail CBDC would provide citizens with a digital substitute for cash. Were citizens to prefer to hold their money in the risk-free form, however, a digital euro could pose a risk to commercial banks, leading to disintermediation. To address this risk, the ECB plans to impose a limit on the amount of digital euro that citizens can hold.[8] As this limit might be relatively low, citizens may find the main difference between private and public money to be insignificant.

Beyond the direct benefits for individual users, the increasing use of digital payments based on private money is a threat to the traditional role of central bank money as a fundamental underpinning of the sovereign currency.[9] Further, most electronic payments in Europe are processed either by companies headquartered outside the European Union[10] or processed under rules set by companies domiciled outside the EU.

TECHNOLOGY OPTIONS

Digital currencies can be implemented using different technological approaches and system architectures. Accordingly, countries around the world are considering multiple options for the implementation of CBDC, including both decentralised approaches, such as blockchain/DLT-based, and centralised ledgers. Considering that retail central bank money settlements should be controlled exclusively by one central bank, centralised solutions might better suit this digital currency use case.[11] Some of these solutions, however, are highly influenced by blockchain-related concepts, such as the Hamilton Project of the Federal Reserve Bank of Boston and the MIT Digital Currency Initiative.[12]

Besides discussions on whether CBDC should be implemented on a centralised or a decentralised infrastructure, there are two additional aspects often considered in relation to the CBDC system design. The first aspect is related to financial intermediaries and the different roles they can take in a CBDC system.[13] As central banks currently do not provide services directly to citizens and would not have the resources to do so, the introduction of retail CBDC is unlikely to change this. Although the ECB should retain full control over the issuance and settlement of digital euro, financial intermediaries should play an important role in the distribution of the digital euro in this two-tier system.[14] As the intermediaries are expected to do onboarding and probably also submit user transactions,[15] their role in the system is relevant for all cash-related features, namely privacy, offline payments and inclusion.

The second commonly discussed technology aspect relates to whether CBDC should be account or token based. This classification was created before crypto assets and the concept of tokens slightly differs from the standard crypto terminology. Traditionally, account-based payment systems record user balances in the form of accounts. Users need to identify themselves to be able to make transactions which affect the balances. In a token-based system, the token is an object used for a payment by its owner that needs to be verified during a transaction.

Although it has been argued that this classification into account and token-based systems might be less suitable[16,17] since the appearance of crypto assets, the basic separation between account balances and tokens as owned digital objects remains valid. In the account-based case, the assets are recorded per address, while in the token-based case, the transaction data objects themselves contain information that is used to prove ownership of received funds.

The ECB has not yet made any final decision on the underlying technology framework, but more information is expected in the coming months.[18] Before the current investigation phase, the concepts related to the digital euro were explored by the ECB in an experimentation process within four work-streams. Both centralised and decentralised solutions have been considered.[19] Additionally, a concept that would literally digitise banknotes through fixed value tokens or 'digital bills' was evaluated.[20] In this concept, each bill has its own ledger that tracks the ownership of the bill. Finally, in a more recent technical documentation provided for prototype development,[21] the ECB refers to the Hamilton Project as a reference design. Although centralised, the design has many similarities to Bitcoin, such as the transaction format, which is also based on unspent transaction outputs (UTXO-based). With this token-based format, funds are simply transaction-generated objects that payees can consume and use for further payments.

DIGITISATION OF CASH-LIKE PROPERTIES

Anonymity and privacy

Due to its physical token-based nature, cash provides anonymity in payments by allowing a traceless change in the ownership of banknotes and coins. Electronic systems, however, must record the ownership of funds in some form, which makes it challenging to provide the same level anonymity. This is irrespective of whether the CBDC design is account or token-based.[22] Additionally, legal regulations usually prevent digital payments from being anonymous, or impose limits on transaction values.

Privacy-preserving techniques can be used to limit or prevent access to sensitive data. That transactions stay private has been seen as the most desirable feature of the digital euro.[23] Privacy of user data and confidentiality for businesses are priorities for both citizens and businesses. Privacy aspects of CBDC, related challenges and privacy-enhancing techniques have been broadly discussed elsewhere.[24–30]

Privacy in payment systems entails measures to protect the identities of the payer and payee, and to protect information regarding transaction amounts and the timings of said transactions. To provide a certain level of anonymity, identities may be pseudonymised through their identifiers, such as the addresses used in cryptocurrencies. Further privacy-enhancing techniques must not prevent transaction verifiability, however, as the validity of a transaction must be verified before it is settled. In the two-tier system envisioned by the ECB, some data might be transparent to intermediaries but not to the central bank, depending on the system design and role separation. Theoretically, through role separation, the central bank can store only cryptographically protected data needed for transaction validation, preventing a single entity from observing the entire payment activity of citizens and businesses.

The Hamilton Project

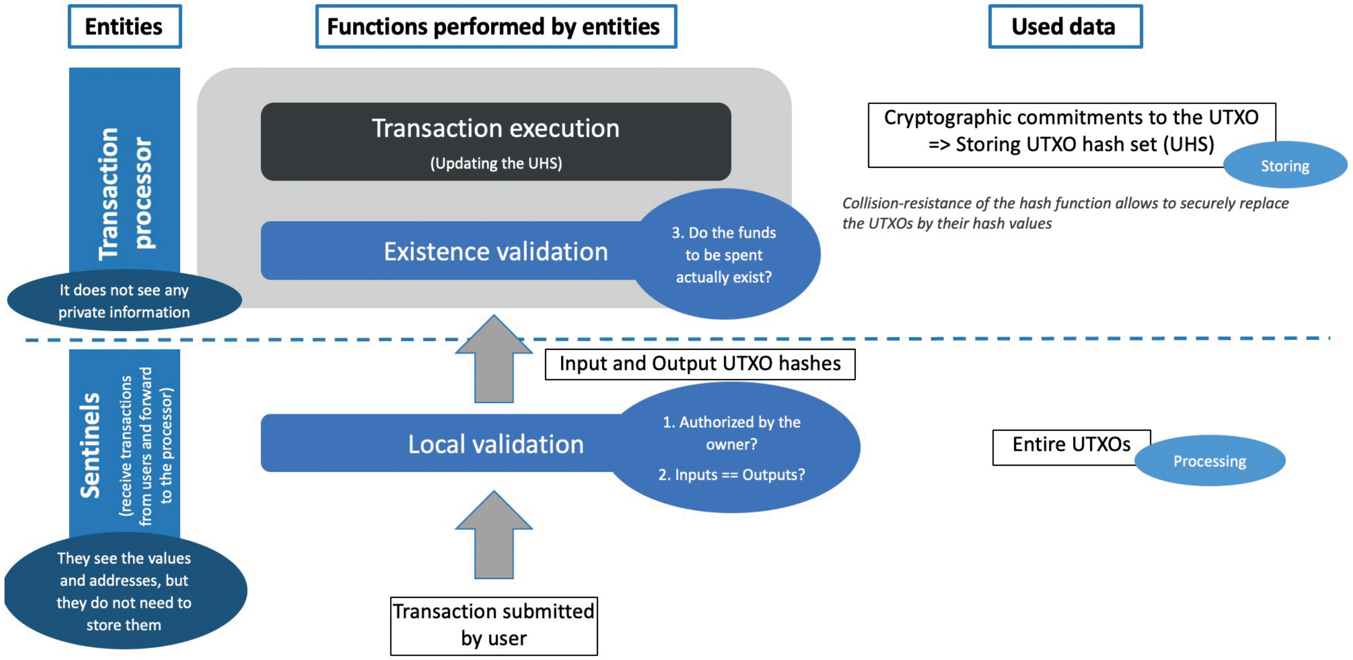
The Hamilton Project uses a design in which different system units see only the portion of information needed to serve their functionality.[31] The transaction processing is separated into multiple validation steps and the final settlement, which limits the amount of information needed to be seen or stored at each step. Furthermore, the system design developed in the Hamilton Project uses hashing to increase user privacy, allowing the last entity in the validation chain to see and store only the hashed data.

This transaction validation process is depicted in Figure 1. With the used UTXO transaction format, a transaction consists of inputs, which are the funds being consumed by the transaction, and the outputs that are funds being sent to receivers. These outputs are unspent funds that can be used by their receivers in future payment transactions. The transaction validation consists of three steps. In the first step, it needs to be checked whether the spending of funds has been authorised by the owner via a signature with the respective private key. Next, a sanity check is conducted to confirm that the total amount of inputs corresponds to the total amount of outputs. The last validation step checks if the funds to be consumed (UTXOs) do indeed exist and have not been spent already. For this, it is sufficient to check that their hashes are stored in the set of valid hashes. Finally, the set of hashed UTXOs needs to be updated by removing the consumed inputs and adding newly generated outputs, which is done by the transaction processor in the transaction execution step after all validation steps are successfully finished. This describes one of the possible approaches to enhance privacy. Additional techniques such as zero knowledge proofs could hide sensitive information even in the first two validation steps.[32]

Interestingly, the current Hamilton design could imply additional cash-like aspects, insomuch as users could still lose their money were they to lose their private keys or the data pertaining to unspent funds.

Privacy and the digital euro

The transaction format of the Hamilton Project is mentioned in the ECB's current prototype design.[33] However, the privacy preserving methods, such as UTXO hashing and potential assignment of transaction verification steps to different stakeholders, are not elaborated in the published documentation. By delegating the first two steps of transaction validation to intermediaries, citizens and businesses would protect their privacy in front of the ECB. However, such allocation of responsibility could theoretically endanger financial stability as the


Entities
Functions performed by entities
Used data
Transaction processor
It does not see any private information
Transaction execution
(Updating the UHS)
Existence validation
3. Do the funds to be spent actually exist?
Cryptographic commitments to the UTXO => Storing UTXO hash set (UHS)
Storing
Collision-resistance of the hash function allows to securely replace the UTXOs by their hash values
Input and Output UTXO hashes
Sentinels
(receive transactions from users and forward to the processor)
They see the values and addresses, but they do not need to store them
Local validation
1. Authorized by the owner?
2. Inputs == Outputs?
Entire UTXOs
Processing
Transaction submitted by user

Source: Project Hamilton Phase 1: A High Performance Payment Processing System Designed for Central Bank Digital Currencies, Federal Reserve Bank of Boston and MIT Digital Currency Initiative

Figure 1: Separation of transaction validation and processing steps in the Hamilton Project

intermediaries would gain partial control over the validation process and would be able to 'print money'. It is thus reasonable that the ECB should maintain control over the critical steps of the validation process. In the Hamilton example, this would mean that the ECB also checks that no more funds are spent than available, which would require modifications to the current system design in order to support user privacy. Additional modifications would also be needed to improve the auditability of the system.

Based on currently available documentation,[34] the ECB is currently considering enhancing citizens' privacy through the use of one-time addresses, similar to the usual practice with cryptocurrencies. In this scenario, the intermediaries control user wallets and their keys on their behalf and generate new addresses for each transaction. In this way, the intermediaries would be aware of the activity of their own customers, but the ECB would see only addresses appearing in the UTXO transactions. Always using a new address to receive new funds is an additional measure to improve user privacy.

The ECB additionally argues that a very high level of anonymity cannot be granted due to other policy goals, such as anti-money laundering (AML) and combating the financing of terrorism, as well as maintaining financial stability by limiting how much funds can be kept in central bank money.[35] The ECB therefore plans to find a balance between privacy and transparency by providing 'selective privacy' for low-value payments and the offline functionality.[36] Offline payments are seen as a way to enhance user privacy as they do not require a connection to the intermediaries at the moment of payment.

P2P offline payments

Peer-to-peer (P2P) offline payments are defined as payments between two users without a connection to the ledger.

Currently, no payment method supports both online and offline operation without considerable risk exposure. Businesses can accept credit cards when their card terminal cannot establish a connection to the provider to check the payment status, but they are then exposed to the risk that the payer does not have the funds for the payment transaction.

As offline operation supports inclusion and system reliability by enabling payments without an internet connection, centrals banks designing CBDCs consider this feature to be important and are investigating it accordingly.[37,38] The main technical challenge of digital offline payments is how to prevent double-spending. As the tokens are digital and not physical, a malicious payer could use a copy of the same payment token for multiple payments, leading to a problem known as the 'double-spend problem'. The problem exists for token as well as account-based payment systems. In offline settings, the payee has no possibility to check the ledger to see whether the token has been spent in a token-based implementation or whether the payer has enough funds in an account-based system. The only connection established is the one between the payer and payee over near-field communication (NFC) or Bluetooth. This setup is illustrated in Figure 2.

Hardware-provided security, through secure elements (SE) or trusted execution environments (TEEs), together with the public key infrastructure (PKI) can be used to solve the double-spend problem.[39] SE/TEEs provide a separate or isolated processing environment that guarantees the integrity and confidentiality of the data and the code running inside. Integrity means the code and data cannot be modified by an unauthorised user, while confidentiality ensures that unauthorised users cannot read the data. Therefore, secure hardware protects the private key created for spending offline funds, so that these funds can be used only by the person controlling the device. It additionally ensures that the funds are spent only once, as the application controlling spending would be installed by a trusted party, and its code and data cannot be modified without authorisation. Modern mobile phones are equipped with secure hardware and could theoretically be used for offline payments.

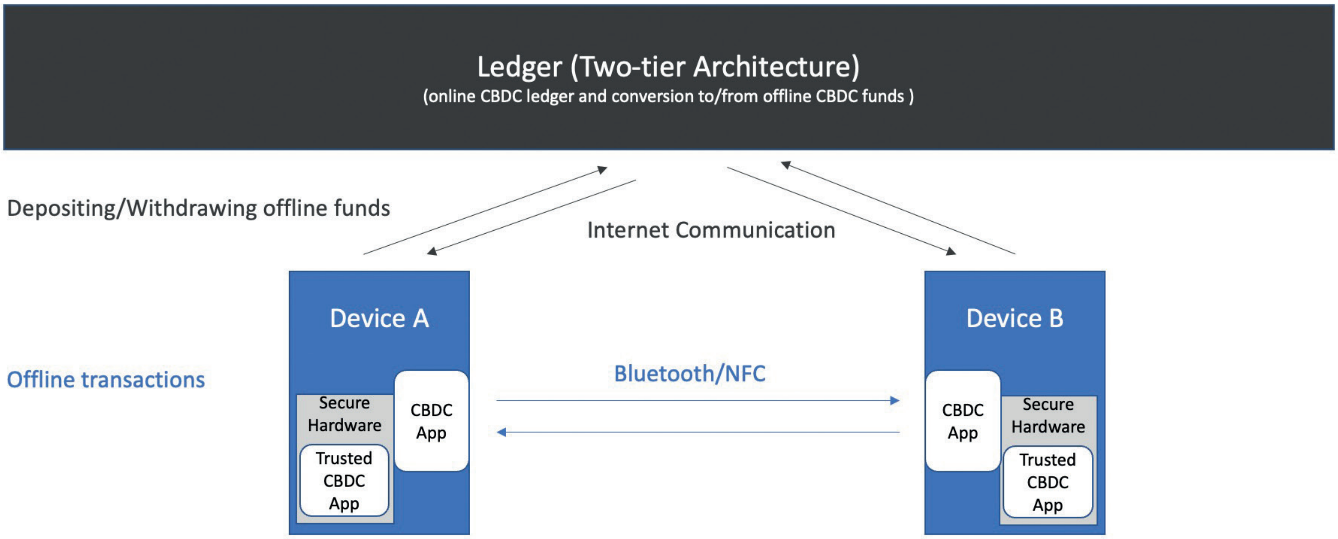


Figure 2: Offline payments using devices with secure hardware

The design of the offline payment system is not strongly dependent on the design of the online CBDC system. These two systems can function relatively independently by allowing users to load offline CBDC to their devices, for instance, from their online CBDC wallets. They can convert them back to online funds once they wish to do so and can again connect to the internet.

Example offline payment protocol

An example of this approach is the offline CBDC payment protocol developed by VISA Research, which is based on secure hardware and PKI, with the central bank as the root certificate authority for generating digital signatures.[40] Financial intermediaries are also included as intermediate certificate authorities to support the process around the offline use of CBDC, such as issuing digital certificates to vetted devices. Users need to deposit their funds to their offline account by, for instance, converting their usual online CBDCs into offline funds. A user's offline funds get credited once the trusted application running on the user's secure hardware obtains a signed message from a trusted server that offline funds have been generated by debiting the online CBDCs. The user controlling the device can transfer these funds to another user without either of them having to communicate with the central bank or any intermediary. In order to make a payment, the payer sends their certificate to the payee together with the payment confirmation as a signed message that includes the transferred amount and the payee's certificate. This requires that the payee sends their certificate to the payer prior to the actual transfer. Upon receiving the sent information from the payer, the payee can check it for correctness. If the certificates are correct and the message was signed by the respective key, the payee can be assured that the payment is valid. As the payer's trusted application executes on secure hardware, double-spending is prevented by ensuring that the application deducts the funds before sending them to the payee. Finally, the payee can further spend the funds offline or convert them into online funds once an internet connection can be established. The protocol also uses counters within the payment confirmations to prevent one confirmation from being maliciously used multiple times without deducting the offline balance of the payer. This type of attack is known as 'replay attack'. To prevent replay attacks, this protocol assumes that a device receiving offline payments stores locally a list of all payer addresses that have sent funds to it. Even if this locally maintained list could be securely stored, this contributes to a reduction in privacy compared with the physical exchange of banknotes and coins.

Offline payments and the digital euro

A work stream of the digital euro project devoted to hardware bearer instruments evaluated whether existing hardware solutions can be used for offline payments.[41,42] During this work, the Eurosystem collaborated with industry and academia and chose six companies to independently deliver proofs of concept. The aim was to assess the technological feasibility of offline CBDC payments. The use of secure hardware was unanimously identified as the way to prevent double-spending and counterfeiting. Various devices, such as smartphones, smartcards or wristbands, were considered.

Nevertheless, certain challenges for a straightforward implementation and the use of offline payment methods based on secure hardware have been noted.[43] The secure hardware devices are kept directly by users, who have a strong economic incentive to compromise their own devices in order to double-spend or counterfeit CBDC. Additionally, if a device is compromised, the user can spend their funds many times over, meaning there is no graceful degradation. The required trust in the chip and device manufacturer, as well as in the supply chain, is an additional challenge. Finally, funds might be lost in the event that the device is lost or damaged, but these characteristics resemble those of physical cash.

Consecutive offline payments are technically possible in both token and account-based transaction models. Nevertheless, as the possibility of one of these devices being compromised cannot be fully discarded, ways to incentivise users to go online to reconcile with the ledger have been considered.[44] This could help to detect a potential compromising of the system. It is also reasonable to expect that the maximum value of offline payment transactions would be capped.

Providing a relatively high level of anonymity in offline payments is possible as the full history of offline payments does not need to be reconciled once the device is online. The software used in secure elements can be used to enforce an upper limit on balance or transaction amounts, as well as the number of offline transactions. Some of these features might be desired to balance between regulatory requirements and the desire for privacy, and are therefore being considered by the ECB for the digital euro.[45]

Finally, in its report on the progress of the digital euro investigation phase, the ECB states that a solution for offline P2P payments should be developed, but it concludes that the development of online payments should not be postponed by possible delays in the development of the offline solution due to technological and regulatory challenges.[46]

Inclusion

Financial inclusion might not be a pressing challenge within the euro area, but high inclusion is a characteristic of physical cash and the ECB sees it as an important and desirable property of the digital euro. In the two-tier system with financial institutions as intermediaries that assist in the process of onboarding and opening of the digital wallets, the high participation of such institutions is crucial for inclusion.

Digital wallets could be a part of the standard digital banking offering by commercial banks. Alternatively, they could be independently developed mobile apps with restricted access for users who have been screened by an intermediary's know-your-customer (KYC) procedure. Depending on the KYC/AML policy design, digital wallets used for low-value transactions might not even require a full KYC process. For instance, China's e-CNY pilot allows for the registration of wallets with limited capabilities using a mobile phone number.[47] Furthermore, offline payments can contribute to inclusion in cases when access to the internet is not available.

CONCLUSION

Replicating the characteristics of physical cash in its digital form is a challenging task. Nevertheless, technological innovation is creating a path towards cash-like digital currencies. This paper has discussed some recent CBDC projects to shed light on how technology can enable the properties of cash in a digital world.

Full anonymity of physical cash is highly appreciated by citizens but difficult to achieve for digital payments. A wide spectrum of privacy-preserving design choices has already been developed and evaluated for digital currencies and many further projects are ongoing. A trade-off between privacy and auditability is an additional challenge. Supporting digital offline payments introduces a new risk in the form of a double-spend problem — a risk that does not exist in the traditional world of physical cash. A possible solution is to run a trusted application on secure hardware. Finally, high inclusion as an important characteristic of cash can be enabled through the broad availability of suitable devices, such as mobile phones with internet access.

Although this paper focuses on the current technical feasibility of cash-like features, design decisions are informed by more than just technology. Important policy aspects will certainly be considered and might further limit the digital euro's resemblance to cash.

References

(1) CBDC Tracker (2023) available at: https://cbdctracker.org/ (accessed 1st April, 2023).

(2) European Central Bank (2023) 'Digital euro: Timeline', available at: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html#timeline (accessed 30th April, 2023).

(3) Bank of International Settlements (2023) 'BIS Innovation Hub work on central bank digital currency', available at: https://www.bis.org/about/bisih/topics/cbdc.htm (accessed 30th April, 2023).

(4) European Central Bank (2022) 'ECB selects external companies for joint prototyping of user interfaces for a digital euro', available at: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews220916.en.html (accessed 30th April, 2023).

(5) European Central Bank (2023) 'Digital euro', available at: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (accessed 30th April, 2023).

(6) Panetta, F. and Lagarde, C. (2022) 'Key objectives of the digital euro', European Central Bank, available at: https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog220713~34e21c3240.en.html (accessed 30th April, 2023).

(7) European Central Bank, ref. 5 above.

(8) Panetta, F. (2022) 'The digital euro and the evolution of the financial system', introductory statement at the Committee on Economic and Monetary Affairs of the European Parliament, Brussels, 15th June.

(9) European Central Bank (2022) 'The Case for a Digital Euro: Key Objectives and Design Considerations', available at: https://www.ecb.europa.eu/pub/pdf/other/key_objectives_digital_euro~f11592d6fb.en.pdf (accessed 30th April, 2023).

(10) *Ibid*.

(11) Wüst, K., Kostiainen, K., Delius, N. and Capkun, S. (2022) 'Platypus: A central bank digital currency with unlinkable transactions and privacy-preserving regulation', Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, 7th–11th November.

(12) Federal Reserve Bank of Boston and Massachusetts Institute of Technology (2022) 'Digital Currency Initiative. Project Hamilton Phase 1 A High Performance Payment Processing System Designed for Central Bank Digital Currencies', available at: https://www.media.mit.edu/publications/a-high-performance-payment-processing-system-designed-for-central-bank-digital-currencies/ (accessed 30th April, 2023).

(13) Auer, R. and Boehme, R. (2021) 'Central bank digital currency: The quest for minimally invasive technology', BIS Working Paper, BIS, available at: https://www.bis.org/publ/work948.htm (accessed 30th April, 2023).

(14) Panetta, F. (2022) 'Building on our strengths: The role of the public and private sectors in the digital euro ecosystem', European Central Bank available at: https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220929~91a3775a2a.en.html (accessed 30th April, 2023).

(15) European Central Bank (2023) 'Annex 1: Functional and non-functional requirements linked to the market research for a potential digital euro implementation', available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf (accessed 30th April, 2023).

(16) Culligan, A. (2020) 'Token or account based CBDC?', SETL, available at: https://setl.io/token-or-account-based-cbdc/ (accessed 30th April, 2023).

(17) Garratt, R., Lee, M., Malone, B. and Martin, A. (2020) 'Token- or account-based? A digital currency can be both', Liberty Street Economics, available at: https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/ (accessed 30th April, 2023).

(18) European Central Bank (2023) 'Progress on the investigation phase of a digital euro — third report', available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230424_progress.en.pdf (accessed 30th April, 2023).

(19) European Central Bank (2021) 'Digital euro experimentation scope and key learning', available at: https://www.ecb.europa.eu/pub/pdf/other/ecb.digitaleuroscopekeylearnings202107~564d89045e.en.pdf (accessed 30th April, 2023).

(20) European Central Bank and selected member central banks (2021) 'Work stream 3: A New Solution — Blockchain & eID', available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/deexp/ecb.deexp211011_3.en.pdf (accessed 30th April, 2023).

(21) European Central Bank (2022) 'Annex 1 — Front-end prototype providers technical onboarding package', available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs221207_annex1_front_end_prototype_providers_technical_onboarding_package.en.pdf?96894d1ebc6c998d75233c57bf1c66eb (accessed 30th April, 2023).

(22) Armelius, H., Claussen, C. A. and Hull, I. (2021) 'On the possibility of a cash-like CBDC', working

paper, Sveriges Riksbank, available at: https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf (accessed 30th April, 2023).

(23) Panetta, F. (2021) 'A digital euro to meet the expectations of Europeans', European Central Bank, available at: https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html#:~:text=We%20will%20do%20our%20best,euro%20is%20to%20be%20accepted (accessed 30th April, 2023).

(24) Chaum, D., Grothoff, C. and Moser, T. (2021) 'How to issue a central bank digital currency', SNB Work Paper, Schweizerische Nationalbank, available at: https://www.snb.ch/en/publications/research/working-papers/2021/working_paper_2021_03 (accessed 30th April, 2023).

(25) Gross, J., Sedlmeir, J., Babel, M., Bechtel, A. and Schellinger, B. (2021) 'Designing a central bank digital currency with support for cash-like privacy', SSRN, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891121 (accessed 30th April, 2023).

(26) Auer, R., Boehme, R., Clark, J. and Demirag, D. (2023) 'Mapping the privacy landscape for central bank digital currencies', *Queue*, Vol. 20, No. 4, pp. 16–38.

(27) Ballaschk, D. and Paulick, J. (2021) 'The public, the private and the secret: Thoughts on privacy in central bank digital currencies', *Journal of Payments Strategy & Systems*, Vol. 15, No. 3, pp. 277–286.

(28) Grothoff, C. and Moser, T. (2021) 'How to issue a privacy-preserving central bank digital currency', Policy Brief, SUERF, The European Money and Finance Forum, available at: https://www.suerf.org/docx/f_0ea841a00684473af118beb024287ce3_27227_suerf.pdf (accessed 30th April, 2023).

(29) Fanti, G., Lipsky, J. and Moehr, O. (2022) 'Central bankers' new cybersecurity challenge', International Monetary Fund, available at: https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr (accessed 30th April, 2023).

(30) Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wüst, K. and Zhang, F. (2020) 'Design choices for central bank digital currency: Policy and technical considerations' NBER working paper, available at: https://www.nber.org/system/files/working_papers/w27634/w27634.pdf (accessed 30th April, 2023).

(31) Federal Reserve Bank of Boston and Massachusetts Institute of Technology, ref. 12 above.

(32) *Ibid*.

(33) European Central Bank, ref. 21 above.

(34) European Central Bank, ref. 15 above.

(35) Panetta, F. (2022) 'A digital euro that serves the needs of the public: Striking the right balance', introductory statement at the Committee on Economic and Monetary Affairs of the European Parliament, Brussels, 30th March.

(36) European Central Bank (2022) 'Progress on the Investigation Phase of a Digital Euro', available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf (accessed 30th April, 2023).

(37) Minwalla, C., Miedema, J., Hernandez, S. and Sutton-Lalani, A. (2023) 'A central bank digital currency for offline payments', Bank of Canada, available at: https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/ (accessed 30th April, 2023).

(38) Deutsche Bundesbank (2021) 'Eurosystem experimentation regarding a digital euro, Research workstream on hardware bearer instrument', available at: https://www.bundesbank.de/resource/blob/873282/bd327431598f204c2ebac99f197ce863/mL/eurosystem-experimentation-regarding-a-digital-euro-data.pdf (accessed 30th April, 2023).

(39) Mihai, C., Gu, W. C., Kumaresan, R., Minaei, M., Ozdayi, M. and Price, B. (2020) 'Towards a two-tier hierarchical infrastructure: An offline payment system for central bank digital currencies', arXiv preprint arXiv:2012.08003.

(40) *Ibid*.

(41) Bank for International Settlements (2023) 'Project Polaris — A Handbook for Offline Payments with CBDC', available at: https://www.bis.org/publ/othp64.htm (accessed 15th May, 2023).

(42) Deutsche Bundesbank, ref. 38 above.

(43) Allen, ref. 30 above.

(44) Deutsche Bundesbank, ref. 38 above.

(45) Panetta, ref. 35 above.

(46) European Central Bank, ref. 36 above.

(47) Cheng, P. (2022) 'Decoding the rise of central bank digital currency in China: Designs, problems, and prospects', *Journal of Banking Regulation*, Vol. 24, pp. 156–170.