SUOMEN PANKKI
18 11
EUROSYSTEM
FINLANDS BANK

Reining in the expectations of offline payments

A: 130 • 2023

Expository Studies

Julia Nurminen
Johanna Schreck

The views expressed in this article are those of the authors and do not necessarily reflect the views of the Bank of Finland.

ISBN 978-952-323-450-5, online publication
ISSN 1798-1069

Helsinki 2023

Contents

Abstract

In the recent decades, the evolution of the payments landscape has been driven by digitalisation and technological development. With consumer preferences and expectations changing and the use of cash declining, central banks in many jurisdictions have begun to explore digital alternatives that would be capable of preserving the unique properties of tangible cash in the digital age. An option under consideration is a central bank digital currency that functions offline, i.e., an offline CBDC.

The growing interest in offline CBDCs reflects the expectation that the utility of the digital form of publicly available money should closely match that of cash. This is unsurprising given that cash remains the cornerstone of the modern monetary system. It is a public good that comes with benefits such as built-in security features, immediate settlement, anonymity, general acceptability and inclusivity.

Whilst some argue that the aforementioned properties could be incorporated into a CBDC using tokenisation, Project Pluto, an empirical study on offline payments conducted at the Bank of Finland, suggests that the view may be overly optimistic. In fact, the findings of Project Pluto imply that this may be true regardless of whether a CBDC is balance-based or token-based. The prospect is also supported by the precedent set by the Avant card system, conceivably the first CBDC in the world.

Project Pluto demonstrates in particular that the token-based offline CBDC model is encumbered by certain technical and performance-related limitations as well as risks and challenges relating to counterfeiting and privacy. At the same time, the only identified benefit of the token-based model appears to concern the theoretical ability of a central bank to better control the amount of money in circulation. The findings indicate that replicating the properties of cash in a CBDC may at the minimum require certain trade-offs even if the design is based on tokenisation.

It is concluded that as there is likely to be limited demand for an offline CBDC that could fall short of, inter alia, user demands, the expectations placed upon it in terms of e.g. preparedness and contingency planning may also be disproportionate.[1]

Keywords: CBDC, tokenisation, offline payments, mobile payments

[1] We would like to thank our distinguished colleagues Tero Alhonen, Anthony Baltzar, Aleksi Grym, Janne Heikkilä, Mikko Honkajuuri, Kasperi Korpinen, Ossi Lehtonen and Meri Sintonen, who participated and provided valuable contributions in Project Pluto.

1. Introduction

Digitalisation and technological development have changed the payments landscape considerably in the recent decades. As payments have become increasingly digital, cash usage has also declined in many states. This is particularly true in the Nordic countries.

Central banks are well aware of this trend.[2] It has also encouraged many of the institutions to respond to the rapid evolution in order to secure access to a publicly issued money in the form of central bank digital currencies (CBDCs).

Whilst a CBDC is by definition a digital means of payment, a common expectation is that it should still resemble cash. Consequently, the CBDC discussion often intertwines with the topic of offline payments, the need for which may arise when digital payment methods that rely on network connection (e.g. 4G or Wi-Fi) are unavailable.

It is hardly surprising that some expect the evolved form of public money to mimic the properties of the conventional payment instrument. This is reflected in the commitment and ambition of many central banks to develop an offline CBDC.[3] Hence, there seems to exist a prevailing design assumption that if we are designing digital cash, it should function offline.

However, it is doubtful whether the attributes of cash can actually be incorporated into a CBDC. To this end, we present a possible design for an offline CBDC based on an experimental peer-to-peer mobile payment application developed at the Bank of Finland. We also review some of the challenges related to offline CBDCs more generally. Particular attention will be paid to the token-based offline CBDC as it is often considered to constitute a more suitable technological solution for developing digital cash than the balance-based option.

Our analysis shows that an offline CBDC may not be able to fully replicate the properties of cash even if it is based on tokenisation. We note that there are multiple technical challenges encumbering the practical implementation of a token-based offline CBDC. It is also unclear whether there is currently enough demand for a CBDC suitable for digital offline payments given consumer expectations and technical preconditions relating to the product.

[2] See e.g. Sveriges Riksbank, Payments Report 2022 (December 2022), www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2020/1.-the-payment-market-is-being-digitalised/cash-is-losing-ground/; European Central Bank (ECB), Study on the payment attitudes of consumers in the euro area (SPACE) (December 2022), para. 3.2.1, www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html#toc7.

[3] See e.g. F Pannetta, The digital euro: our money wherever, whenever we need it (introductory statement at the Committee on Economic and Monetary Affairs of the European Parliament, Brussels, January 2023), www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123~2f8271ed76.en.html and ECB, Progress on the investigation phase of a digital euro (September 2022), para. 2.1, www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf?8eec0678b57e98372a7ae6b59047604b; proposal for a regulation on the establishment on of the digital euro, COM(2023) 369 final, Art 23(1), https://finance.ec.europa.eu/system/files/2023-06/230628-proposal-digital-euro-regulation_en.pdf; Bank of England and HM Treasury, The digital pound: a new form of money for households and businesses? (February 2023), Consultation Paper, www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf; Bank of England, The digital pound: Technology Working Paper (February 2023), www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf?la=en&hash=A97A5C2056FF5CD4D494B1E6A2EED7B8271ACA54; Central Bank of the Bahamas, Project Sand Dollar: A Bahamas Payments System Modernisation Initiative (December 2019), p. 10, www.centralbankbahamas.com/viewPDF/documents/2019-12-25-02-18-11-Project-Sanddollar.pdf.

Indeed, according to the findings of Project Pluto, the main benefit from the use of tokenisation appears to concern the theoretical ability of a central bank to better control the amount of money in circulation. Therefore, we conclude our analysis by showing that the objectives attached to offline CBDCs especially in the surrounding policy discussion may be disproportionate in comparison to its actual potential to serve as a viable complement to cash.

2. CBDC – digital cash?

The declining use of cash especially at point-of-sale and in person-to-person payments is evident in a recent study on the payment attitudes of consumers in the euro area.[4] Concurrently, the number of CBDC projects undertaken by public institutions seem to be increasing. These trends highlight the paradox facing central bankers today: whilst digitalisation and technological development have obviated the use of the traditional publicly available form of central bank money in many contexts, as evidenced by the broad range of digital payment methods available today, preserving the concept of cash remains mission-critical for central banks.

This owes to the fact that cash, together with central bank deposits, constitute the cornerstone of the modern monetary system. Furthermore, from a consumer point of view, banknotes and coins have distinctive properties that should arguably be replicated in any publicly issued forms of cash. The development and issuance of a CBDC may thereby be justified as a necessary response to the evolving operational context and as an alternative for commercial digital payment methods.

2.1. The properties of cash

The support for an offline CBDC can be understood to flow from the *sui generis* nature of central bank money, the essential role it plays in financial infrastructures and its public good nature. In particular, due to the public good attribute it is arguable that cash should serve as the benchmark that at least any publicly developed payment method or system should meet. In light of this, a more detailed account of the properties of cash is warranted.

First, paying by cash is *safe* because the settlement of the payment transaction takes place upon the payer handing a banknote or a coin over to the payee. The immediacy and finality of cash payments help to minimise counterparty risk. Moreover, the safety of cash payments is also enhanced by certain built-in security features which make the payment instrument easy to authenticate and relatively difficult to counterfeit.[5]

Acknowledging any possible jurisdictional differences relating to the legal form of money, banknotes and coins may generally be defined as *bearer instruments*. This commonly means that the rights entailing to the particular asset are held by the person with possession of it. The nature of cash as a bearer instrument also denotes that it suffices to authenticate the banknote rather than the person handing it over to the payee. This means that cash payments can be made *anonymously* because 'the legal identity of user is not verified when they access a service' or make a purchase.[6]

[4] ECB, SPACE (n2).

[5] A Lee, B Malone and P Wong, Tokens and accounts in the context of digital currencies (December 2020) FEDS Notes, Board of Governors of the Federal Reserve System, https://doi.org/10.17016/2380-7172.2822.

[6] ECB, Eurosystem report on the public consultation on a digital euro (April 2021), p. 18, www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf.

Privacy is often mentioned in parallel with the concept of anonymity. As digital payments require the involvement of a third party e.g. for the purposes of achieving settlement finality, they tend to leave behind traceable information. Indeed, in parallel with the rise of digital payment methods, payers may be sharing data which private entities seek to utilise, however, generally only to the extent permitted by law and within the limits set by a payer.[7] Alongside any potential commercial rationales, the data appetite of certain parties may also be attributable to the legal requirements concerning e.g. prevention of money laundering and terrorist financing.

In contrast, cash is in this sense untraceable because the issuing central bank only makes a note of the issuance and the final return of a banknote.[8] However, anonymity may also be seen as a source of vulnerabilities. Tracking down a fraudulent party in a cash payment chain is in effect impossible and a party's ability to dispute trades settled in cash may be limited in some instances. Regardless of the risks that full anonymity in particular may pose to payments, the payment system and the users, some have argued that the anonymity and privacy properties associated with cash should be preserved in a CBDC although it may be impossible in view of the currently applicable legal frameworks.

Finally, cash has conventionally been considered as an *accessible* payment method. The use of cash does not require the transacting parties to have access to smart phones, computers or a network connection. Additionally, cash may be the only form of money with legal tender status in certain areas. This entails that in principle, the payer has the general right to pay with cash and the payee is obliged to accept it. The accessibility property can be further safeguarded with legislation.[9]

2.2. The token hype

Some may argue that the properties of cash would be best captured in a token-based digital version of publicly available central bank money.[10] However, tokenisation is also a technological concept underpinning many crypto assets. This has at times resulted in terminological confusion.[11] Hence, we take the opportunity to clarify the definition of

[7] Generally on the topic, see e.g. R Garratt and M Lee, Monetizing Privacy (January 2021) Staff Report No. 958, Federal Reserve of New York, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr958.pdf?sc_lang=en.

[8] Y Mersch, Digital Base Money: an assessment from the ECB's perspective (Speech at the Bank of Finland, Helsinki, January 2017), www.ecb.europa.eu/press/key/date/2017/html/sp170116.en.html.

[9] In the case of Finland, see e.g. Bank of Finland, Lainsäädäntöesitys - käteispalveluiden taso ('Legislative proposal - the level of cash services') (March 2022), www.suomenpankki.fi/globalassets/fi/media-ja-julkaisut/lausunnot/documents/lainsaadantoesitys-kateispalveluiden-taso-03032022.pdf, setting forth a proposal to initiate a legislative review to secure the provision of cash services at a reasonable level. In the case of Sweden see Lag om ändring i lagen (2010:751) om betaltjänster ('Act amending the act (2010:751) on payment services'), requiring Swedish credit institutions and branches of foreign credit institutions to provide cash services to a satisfactory extent throughout the state. See also the European Commission proposal for a regulation on the legal tender of euro banknotes and coins of 28 June 2023, COM(2023) 364 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0364&qid=1689234403517.

[10] For further discussion, see e.g. H Armelius, CH Claussen and I Hull, On the possibility of a cash-like CBDC (February 2021) Sveriges Riksbank, Staff Working Memo, www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf.

[11] Many central banks have emphasised that regardless of the technology used in a CBDC, they are not crypto assets. See e.g. Bank of England and HM Treasury, The digital pound: a new form of money for households and businesses? (February 2023) Consultation Paper, p. 13, www.bankofengland.co.uk/-

tokenisation and tokens in relation to CBDCs by first providing a high-level overview of their use in the field of crypto.

The best-known example of tokenisation in the crypto asset context is probably Bitcoin. Bitcoin can be characterised as a peer-to-peer computer network for recording transactions. The network is maintained by participants who may be incentivised to run the relevant software by rewarding them with the same native units the ledger keeps an account of.[12] Therefore, in addition to being a network, Bitcoin also refers to a programmatically defined asset on a blockchain, the value of which appears to derive exclusively from trading on the secondary market.[13] These representations of value or rights are commonly called tokens.[14]

Tokenisation has attracted further attention due to the development of programmes running on the Bitcoin-inspired Ethereum blockchain. In the case of Ethereum, tokenisation is essentially used to offer code-based programmes that can execute agreements automatically in the particular type of distributed ledger. These programmes are known, arguably somewhat misleadingly in a legal sense, as smart contracts.

The misplaced proposition that using distributed ledger technology (DLT) such as blockchain is essential whenever tokenisation comes into play may derive from the increased interest in crypto assets and the consequent token hype. It is also noteworthy that a system based on DLT may in fact be either token-based or balance-based.[15] It is understood that the former would mean that the participants to the system keep record of the total outstanding value issued whilst the latter would simply entail that the parties share the responsibility for keeping an account of individual holdings.[16]

2.3. Nothing new under the sun

Regardless of the token hype and its ostensible connection with offline payments, an offline CBDC is by no means a novel idea. The Avant card was developed by the Bank of Finland already in the 1990s and it was launched in an era when continuous online connection was unreliable.[17] As in an offline CBDC, the foundational design principle for the then pioneering payment method was its strong resemblance to cash.[18] In practical terms this meant e.g. that the card had to be prefunded.[19]

Alongside public sector initiatives, private sector has produced offline payment solutions in the past as well. Examples include Mondex and to some extent the competing VisaCash solution. The former was an electronic cash scheme that enabled value to be stored on a payment card. The Mondex payment platform also seemed

/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf; ECB, Report on digital euro (October 2020), Annex 2, www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

[12] Such parties would be referred to as miners.

[13] A Lee, B Malone and P Wong, Tokens and accounts in the context of digital currencies (n6).

[14] However, it should be noted that as a system, Bitcoin can be interpreted to fit the definition of both token-based and balance-based model. See e.g. R Garratt, M Lee and A Martin, Token- or Account-Based? A Digital Currency Can Be Both (12 August 2020), Federal Reserve Bank of New York, https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/.

[15] A Grym, Lessons learned from the world's first CBDC (August 2020) Bank of Finland Economics Review, p. 15, https://publications.bof.fi/bitstream/handle/10024/43587/BoFER_8_2020.pdf?sequence=1&isAllowed=y.

[16] ibid.

[17] ibid., p 14.

[18] ibid., p. 3.

[19] ibid.

capable of operating entirely offline. This was because the payments made using the platform did not need to be authorised by a third party.[20] Like the Avant card, it appears that the fully commercial digital cash solution failed to achieve sufficient acceptance rate.

It may be possible to attribute the limited success of the Avant card system and Mondex to the fact that they emerged in an era when digital services were not yet a common norm. However, even if the two had simply been ahead of their time, network connection has since become something of a precondition for digital payments.

First, the global data network enables payers to freely access a multitude of payment instruments and use cases for them, as well as liquidity. Digital payments can also reach a global audience and thereby boost the commercial opportunities available e.g. for merchants. Moreover, it is probable that online payment methods are more convenient and efficient in terms of the costs accrued by users. This may be particularly true if the user is required to spend time and money to either fund their reloadable offline payment instrument or obtain a new non-reloadable instrument. Similar reasoning applies to cash given that it must be withdrawn from a distribution point such as cash machine before it can be spent.

Second, network connectivity also enhances the security of payments as the control mechanisms available are relatively diverse and straightforward to implement. Additionally, access to a network helps to overcome technical limitations such as those related to storage of data.[21] Thus, the very aspects of digital technology that we consider valuable, useful – even essential – often require network connectivity.

3. Materialising an offline CBDC

The previous sections outlined some motivations driving the development of offline CBDCs. The following sections will turn to assess two of the technological solutions available for materialising the vision of digital cash.

The technological deliberations relating to offline CBDCs often focus on a choice between a balance-based and a token-based model. The token-based CBDC can be considered to better facilitate anonymous peer-to-peer offline payments and therefore, a more suitable option for developing a digital form of cash.[22] However, this does not imply that an offline payment system should by default be based on tokenisation. Additionally, it should be noted that the token-based model may equally well be used to operate an online payment system.

3.1. Balance-based model

In essence, the balance-based model entails that its user holds funds on a payment account located in a ledger that keeps the record of the balance. Since the balance-based model is already widely used technological solution in payments, it suffices to state that it is primarily concerned with the identification and authentication of the payer in connection with a payment transaction.[23] If the identity of the payer is successfully authenticated and their right to use the funds thereby verified, the account balance will

[20] J Westland et al., Customer and merchant Acceptable of Electronic Cash: Evidence from Mondex in Hong Kong (1998) 2(4) ICEJ, p. 7, www.jstor.org/stable/27750864.

[21] See e.g. ECB, Annex I: Functional and non-functional requirements linked to the market research for a potential digital euro implementation (January 2023), p. 44, www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf?8f308548cc80b5f187a5560bd50e72ce.

[22] H Armelius, CH Claussen and I Hull, On the possibility of a cash-like CBDC (n11).

[23] A Grym, Lessons learned from the world's first CBDC (n15), p. 14.

be updated in accordance with the details of a signed transaction message transmitted across a payment network.[24]

3.2. Token-based model

For the purposes of this paper, a token is defined as a digital piece of data or file containing information and representing monetary value expressed in the national unit of account.[25] In this instance, an offline CBDC is by its fundamental legal nature a central bank liability regardless of whether tokenisation is used or not.

Alongside monetary value, tokens may also contain other information such as a time stamp and an identifier. The attributes help to verify the authenticity of the token. Tokens may also carry historical transaction data or data relating to the payer and payee. Interestingly, it is common that crypto tokens contain information about the transacting parties. However, it should be noted that the practical feasibility of storing such data in a token may be limited e.g. due to potential issues that relate to data protection and privacy. These issues will be discussed in more detail in section 5.

It is possible to generate CBDC tokens in two alternative ways. The first approach has been trialled in the e-krona pilot undertaken by the Swedish Riksbank.[26] A key feature of the option is that each token can be used only once. This means that the spent tokens are redeemed (including destruction) after the transaction has been settled and new tokens are generated for a subsequent payment.[27] It follows that the payment device must be capable of generating and redeeming tokens.

The second approach involves the issuance of reusable tokens that circulate in the economy until they are redeemed by the issuing central bank. In other words, the right to generate and redeem tokens is reserved exclusively for the central bank.

4. Case study

4.1. Project Pluto

To date, most central banks have offered digital central bank money only to financial institutions using balance-based systems. This is also one of the key reasons why practical testing of any proposed token-based CBDC is important.

In light of this, an offline CBDC experiment in which a simple peer-to-peer mobile payment application was recently conducted at the Bank of Finland. Project Pluto focused on the token-based model in particular. The objective was to identify opportunities and challenges related to offline CBDC payments and whether the token-based model could be superior to the balance-based model. An overview of Project Pluto is provided in the annex.

In contrast to the Riksbank's e-krona pilot, the Pluto application utilises reusable tokens. This is for two primary reasons: First, allowing remote payment devices to generate CBDC tokens may increase the risk of counterfeiting. Second, experimenting with reusable tokens is considered to carry greater novelty value and thus, more opportunity for learning.

[24] ibid., p. 15; Committee on Payments and Market Infrastructures, Central bank digital currencies (March 2018), Bank for International Settlements, p. 4, https://www.bis.org/cpmi/publ/d174.pdf.

[25] See also e.g. Sveriges Riksbank, Economic Review 2022 No. 2 (2022), pp. 6–25, www.riksbank.se/globalassets/media/rapporter/pov/engelska/2022/economic-review-2-2022.pdf.

[26] Sveriges Riksbank, E-krona, www.riksbank.se/en-gb/payments--cash/e-krona/.

[27] Sveriges Riksbank, E-krona pilot Phase I (April 2021), p. 6, www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf.

One crucial question regarding offline payment applications is the access to secure elements (SE) as a measure to make the solution as tamper resistant as possible. SEs can be found in many mobile devices and SIM cards but not all. This kind of hardware-based approach to security has traditionally been seen superior to software-based solutions.[28] Nevertheless, relying on the device's SE does not come without challenges. This is because not all smartphones are equipped with a SE and not all manufacturers provide access to them. The issue was recognised but not addressed in detail in Project Pluto because the scope of the experiment excluded such security measures.

4.2. Funding and defunding

Both the balance-based and token-based offline wallets developed and tested in Project Pluto require to be prefunded. In practical terms this means that in resemblance to cash withdrawals, the end-user must transfer funds from their online CBDC account to their offline CBDC wallet whilst online. This also implies that the user cannot access their online CBDC account in an offline mode.

Although the prefunding requirement constitutes a major weakness of the system in terms of usability, from a central bank perspective the feature seems unavoidable. This owes to the fact that, if the payment transaction is initiated offline but the final settlement occurs only after the device is back online (store-and-forward model), the central bank may lose a visibility over its balance sheet and be exposed to a credit risk that it is unwilling to assume. The credit risk could materialise e.g. if the payer acts fraudulently or in case of a malfunction in the payment application.

The balance-based offline wallet developed in Project Pluto can be funded by the user by transferring money from the online account to the offline wallet. The online account is debited, the offline wallet is credited and the balances are updated accordingly. As the payment device is required to be online during funding and defunding, the synchronisation of the device with the central bank server also takes place immediately. In other words, contrary to the token-based model, the balance-based model does not involve any tokenisation of funds but simply the updating of the balances.

Funding the token-based offline wallet also requires that the online account is first debited for the correct amount. Subsequently, corresponding sum of one-cent tokens are generated on the central bank server, illustrating the restriction that funds cannot be tokenised locally. Each token is assigned a unique identifier before they are transferred to the user's offline wallet. A new wallet balance is calculated on the basis of the aggregate value of tokens stored therein.

As already indicated above, defunding the offline wallet requires the payment device to be online. Whilst the balance-based model is again simply concerned with updating the offline and online balances, in the token-based model the tokens are redeemed and destroyed by the central bank on its server.

4.3. Paying

Higher privacy levels and anonymity associated with the token-based model can relate to what is identified in the course of a payment transaction. The token-based model might theoretically enable fully anonymous payments. However, due to regulatory requirements, the identity of the user might still need to be verified when they are onboarded.

A common feature of the two models developed in Project Pluto is that the transacting parties need to be in proximity of each other in order to make and receive

[28] BIS Innovation Hub, Project Polaris: Handbook for offline payments with CBDC (May 2023), p. 30. See https://www.bis.org/publ/othp64.pdf.

offline payments. The parties' devices are connected using Bluetooth. The payment transaction contains information about the payee's wallet and the amount to be transferred. Once it has been verified that the payer's wallet has sufficient funds, the payment is sent and the payer's offline wallet is debited in accordance with the transaction details. Finally, the payer receives a push notification confirming a successful payment. After the devices return online, the details will be reconciled with the central bank server.

To create a transaction with the token-based model, information regarding the payee's wallet and the number of tokens to be transferred is needed. The transaction also contains a time stamp. With a view of ensuring that the tokens have been transferred and received successfully, they are locked until released from the payer's wallet.

5. Issues and questions related to offline CBDCs

One key objective of Project Pluto was to form a more concrete understanding of the risks and challenges of offline CBDCs. In this respect, specific attention was paid to tokenisation. The following sections will study the uncertainties that currently encumber the token-based model.

In short, the key concerns of offline CBDCs identified in Project Pluto include those related to counterfeiting, privacy, performance and data transfer. These issues could in turn affect the convenience and user experience of an offline CBDC and thus, its utility in terms of preparedness and contingency planning. Therefore, it is also likely that certain trade-offs dependant on the risk appetite of a central bank will be necessary when designing an offline CBDC regardless of whether it relies on tokenisation or is based on the balance-based model.

5.1. Counterfeiting

One of the major risks of offline CBDCs is counterfeiting. It can be approached from two perspectives. First, if the payment device generates and redeems tokens, a bad actor may be able to take over the device and generate more tokens. In Project Pluto, this risk was controlled by allowing only the central bank server to generate and redeem tokens.

Nevertheless, even if tokens can only be generated and redeemed by the central bank, counterfeiting may still occur if the bad actor succeeds in cloning tokens already stored in the offline wallet. In a similar vein, manipulating the offline balance may also be possible. The risk of counterfeiting by cloning could not be overruled in Project Pluto. Hence, references to counterfeiting should in the following sections be understood to mean the risk of counterfeiting by cloning tokens.

5.2. Scalability and risk allocation

Notwithstanding the fact that the counterfeiting risk can be controlled to an extent with certain technical measures and design choices, it may still be impossible to eliminate it in full. The risk is also not unique to digital tokens but applies to cash as well. However, this is not to say that the risk profiles and consequences of counterfeiting are the same in both cases.

Counterfeiting cash is a production-heavy process: alongside the necessary technical expertise on the unique patterns, special inks, holograms and printing of banknotes, the bad actor also requires access to raw materials and machinery. In other words, there exists several production-related factors that limit the ability of the bad actor to counterfeit banknotes. Whilst this does not fully prevent the production of counterfeits, there exist inherent limitations to scaling up such activity.[29]

With regard to counterfeiting digital tokens, the bad actor does not, at least in theory, need any physical resources apart from a computer or mobile device. Furthermore, the marginal cost of producing more than one counterfeited digital token is essentially zero. Therefore, counterfeiting digital tokens may be more enticing than counterfeiting cash.

It is for the reason of limited scalability that central banks are willing to assume the risk of banknote counterfeiting. It does not seem probable that confidence in a payment system erodes excessively if a marginal number of counterfeit banknotes circulate in the economy. Furthermore, because of limited damages, it may not even be practical or feasible to make banknotes infinitely difficult to counterfeit. By contrast, counterfeiting digital tokens scales up efficiently. This means that the integrity of the payment system could be compromised if the effectiveness of the safety features of an offline CBDC cannot be guaranteed.

We argue that the consequences of such loss of trust in an offline CBDC system would be more severe than in the case of cash. News of incidents in which counterfeited banknotes are discovered do not usually result in people disposing of their cash holdings. This may be attributable also to the fact that people are familiar with the risk or that they can physically examine the authenticity of banknotes.

Controlling the damages deriving from counterfeit digital tokens could also require the reconsideration of the conventional risk allocation rules. For instance, according to the general rule applying to banknotes in Finland, the payee bears the risk of economic loss if the payment instrument proves to be a counterfeit. If this same approach was to apply to digital tokens, the attractiveness of the payment method could decline considerably. Additionally, it is doubtful whether a CBDC user would be willing to assume the risk that a token accepted by the payment device may in fact be a counterfeit and therefore, worthless.

It follows that deviation from the general rule may be justifiable in the context of digital tokens given that central banks may be best able to manage the risk of counterfeiting as well as control and minimise its impacts. However, it is questionable whether a central bank could assume the potentially significant damages resulting from the materialisation of the credit risk.

5.3. Dealing with counterfeiting: traceability

One way to control the risks of offline payments is to set and enforce holding and transactions limits. However, there exist additional measures which may also enhance the safety of offline CBDC payments.

As a general principle, the payment devices used to make offline CBDC payments should return to an online mode occasionally. This is necessary because it seems impossible to detect counterfeited tokens for as long as the payment devices remain offline. Moreover, requiring the devices to connect online on a regular basis enables the development of more specific features that are aimed at enhancing the safety of the system.

[29] See e.g. Europol, Possibly largest ever bust of banknote counterfeiters in the history of the euro (17 July 2020), www.europol.europa.eu/media-press/newsroom/news/possibly-largest-ever-bust-of-banknote-counterfeiters-in-history-of-euro; Europol, Hit against euro counterfeiters linked to the Camorra (20 May 2021), www.europol.europa.eu/media-press/newsroom/news/hit-against-euro-counterfeiters-linked-to-camorra#:~:text=On%2020%20May%202021%2C%20Europol,distribution%20of%20counterfeit%20euro%20banknotes%2C.

To start with, in the token-based model a digital token can be assigned with a unique identifier. Combined with a recurring reconciliation with the central bank server, the feature allows the tokens to be traced. In practical terms this means that once the payment device returns online, the central bank can detect and redeem counterfeit tokens using the unique identifiers assigned to each of them. As a result, the central bank can at least in theory exercise more precise control over the total amount of money in circulation.

The issue, however, is that transaction chains cannot be traced if the payment devices remain permanently offline. As it is almost impossible to prepare for such a situation, the risk of some devices not returning online at all is significant. This owes to the fact that in principle, a chain of just two devices that remain offline is needed to make tracing impossible, as illustrated in chart 1.

To summarise, in the token-based model it generally suffices to verify the authenticity of a single token. Furthermore, the total amount of money can only be increased on the central bank server using a specific encryption key. By contrast, the balance-based model does not allow the validity of the balance to be verified without reconciling all past transactions. Therefore, the balance-based model seems to entail a higher theoretical risk of a bad actor managing to increase the balance of the offline wallet. This is because to detect that a balance has been illegitimately manipulated, all past payment transactions would need to be scrutinised.

This means that in the balance-based model, it is possible to verify the counterparty and the payment device but not the balance until the device is reconciled with the central bank back-end. In the token-based model the counterparty, the device and the monetary value, i.e. the tokens, can all be verified.

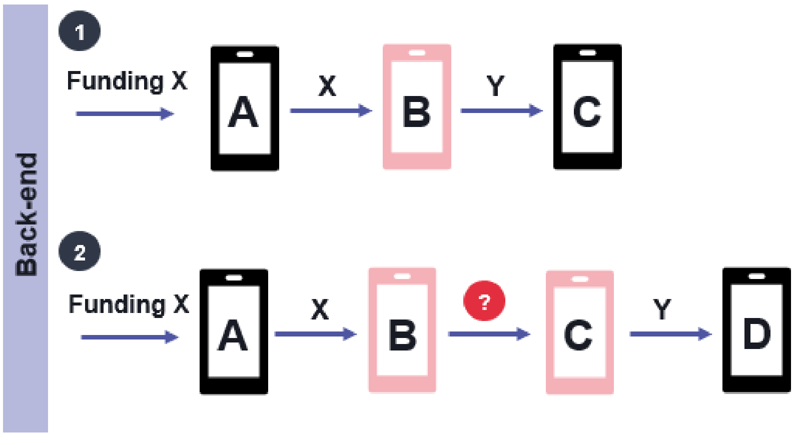
Chart 1. **The risk of devices staying offline**

THE RISK OF DEVICES STAYING OFFLINE

The figure below shows two transaction chains where a token (X) is transferred between several devices. This illustrates the problem that arises if payment devices stay offline. An assumption is that when a device comes back online it can verify that the tokens it holds are in fact valid. The device performs checks also in offline mode, but the online verification with the back-end ledger is final.

In the picture mobile devices coloured red stay offline whereas the black phones return to online mode soon after they have made the transactions.

In transaction chain #1 device A is in offline mode and sends a token X to device B. Device B then sends a counterfeited token Y to device C. The device C only detects the counterfeit when it switches to online. Now from the transaction history of the devices the back-end can plausibly state that B is the source of the counterfeit even if B stays offline. This is because it is possible to mirror the transaction chain through information received from wallets A and C when they enter online mode.



In transaction chain #2 devices A and D return to online mode after completing the transactions. From that information we can observe that A has transacted with B and D has received a counterfeited token from C. It is impossible to detect whether B or C has produced the counterfeit. There is also no way of knowing whether there have been more devices in between B and C.

This simple example is not complete but helps to demonstrate how important it is that devices return to online mode regularly.

5.4. Dealing with counterfeiting: blacklisting

The risk of counterfeiting could also be managed by gathering information about bad actors onto a blacklist. The blacklist would be saved and updated locally on a payment device each time it returns online, enabling the device to automatically recognise blacklisted users and refuse payments from them.

The transaction history of a blacklisted user would also be reviewed each time their respective device connects online. If a user was added to the list inadvertently or incorrectly, they could be removed from it. The transaction history could then be used to trace the actual bad actor instead. Updates of the blacklist could also serve as incentive for the users to return online with sufficient frequency as the risks faced by an individual users would consequently also be mitigated.

5.5. Privacy

The safety of offline CBDC payments could be further improved by allowing a wider data set to be stored inside the tokens. However, it should be noted that implementing certain security measures and simultaneously ensuring that the privacy of a user is adequately protected is a balancing act. This is particularly true in the case of offline CBDCs because the number of control mechanisms available is limited due to the lack of continuous network connectivity.

From a privacy perspective the above means that storing and transferring payment transaction data and personal data inside and with the token may need to be assessed against certain relevant legal frameworks. Whilst the exact regimes may vary from one jurisdiction to another, the general principle is that sufficient safeguards need to be in place to address e.g. breaches of privacy and data protection.

In Project Pluto, the decision to store data elsewhere on the payment device rather than inside the token was partially based on these privacy concerns. In particular, it was recognised that storing data in a reusable token could compromise bank secrecy.

Once the payment device is synchronised with the central bank back-end, the information saved on the device can be deleted. It should be noted that this approach does not address the policy issue concerning the ability of a public entity such as a central bank to monitor payment transaction data and personal data.

Apart from the potential legal and regulatory challenges, the inclusion of large data sets in a digital token would also make the system computing-intensive. This could in turn decrease operational efficiency. The issues related to performance and data transfer will be discussed in more detail next.

5.6. Performance and data transfer

A data-rich token design can easily lead to challenges in terms of system performance. However, one key learning from Project Pluto was that even the simplest of the token models is encumbered by performance-related issues. This turned out to be true even in the case where one-cent tokens contained no other data apart from a unique identifier and a watermark. More specifically, performance-related issues emerged because the amount of data transferred increased linearly with the monetary value transferred.

The payment system's performance is also affected by the choice of data transfer technology. The application developed in Project Pluto uses a Bluetooth connection with limited speed and capacity. This could potentially be a significant problem especially if the CBDC promises real time transaction settlement. Furthermore, it would probably be difficult for the user to accept that the payment transfer speed depends on the amount of money transferred.

The problem underscores the challenge of reusable tokens whereby the number of tokens transferred becomes very large even in low-value transactions. Whilst using chippable single-use tokens might solve the problem in theory, in practice it might introduce other issues related to security and performance as tokens would need to be generated on the local device, as described earlier.

Even if the token transfer rate could be optimised and the theoretical maximum increased, challenges arise in terms of the system's service promise. From the perspective of the user, it makes little sense if the speed of the service depends on value of the transaction.

Data transfer performance could be enhanced by using near field communication technology (NFT). Nevertheless, the wider adoption of NFT would require access to certain hardware and software components which certain mobile device manufacturers currently restrict.[30]

Chart 2. **Calculations concerning the transfer of tokens**

Transferring tokens via Bluetooth

The Pluto Project team offered a few rough calculations that illustrate some of the technology constraints on token-based systems.

The theoretical data transfer rate over Bluetooth (BLE 5.0) is 2 megabits (250,000 bytes) per second. The size of one token is about 36 bytes. The theoretical maximum number of tokens that can be transferred is therefore:

$$250{,}000 / 36 \approx 6{,}944 \text{ tokens} = 69.44 \text{ tokens per second}$$

However, due to the maximum size of the file (265 bytes) and additional costs for sending the packets, the data transfer rate is only about 1.43 megabits (178,750 bytes) per second. So, the number of tokens that could be transferred is:

$$178{,}750 / 36 \approx 4\ 965 \text{ tokens} = 49.65 \text{ tokens per second}$$

These calculations do not consider the fact that each file also requires the transmission of metadata such as the transaction to which the tokens belong. The transfer of this data further slows transfer speed and performance.

5.7. Convenience and user experience

A core issue in the design of any new payment method or system is whether there will be any demand for it. Payment markets are heavily affected by network effects. For a new retail payment method to gain popularity, both consumers and merchants in particular need to adopt it. Naturally, when it comes to a public good designed and issued by a central bank, its adoption can be encouraged through legislation and regulation.

A key selling point of offline payment methods, including an offline CBDC, is that they can be used even when there is no network access. This arguably facilitates digital payments even if the users are outside network coverage or networks have failed as a result of e.g. cyberattack or natural disaster.

However, the user experience could be far from seamless. To use an offline payment solution like the one developed in Project Pluto, the user would need to adopt the payment method and fund the payment offline CBDC wallet while online and before they are able to operate without network connection. This means that a user would need to prepare in advance by downloading the payment application and prefunding the offline wallet.

[30] European Commission, Antitrust: Commission sends Statement of Objections to Apple over practices regarding Apple Pay (Brussels, May 2022), https://ec.europa.eu/commission/presscorner/detail/fi/ip_22_2764.

The prefunding functionality creates a degree of difficulty when it comes to tapping into offline payments. Prefunding a physical wallet is a familiar course of action when we think of cash and physical wallets: it requires locating a cash machine and withdrawing money ahead of the moment it is needed.

Yet studies about consumer payment habits and behaviour conclude that people generally look for convenient, easy, fast and secure ways to pay. According to the European Central Bank study on payment attitudes of consumers, convenience was deemed a crucial feature when it comes to the adoption of a new payment method.[31] Payment trends such as contactless, mobile and embedded payments suggest that consumers and merchants expect paying to be increasingly effortless. A prefunded offline device hardly fits the bill.

When euro area citizens were asked what they considered to be the main advantages of cash, their responses were topped by the ability to track spending, anonymity, immediate settlement, wide acceptance, ease of use and speed.[32] Still it is questionable whether all the attributes inherent in cash can be incorporated into an offline CBDC. Even if a *per se* likeness to cash could be achieved by using certain technological solutions such as tokenisation, there are factors that will always limit the extent to which the properties of cash can be implemented in an offline CBDC.

First, as shown above, the central bank needs a remote central ledger for keeping record of the digital central bank money in order to control its balance sheet and the issuance of money. In practice, this means that the payment device must return online from time to time, i.e., an offline CBDC can never fully operate offline. Second, offline CBDC payments cannot be completely anonymous as the issuer of the CBDC, or other relevant intermediary responsible for the distribution, should comply with relevant legal and regulatory requirements. Third, it seems impossible to operate in a digital environment without leaving any traces behind.[33]

5.8. Preparedness

An interesting question relating to offline payments concerns its utility in terms of preparedness and contingency planning. Although the use of cash is decreasing, exposure to e.g. hybrid threats such as cyberattacks as well as the general uncertainty in the financial sector operating environment is increasing. An offline payment method developed by a central bank could seem like an obvious solution for a viable backup system. However, certain characteristics of an offline CBDC may prevent it from fulfilling this function.

First, when there is no network connection available, individuals would only have access to the funds already in their prefunded offline CBDC wallet. Thus, for it to be useful in times of crisis, the public awareness of the offline CBDC would probably need to be extremely high and its adoption rate close to universal.

Cash, however, is deemed a familiar, safe and trusted payment method. It can also be distributed without network connection. Moreover, CBDC designs may rely heavily on the banking sector for distribution, including the funding and defunding of offline CBDC wallets. This could effectively result in a situation where the unbanked population continue to rely on cash as they might not have access to bank accounts or mobile devices necessary for the distribution and use of the CBDC.

Whilst an offline CBDC could supplement the existing payment methods and indeed, add to the overall resilience of a society in terms of the number of payment methods and systems available, it certainly is not a panacea. Instead, offline CBDCs are currently affected by numerous issues related to performance, usability and security. For an offline

[31] European Central Bank, SPACE (n2).

[32] ibid.

[33] H Armelius, CH Claussen and I Hull, On the possibility of cash-like CBDC (n11).

CBDC to function as a backup system, it is necessary to either resolve the aforementioned challenges or determine the design-related trade-offs central banks and societies more generally are willing to make. Consequently, the value of an offline CBDC in terms of preparedness and contingency planning may currently be limited, implying that for the time being cash is in this sense a superior payment method.

6. Conclusions

The technologies for offline CBDCs have been available for several decades. Yet the number of offline payment methods offered has been near zero and the success of the few limited.

However, concurrently with the emergence of various CBDC projects, interest in offline payments is growing. This is due to the evolution of payment habits and preferences. The change has had an impact on the availability and general acceptability of cash, the only form of central bank money currently available to the public. Consequently, it is often argued that central banks should develop a digital equivalent of cash such as an offline CBDC. However, as the findings of Project Pluto and this paper suggest, it is uncertain whether an offline CBDC is fit for the purpose.

With regard to the objectives that can be achieved with an offline CBDC, one should be particularly careful in attaching policy expectations such as those related to preparedness, contingency planning and financial or digital inclusion to it. This is because in line with the analysis presented herein, an offline CBDC may fail to live up to them.

First of all, there must be sufficient demand for an offline CBDC. This means that the offline CBDC should be able to compete with the existing digital payment methods as well as with cash. We take the view that offline CBDCs may currently fall short of the standards set by the two. An offline CBDC can neither replicate all the properties of cash nor provide the same benefits that e.g. an online CBDC might be able to provide.

In fact, it may be that offline CBDCs combine the worst of both worlds. Like all digital payments, an offline CBDC requires access to electricity and data networks. In addition, the increased likelihood of fraud, together with technical issues affecting the performance of the offline CBDC system, mean that frequent online synchronisation is required. Similar to cash, losing one's mobile device would generally result in the user losing the money held in an offline wallet. The wallet would also have to be prefunded the same way cash needs to be withdrawn from a cash machine. Furthermore, an offline CBDC introduces some other novel and unresolved challenges that could affect the integrity of the payment system.

This suggests that balancing the technical design, use cases and policy objectives of an offline CBDC with the risk appetite and the tasks of central banks is necessary. For instance, ensuring the integrity of the payment system and the safety of payments may impose limits on the user experience and features of the offline CBDC. However, it should also be noted that compromises especially in terms of convenience may be acceptable if the principal use case of the payment method concerns contingency planning and preparedness.

This paper also points out that with the emergence of cryptocurrencies, tokenisation has become a popular buzzword. This hype may partly explain the popularity of tokens also in discussions on offline payments. However, as illustrated by Project Pluto, the concept of tokenisation is heavily dependant on the context.

Furthermore, putting the token hype aside, it is doubtful whether tokenisation can de facto add much value to the design of an offline CBDC. Indeed, the only clear benefit of the token-based model identified in Project Pluto concerns the ability of a central bank to better control the amount of money in circulation. However, even this benefit is of theoretical nature and possibly of limited practical importance.

If the performance-related drawbacks of a token-based model are disregarded, a choice between the models does not seem to have an impact on the user experience. Both solutions have their weaknesses when it comes to usability. In fact, a cumbersome user experience might be the greatest obstacle for an offline payment solution to overcome for it to avoid a fate similar to that of the first CBDC in the world.

Annex: Overview of Project Pluto

Project Pluto was an experiment conducted by the Bank of Finland. The project team applied one set of design choices and developed a simple offline CBDC payment application.

The functions available to a Pluto user are funding and defunding of the offline CBDC wallet in an online mode and offline transactions. While it is of course possible to transact in an online mode as well, this was not the experiment's focal point. The figure below illustrates the main functions of Pluto.

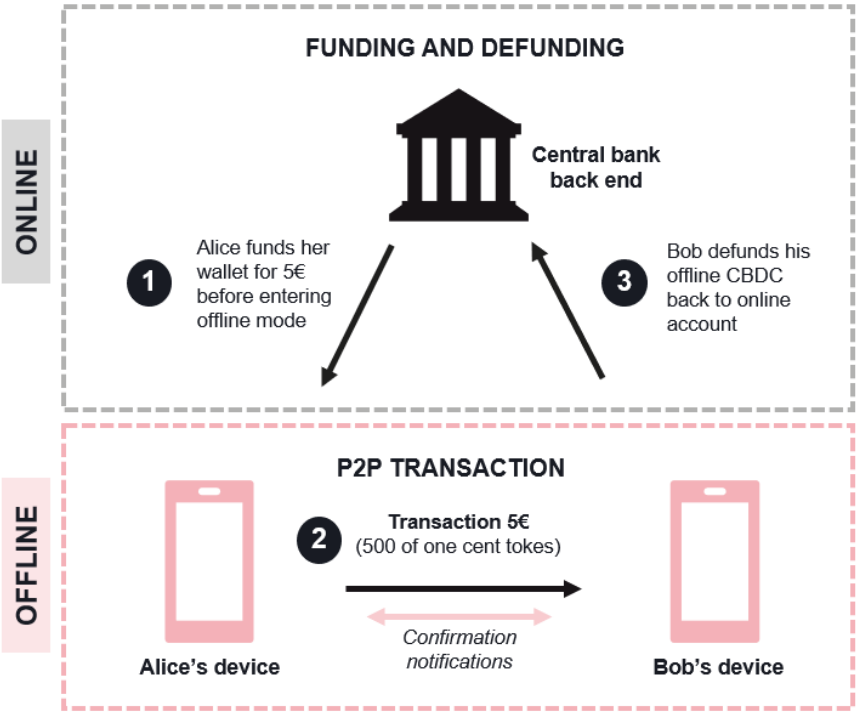
It should be noted that Project Pluto did focus on studying the distribution model of a CBDC. Hence, for the sake of clarity, it was decided that the central bank should be responsible for the distribution of the CBDC.

The Pluto offline CBDC wallet, accessible through the payment application, is connected to an online CBDC account on the central bank back-end.

(1) When the online CBDC account is debited, the central bank back-end generates an appropriate number of one-cent tokens. These tokens are consequently transferred to the offline CBDC wallet where the value is now also stored (bearer instrument). In the below example, Alice funds her offline wallet with five euros, corresponding to 500 tokens. This is also the balance of her offline CBDC wallet.

(2) In order to make an offline payment, the payer's and the payee's devices need to be connected using Bluetooth. Alice and Bob are connected via Bluetooth and Alice can transfer a maximum amount of five euros – the balance of her offline CBDC wallet – to Bob. Both receive a confirmation once the transfer has been completed and is final. The value/tokens are now stored on Bob's device.

(3) When Bob returns online, he can transfer these tokens to his online CBDC account (defunding). He can also choose to keep them in the offline wallet. Nevertheless, details of the tokens will be reconciled with the back-end server once the device is back in online mode. This is also when the authenticity of the tokens is confirmed.



Sources

Legislation

Lag om ändring i lagen (2010:751) om betaltjänster ('Act amending the act (2010:751) on payment services') (SWE)

European Union regulation

European Commission, Proposal for a Regulation on Markets in Crypto Assets, COM (2020) 593 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Proposal for a regulation on the establishment on of the digital euro, COM(2023) 369 final, Art 23(1), https://finance.ec.europa.eu/system/files/2023-06/230628-proposal-digital-euro-regulation_en.pdf

Proposal for a regulation on the legal tender of euro banknotes and coins of 28 June 2023, COM(2023) 364 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0364&qid=1689234403517

Other sources

Armelius H, Claussen CH and Hull I, On the possibility of a cash-like CBDC (February 2021) Sveriges Riksbank, Staff Working Memo, www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf

Bank of England, The digital pound: Technology Working Paper (February 2023), www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf?la=en&hash=A97A5C2056FF5CD4D494B1E6A2EED7B8271ACA54

Bank of England and HM Treasury, The digital pound: a new form of money for households and businesses? (February 2023), Consultation Paper, www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf

Bank of Finland, Lainsäädäntöesitys - käteispalveluiden taso ('Legislative proposal - the level of cash services') (March 2022), www.suomenpankki.fi/globalassets/fi/media-ja-julkaisut/lausunnot/documents/lainsaadantoesitys-kateispalveluiden-taso-03032022.pdf

BIS Innovation Hub, Project Polaris: Handbook for offline payments with CBDC (May 2023), https://www.bis.org/publ/othp64.pdf.

Central Bank of the Bahamas, Project Sand Dollar: A Bahamas Payments System Modernisation Initiative (December 2019), www.centralbankbahamas.com/viewPDF/documents/2019-12-25-02-18-11-Project-Sanddollar.pdf

Committee on Payments and Market Infrastructures, Central bank digital currencies (March 2018), Bank for International Settlements, https://www.bis.org/cpmi/publ/d174.pdf

Garratt R and Lee M, Monetizing Privacy (January 2021) Staff Report No. 958, Federal Reserve of New York, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr958.pdf?sc_lang=en

R Garratt, M Lee and A Martin, Token- or Account-Based? A Digital Currency Can Be Both (12 August 2020), Federal Reserve Bank of New York, https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/

Grym A, Lessons learned from the world's first CBDC (August 2020) Bank of Finland Economics Review, https://publications.bof.fi/bitstream/handle/10024/43587/BoFER_8_2020.pdf?sequence=1&isAllowed=y

European Central Bank, Annex I: Functional and non-functional requirements linked to the market research for a potential digital euro implementation (January 2023), www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf?8f308548cc80b5f187a5560bd50e72ce

European Commission, Antitrust: Commission sends Statement of Objections to Apple over practices regarding Apple Pay (Brussels, May 2022), https://ec.europa.eu/commission/presscorner/detail/fi/ip_22_2764

European Central Bank, Eurosystem report on the public consultation on a digital euro (April 2021), www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

European Central Bank, Progress on the investigation phase of a digital euro (September 2022), www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf?8eec0678b57e98372a7ae6b59047604b

European Central Bank, Study on the payment attitudes of consumers in the euro area (SPACE) (December 2022), www.ecb.europa.eu/stats/ecb_surveys/space/html/ecb.spacereport202212~783ffdf46e.en.html#toc7

Lee A, Malone B and Wong P, Tokens and accounts in the context of digital currencies (December 2020) FEDS Notes, Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/2380-7172.2822

Mersch Y, Digital Base Money: an assessment from the ECB's perspective (speech at the Bank of Finland, Helsinki, January 2017), www.ecb.europa.eu/press/key/date/2017/html/sp170116.en.html

Pannetta F, The digital euro: our money wherever, whenever we need it (introductory statement at the Committee on Economic and Monetary Affairs of the European Parliament, Brussels, January 2023), www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123~2f8271ed76.en.html

Sand Dollar, www.sanddollar.bs/about

Sveriges Riksbank, Economic Review 2022 No. 2 (2022), www.riksbank.se/globalassets/media/rapporter/pov/engelska/2022/economic-review-2-2022.pdf

Sveriges Riksbank, E-krona, www.riksbank.se/en-gb/payments--cash/e-krona/

Sveriges Riksbank, E-krona pilot Phase I (April 2021), www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf

Sveriges Riksbank, Payments Report 2022 (December 2022), www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2020/1.-the-payment-market-is-being-digitalised/cash-is-losing-ground/

Westland J et al., Customer and merchant Acceptable of Electronic Cash: Evidence from Mondex in Hong Kong (1998) 2(4) ICEJ, www.jstor.org/stable/27750864