A conceptual model for point-of-sale payment with retail CBDC*

Lars Hupel†

November 5, 2024

Abstract

The European Central Bank, like many other central banks, is pushing forward with the introduction of a Central Bank Digital Currency (CBDC). The Digital Euro is designed for retail use cases, which include peer-to-peer and merchant payments. Many different form factors are supported, with a focus on offline capabilities. While the picture is clear about how users can access and obtain CBDC, the acceptance side is not fully understood yet. CBDC will become one of many different payment options at points of sale. This paper analyzes the technical background of CBDC wallets and proposes a conceptual model of introducing CBDC payment to consumers.

JEL classification: E42, E58, G21

1 Introduction

Central Bank Digital Currency (CBDC) is an emerging development in digital payments, with most central banks worldwide researching, piloting, or even operating a digital version of cash. A common definition includes the following characteristics [20]:

- a digital representation of a country's or region's existing currency,
- issued directly by the central bank,
- usable in electronic payments,
- instantly settled, and
- being legal tender.

*This article has been accepted for publication in Journal of Payment Strategy & Systems and uploaded to SSRN with permission by the publisher.
†Giesecke+Devrient GmbH, Prinzregentenstr. 161, 81677 München, Germany, lars.hupel@gi-de.com

Furthermore, there is a distinction between *Retail CBDC*, which can be used by anyone in the jurisdiction, and *Wholesale CBDC*, which is only available for regulated financial institutions [29]. The name refers to the idea that the former allows for retail payments, whereas the latter would be used by financial institutions exclusively. This paper focuses on retail CBDC and investigates how this new instrument can be used for *Point-of-sale (POS) payments*.

1.1 Two-tier model

Users must have a way to interact with the CBDC ecosystem. Most central banks are exploring a two-tier model, whereby the central bank acts as the sole issuer of CBDC, but intermediaries—such as commercial banks, FinTech companies, and other financial institutions—are responsible for onboarding users and distributing CBDC. In this setting, intermediaries would provide services to users, according to the rules set by the central bank and regulators. In other words, central banks would not be dealing with users directly. This naturally extends to both consumers and merchants.

1.2 Wallets and payments

To better understand how CBDC payments differ to today's prevalent schemes, we first need to look at *wallets*. In CBDC, they are combinations of hardware and software that serve as containers of cryptographic keys. Depending on the CBDC implementation model, the keys may represent funds directly or serve as credentials to unlock funds stored elsewhere. Wallets should provide an easy-to-use interface that allows holders to conduct transactions. Both sides of a transaction would hold a wallet, and in most CBDC systems, they are symmetric: customer and merchant wallets differ only in their configuration. This allows for flexible payment flows, including direct peer-to-peer transactions. In this way, CBDC wallets resemble physical "cash wallets" more than other forms of digital wallets (see next paragraph).

1.3 Public money vs. private money

E-money operators, like PayPal, prepaid credit cards, and mobile money, are becoming increasingly popular around the world [33]. They, too, offer wallets to their customers. Their underlying instrument is a private form of deposit money, typically issued by a non-bank financial institution [21, 37].

CBDC however, is a direct claim from the user to the central bank, even in a custodial scenario (see also Table 1). This means the CBDC holdings managed by a financial intermediary through custodial wallets are not represented on that intermediaries' balance sheet [6]. The situation can be compared to, for example, securities accounts. In the event of the managing institution's insolvency, a user's holdings are not at risk [40].

Consequently, a wallet holder is not exposed to credit risk from an intermediary, only operational risk [9].

For this reason, CBDC payments behave differently from private payment rails because there is no need for a (typically deferred) settlement step. CBDC could change the role of acquirers, with small businesses potentially opting to accept CBDC directly on their own devices without intermediaries.

1.4 Structure of this paper

I will first introduce the concept of CBDC wallets and discuss their different types (Section 2), focusing on their design and form factors (Section 2.4). Then, I will explain two methods for initiating payment, namely pull and push, and how they relate to POS payments (Section 3). This includes an overview of technical communication channels to execute a payment (Section 3.1). Finally, I will develop a conceptual model of POS payments, considering the unique characteristics of a retail CBDC (Section 4).

2 Design of CBDC wallets

In cryptocurrencies and CBDC, wallets are the primary point of interaction between users and the system. While ample studies exist on the former, CBDC wallets are not yet widely investigated in the literature. Fortunately, wallets for both domains share similar traits: They manage cryptographic keys that unlock funds and enable users to transact.

Wallets are the primary way for customers to initiate payments and for merchants to accept payments, therefore they play a critical role at the point of sale. This means that their design is affected by the interaction of hardware, software, UI/UX, security, and the physical environment in which they are used.

CBDC, being a new form of public money, increases flexibility for customers and merchants, providing them with more choices and, therefore, fostering competition. The flip side is that now, many more payment scenarios must be accommodated in the already crowded space.

2.1 Wallet types

As a starting point, we can categorize wallets across the three dimensions relevant to this paper: custody [17, 39], embodiment, and offline capability [8] (see Table 1).

Naturally, the design choices of the overall system, such as the ledger, influences which wallet types are supported for a given CBDC. Yet, this is not an exact 1:1 mapping,

Table 1: Wallet types across the dimensions custody, embodiment, and offline capability

Dimension	Options	Explanation
Custody	Self-custodial/non-custodial	Wallet managed and under full control of the owner; funds are lost if the wallet and/or credentials are lost
	Custodial	Wallet managed and under full control of a licensed financial intermediary; the owner requests the managing intermediary to initiate a transaction; wallet access can be restored if credentials are lost
Embodiment[a]	Hardware	Logic implemented on (secure) hardware, such as dedicated chips
	Software	Logic implemented through software, such as an app on a smartphone
Offline capability	No offline capability	Transactions must be initiated and validated with online connectivity; this is standard for cryptocurrencies without a trusted third party
	Staged offline	No online connectivity required for transaction initiation, but settlement is deferred until connectivity is regained
	Intermittently offline	No online connectivity required for transaction initiation and settlement, but only for a limited period and/or limited number of transactions
	Fully offline	No online connectivity required for transaction initiation and settlement without restrictions

[a] The Bank for International Settlements chooses a slightly different categorization, borrowing terminology from the cryptocurrency community: "A cold wallet is a hardware device and can be operated offline, while a hot wallet is an online service based on web resources (and can be operated only by online users)" [8]. I have chosen to use "hardware" and "software" because those terms are more common in the CBDC community.

so multiple wallet types might coexist in the same ecosystem, as evidenced by the vast number of wallet implementations for cryptocurrencies [14].

2.2 The special case of offline capability

One of the most important motivations for CBDC adoption is offline capability. Many central banks investigating or implementing retail CBDC consider offline capabilities to be an important feature, including for the European Central Bank's Digital Euro [10, 23, 28].

Today, payments can be made when both parties are offline, for example, with credit cards. Yet, there are two major differences to CBDC:

1. Credit cards face settlement risk because there may be a few days between payment initiation and the actual transfer of funds. CBDC would be settled instantly and irrevocably.
2. Credit cards are prone to double spending, where users spend more funds than they have available. This is by design: the risk is born by the card issuer, who charges interest. CBDC, being more like cash, does not have credit features and must therefore carefully protect against double spending [22].

Applying this to the terminology from above, existing payment schemes only support a weak form of staged offline payments. In contrast, central banks typically aim for at least intermittently offline payment capability. Implementations would reuse existing technology, such as hardware secure elements, to protect against double spending.

This is enabled by designing the CBDC to transfer value directly from one wallet to another.[1] Because CBDC wallets are symmetric, a basic merchant acceptance device could be independent of any acquirer and accept a peer-to-peer payment from a customer, just like cash today [3].

2.3 Coexistence of online and offline wallets

While some CBDC technology platforms cater exclusively to fully offline operation, with no possibility of using custodial and/or online wallets, the consensus among central banks is that both online and offline operations are desirable.

Consequently, a user could hold multiple wallets, some of them purely for online purposes and some others for (optional) offline use. This mirrors the current financial system, where online balances are held as deposit money in commercial banks, and offline "balances" are held as cash. In CBDC, a user could allocate their funds across different wallets. This could be frictionless, since moving money from one digital wallet to another could be facilitated through, for example, a smartphone, and would not require a trip to an ATM.

Applied to the point of sale, the smartphone used by the customer could represent multiple wallets. The Bank for International Settlements points out that it "is important that any online balances and offline balances are segregated, otherwise it may be possible for a user to spend the same value both offline and online and create a double-spend risk" [8]. Therefore, picking the correct wallet that sends the payment matters.

Obviously, this impacts the user experience at points of sale. In Section 4, I describe the necessary setup for such wallet negotiations.

[1] This is different from "payment tokenization" in card schemes, where a "payment token" is moved from one device to another. Those "payment tokens" do not bear monetary value directly.

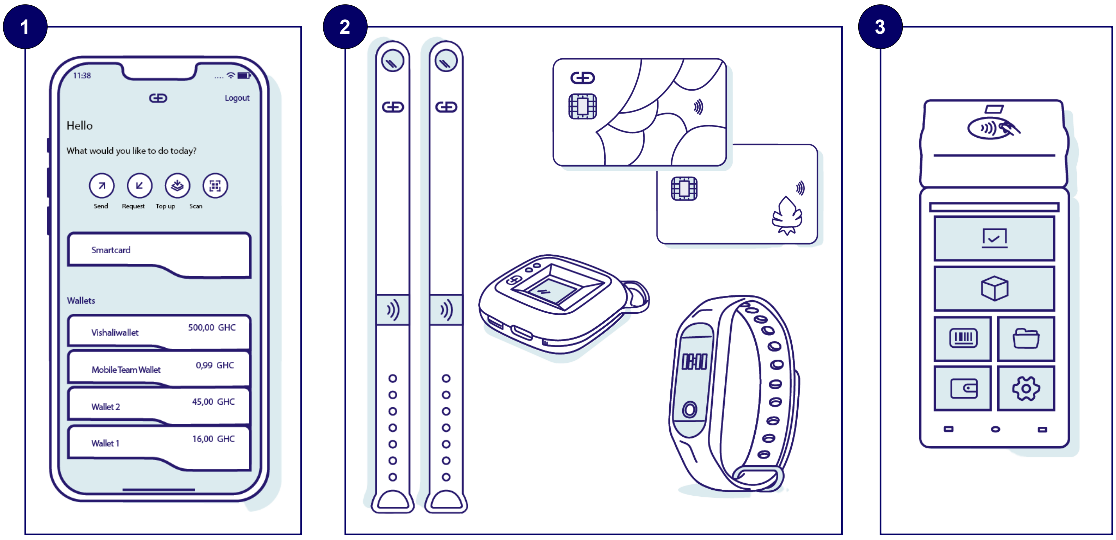


Figure 1: Various CBDC wallet form factors (see Section 2.4 for an explanation)

2.4 Wallet form factors

CBDC wallets can come in many forms, evidenced by the existing CBDC proof of concept and pilot projects. Figure 1 provides some examples:

1. A smartphone, equipped with a wallet app. This app could either access a custodial wallet managed by a user's preferred intermediary, or funds that are stored in secure hardware directly on the device (e.g., an embedded secure element or a SIM card [30]).

2. A dedicated and/or wearable device with a limited user interface, interacting through NFC. Examples include wristbands, smartcards, smartwatches, and key-fobs.

3. A merchant acceptance device. Examples include portable NFC/Bluetooth card readers that connect to a smartphone and dedicated POS terminals that may be based on a standard mobile operating system like Android. Because of CBDC's symmetric nature, the merchant device could itself be (i.e., contain) a wallet.

Importantly, any form factor can work in a dual mode: (1) using funds stored directly on the device—which admits offline payments—or (2) serving as a strong authentication mechanism towards a custodial wallet.

In the first *(peer)* mode, the value transfer is directly executed between two devices. In the second *(authentication)* mode, the value transfer is authorized by the customer's

Table 2: Comparison of existing POS payment schemes with CBDC

Scheme	Money[a]	Offline	Embodiments		Custody		Settlement	Examples
			HW	SW	Cust.	Self		
Credit card	Private	Staged	✓[b]	✓[c]	✓	✗	Delayed	Visa, MasterCard
A2A	Private	None	✗[d]	✓	✓	✗	Instant	Pix, UPI
Cash	Public	Fully	✓	✗	✗	✓	Instant	Euro
CBDC	Public	Intermittent (at least)	✓	✓[e]	✓	✓	Instant	Digital Euro

[a]see Section 1.3
[b]authentication mode only
[c]*Host Card Emulation* [34, 35]
[d]possible, but not used
[e]online-only

device, but executed from the customer's custodial wallet.[2] This means that the card merely serves as a vehicle to authenticate the user to their intermediary.

Offline wallets capable of peer mode are comparable to physical cash wallets. They would also be available for individuals (e.g. children or tourists) without a bank account in the domestic currency.

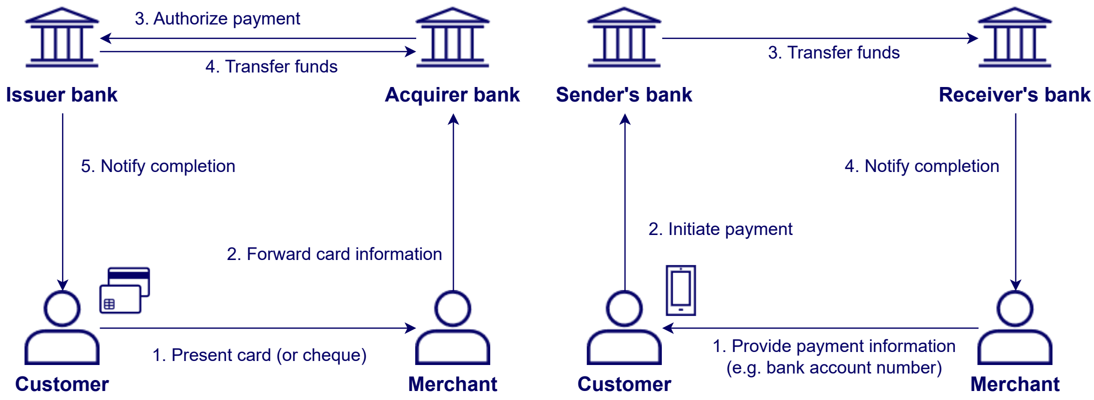
2.5 Comparison to existing POS payment schemes

Current card payment schemes support all of the above form factors, but they can only operate in authentication mode. Traditionally, this was the reason for their delayed settlement since the flow of funds was not triggered immediately after authentication. Modern account-to-account (A2A) payment eliminates this disadvantage by relying on instant payment transfers in the backend.[3] Still, neither allows for (at least) intermittently offline payments that are instantly settled.

Table 2 summarizes the similarities and differences of existing POS payment schemes and CBDC.

[2]This mode illustrates why the term "wallet" is ambiguous. The actual funds reside in a custodial wallet managed by an intermediary on a remote server. But the customer uses a "wallet app" to access those funds.

[3]Although technically, it is possible to do instant payment with card schemes, market adoption has been lackluster.



(a) Pull payment

(b) Push payment

Figure 2: Simplified schematics of payment initiation; in reality, more intermediaries and/or payment networks may be involved (source: author's own elaboration based on GoCardless [18] and World Bank Group [38])

3 Payment initiation

In the traditional world of bank accounts and bank transfers, initiation of the flow of funds can come from two different directions (Figure 2; [18]):

- A standard bank transfer flows from the sender's bank account to the receiver's. This is referred to as a *push payment* because the sender triggers it. Standing orders are also push-based, as are payments in cash.
- The receiver can also initiate the fund transfer: A direct debit (also known as debit order) is an example of a *pull payment*. Checks can also be classified as pull; even though the payer signs checks, the payee triggers the actual transfer.

Both directions have advantages and disadvantages. Yet, there is a trend towards push payments at the point of sale. One factor driving this are mobile payments, which often use merchant QR codes that customers scan with their mobile devices [33].

Many of these schemes operate as A2A and support instant settlement. They experience rapid user adoption, for example Pix in Brazil [31], UPI in India, and Swish in Sweden [19]. Other countries with a higher market share of debit and credit card payments, for example the United States, are slower to catch on [12].

Pull payments are often associated with settlement delay credit. This is why in the context of CBDC, most central banks only consider push.[4] In other words, funds flow from wallet to wallet at the request of the payer.

[4] The notable exception being Bank of Japan, which investigated performance of CBDC pull payments along with batch payments [4].

It stands to reason that push payments in retail CBDC are most relevant at the point of sale. They could be designed in both the peer and authentication modes. Conversely, pull payments would not be able to work in peer mode.

3.1 Communication channels at the point of sale

Zooming in on physical merchant locations, this section describes the technical communication channels that are available at the points of sale, i.e., for proximity payments. For simplicity, I will also assume that the merchant has a "smart" acceptance device, which may come in the form of a standalone POS terminal or a smartphone.

Equipped with such a device, a merchant has the following options to accept a payment:

1. A smart card can be inserted into a card reader, e.g., of a standalone POS terminal or a mobile reader connected to a phone via Bluetooth.
2. A smart card or other mobile and/or wearable device can be touched via NFC.
3. A merchant-presented QR code (either static or dynamic) can be scanned by the customer with their smartphone.
4. A customer-presented QR code (either static or dynamic) can be scanned by the merchant with their POS terminal.

Debit and credit cards mostly focus on the first two (with merchant- and customer-presented QR code payment specified by EMVCo [13]). The actual payment gets transmitted through a card network. Conversely, A2A schemes mostly rely on merchant-presented QR code, which contain the merchant's account or wallet number. The customer's app then initiates a fund transfer to that account.

No existing payment scheme uses any of the communication channels available at the point of sale for actual fund transfer. This is delegated to backend processes at a suitable intermediary, either the customer's own bank (like in A2A schemes), or the merchant's acquirer (like in debit and credit card schemes).

This is where retail CBDC provides a new technological opportunity: NFC and Bluetooth could unify payment initiation and execution.[5] The next section develops a conceptual model how this payment scenario can coexist with other traditional methods, as well as how QR codes could be leveraged for CBDC payments.

[5] The Bank for International Settlements also acknowledges direct value transfers between hardware wallets using QR codes, but implementations are rare [8].

4 Payment model for CBDC

To summarize, the earlier sections of this paper have established

- the fundamental characteristics of a retail CBDC, as an instantly-settled payment instrument that is a direct liability of the central bank, and therefore carries no counterparty risk;
- distinguishing characteristics of retail CBDC vs. other instruments, and its similarity to cash;
- different wallet types and consumer choice, including the option for offline payments with direct value transfer between wallets; and
- the higher relevance of push payments vs. pull payments at the point of sale.

Based on this, the remainder of this paper introduces an existing mechanism to distinguish between different payment options at the point of sale and enhances this concept to enable CBDC payments.

4.1 Consumer choice and complexity

As discussed earlier, users will have ample choices about wallet form factors. For example, they may choose to only use custodial services through an intermediary, only use a smart card, or a combination thereof. In developed economies, it is likely that users may opt for a smartphone to access their various wallets.

This poses a challenge for UI/UX design. Imagine a customer wanting to pay at a store with their smartphone. On the smartphone, they may have a banking app as well as a credit card (e.g., in Apple Pay), a CBDC wallet app, and additionally offline CBDC holdings stored on the smartphone (e.g., in the SIM card). The customer now faces the choice to pick the appropriate payment channel. Both parties may have (diverging) preferences: The customer may prefer to use their credit card due to cashback and the merchant may prefer to accept CBDC due to lower fees. A similar issue arises should the customer present a smart card with multiple co-badged schemes.

This is not a new problem. Domestic and international card schemes co-exist today on shared infrastructure, i.e., customer cards and merchant terminals. In a process known as *Application Selection* [32], mutually supported schemes, then select from that list based on prioritization on the customer's card (see Figure 3).

In the prevailing payment landscape, these complexities are well understood. Current technology provides sufficient flexibility to integrate new payment schemes. CBDC could therefore be seamlessly integrated, although certain specialties must be considered. This mainly concerns offline payment, which is discussed in this section. Note that this

List of AIDs (samples)	
American Express	A00000002501
Discover	A0000001523010
MasterCard	A0000000041010
Maestro	A0000000043060
...	...

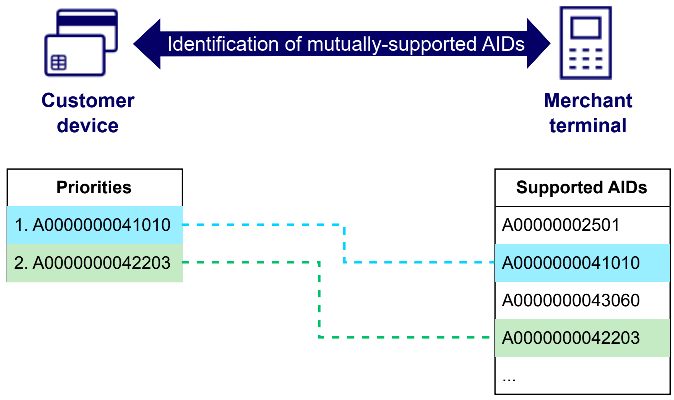


Figure 3: Application selection: negotiating a payment scheme between customer and merchant device based on the *Application Identifier (AID)*, which uniquely identifies the payment scheme

technology can run on cheap commodity smartphones and on existing POS terminals, limiting merchants' need to invest into additional hardware.

4.2 Contact and contactless (NFC) payments

Setting aside QR code payments for now, CBDC would introduce two new applications corresponding to the transfer modes discussed above: direct value transfer between wallets (peer mode) and authentication towards a custodial wallet (authentication mode).

In practice, however, the peer mode is vastly different from existing payment schemes: they were not designed for direct value transfer. Additionally, it would be capable of offline payments.

The Bank of England, in a POS feasibility study, has investigated this flow (among others) [2]. They define the peer mode to be "a payment [...] made between two devices without network connection, supporting offline payments." Note that this leaves open whether the payment recipient is a merchant or any other CBDC wallet holder.

The Bank's study found that the existing EMV applications "were not appropriate for storing offline balances." To transact with those offline balances, the Bank had to implement new software running on the customer device, as well as "a new kernel [on the terminals] that could interact with it" [2].

This result highlights that CBDC presents a new means of payment that enables more use cases, beyond what is available in the market today. Merchants could decide whether to accept payments to a hardware wallet contained in a smartphone or POS terminal or forward them to a custodial wallet. This selection can also happen dynamically depending on the availability of an online connection, but it could also be influenced by regulatory considerations.

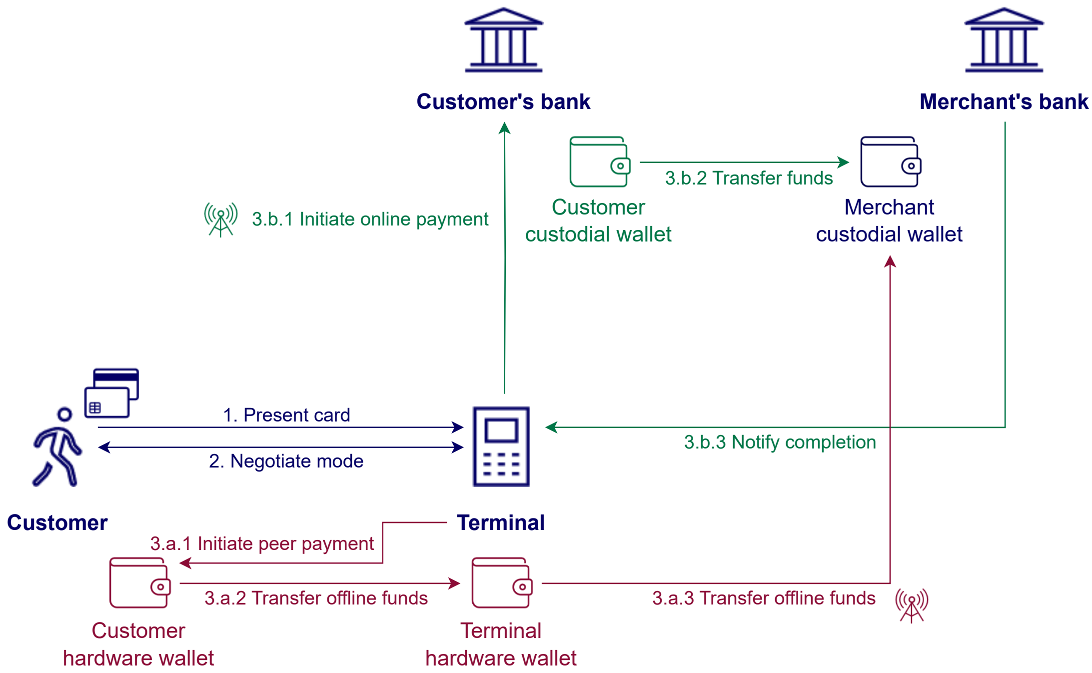


Figure 4: Exemplary payment journey for contact and contactless

Despite the broad agreement that CBDC should enable such offline payments, there is little progress towards standardization. This may be caused by the fact that the implementation of an offline CBDC payment protocol is highly sensitive to the design decisions about the overall CBDC system, which differ widely across countries.

Conversely, the authentication mode can work similarly to existing payment schemes. One of the five lots of the Digital Euro tender, entitled *Secure Exchange of Payment Information* [15, 36], is likely to deal with this.

The European Central Bank has not shared any more details yet. It is plausible though that a card-initiated CBDC payment could mimic an A2A payment, with the customer's card carrying authentication information towards their custodial CBDC wallet. As the study by the Bank of England demonstrated, this could be compatible with existing EMV kernels [2].

Figure 4 shows a possible payment journey. The following steps are executed:

1. Customer presents a payment device, such as a smartcard.
2. Customer device and merchant terminal negotiate mode, resulting in either (a) peer or (b) authentication mode.
3. The flow branches:
    a) In peer mode (illustrated in red) ...

1. The merchant terminal instructs the customer's hardware wallet contained in the smartcard to initiate a peer payment.
2. The customer's wallet transfers funds offline to the merchant's wallet contained in the terminal.
3. Optionally, the terminal can later (or immediately) forward the funds to the merchant's custodial wallet.[6]

b) In authentication mode (illustrated in green) ...

1. The merchant terminal contacts the customer's bank, forwards authentication information, and initiates a payment.[7]
2. The customer's bank transfer funds online from the customer's custodial wallet to the merchant's custodial wallet.
3. The merchant's bank notifies the terminal that the payment is completed.

There is no clear picture yet of how a mode would be selected. In addition to preferences configured by the customer's device, either by the issuer or the user directly, the following considerations might come into play:

- availability of online connection (in case both parties are offline, then payments must be executed directly between hardware wallets);
- local regulation regarding acceptance limits (non-merchants may only be allowed to accept some maximum amount offline to prevent money laundering); and
- presence of secure hardware in the POS terminal (NFC-enabled cheap smartphones may not have the necessary technology to accept offline payments).

However, because online and offline CBDC balances are segregated, it seems clear that offline payments should serve as a fallback option. Otherwise, users may be forced to top up their hardware wallet frequently.

Depending on the form factor, the UI/UX can be designed to require little user intervention at the point of sale. Take Apple Pay: users can set a default card that is used when the side button is pressed. Physical cards do not allow this flexibility.

For merchants, the trade-off is similar. Due to associated high risks, they may not be interested in holding large offline balances in their device. As described above, should

[6] If the merchant terminal does not have hardware capabilities to operate a hardware wallet, the peer payment could also directly flow to the merchant's custodial wallet. The terminal would merely act as a communication proxy. This would be steered through the terminal and would therefore be transparent to the customer's device.

[7] Figure 4 shows a direct communication channel between terminal and the customer's bank. A real implementation may still involve intermediaries and/or an acquirer. For example, the Bank of England study investigated two different communication pathways: one through the central bank and one through the merchant's bank [2].

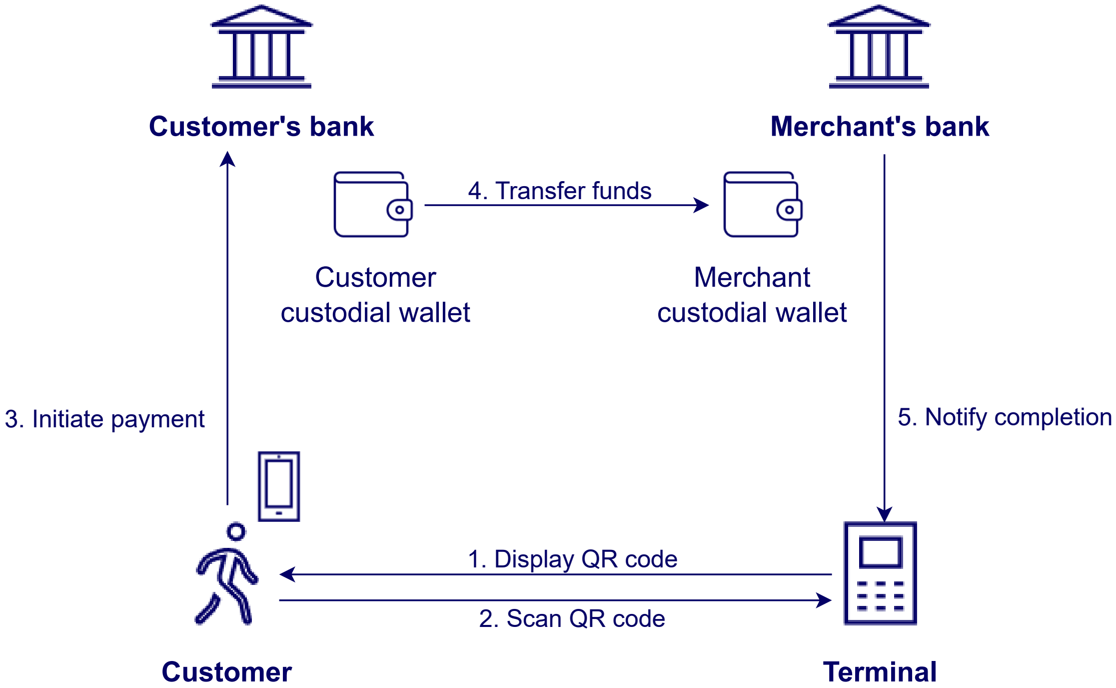


Figure 5: Exemplary payment journey for QR codes

the device break, their income would be lost. The European Central Bank has clarified that businesses have a "zero daily holding limit" of Digital Euro, with only "intraday holdings possible" [16], albeit not for technical, but rather regulatory reasons.

Point-of-sale terminals may need to be upgraded to consider dynamic factors in Application Selection. From the consumer side, the central bank could provide sensible defaults: e.g., on a smartphone, to use online payments whenever possible. This should prevent overburdening users with choice. Combined with an auto-top up feature where a minimum balance on a hardware wallet is maintained, this could enable a frictionless payment experience. Additionally, regulation and lower transaction fees could lead to CBDC being preferred over debit and credit card schemes in the market.

4.3 QR code payments

Payments with merchant-provided QR codes are easy to implement, provided no offline support is required. This approach closely follows A2A payments.

To accept a CBDC payment, the merchant's POS device could generate a dynamic QR code containing the merchant's wallet address, the amount, and a unique transaction ID. The customer scans the code and initiates the transaction through their wallet app (Figure 5).

Fortunately, adding a QR code payment option can be designed unobtrusively. A suitable POS terminal can display a QR code and wait for an NFC connection simultaneously. The customer simply chooses to do one or the other. Should the merchant not have online connectivity—for example, because of an outage—the QR code would not be displayed.

Therefore, the customer's behavior (by scanning a QR code) directly and unambiguously selects the payment flow.

But this assumes that only one QR code standard is in use in a country and that that standard has either been purposely designed or has been made compatible with CBDC. Already in 2021, the World Bank has identified a "proliferation of QR codes in the market, harming compatibility and customer experience" [27, 38]. As a solution, they suggest harmonization, for example, by central banks taking a national approach. This has been conducted successfully in the Bank of Thailand's retail CBDC pilot, which also tested offline payments [5].

4.4 Discussion

David Birch, a financial services advisor, agrees that "CBDCs have to work offline" and asks, "why not make all of the transactions offline so that there are no scaling issues?" Birch argues that this would simplify the "whole design and implementation" [7].

This may be true from a technical perspective. But it is also not a silver bullet: there are additional non-technical arguments why online and offline payments will co-exist well into the future. They represent the fundamental trade-off between accessibility and resilience. An online balance can be easily accessed through multiple devices, and device loss does not imply loss of funds. For offline balances, it is the exact opposite.[8]

Even today, many POS terminals support a dozen different card payment schemes, domestic and international. With no standardized cross-border retail CBDC on the horizon, there is little chance of domestic CBDC crowding out major card networks.

It is, therefore, imperative that a retail CBDC design integrates into the existing payment landscape. A well-designed point-of-sale experience can avoid the impression of fragmentation while still realizing efficiency gains provided by instant settlement and low transaction fees.

An interesting side effect of the CBDC technology is that the peer payment mode could also be provided in non-proximity situations. Direct value transfer not only works via NFC or Bluetooth but could also be conveyed through 4G or Wi-Fi networks. Birch calls this "edge transactions".

[8] As Kahn, Oordt, and Zhu [22] proved, perfect loss recovery is not possible in an offline system that prevents offline spending. Approximate solutions exist, but they are out of scope for this paper.

5 Conclusion

There is no doubt that retail CBDC is moving forward, with the Digital Euro currently being one of the most prominent projects. The European Central Bank clarified that offline capability and merchant payments are within the scope of the Digital Euro. Similarly, the Bank of England has investigated point-of-sale payments through a proof of concept, analyzing the implementation of three different payment modes [2].

Globally, the Bank for International Settlements observes that "throughout 2023, both retail and wholesale CBDC work progressed to more advanced stages" [11].

This has led to user adoption becoming an increased focus of research. Yet, as Lin and Chen point out, "there is a gap in the research on CBDC consumer adoption and its UX" [25]. Within that small body, there is even less treatment of POS payments [1, 24, 25, 26].

This paper sought to contribute a conceptual model for the interaction between customers and merchants through CBDC wallets. Because wallets can work both online and offline, they can contribute to increased resilience and financial inclusion. Instant settlement and CBDC being a central bank liability also reduce risk and enable more flexible payment scenarios. The model can also be applied to other forms of tokenized monies, such as stablecoins or tokenized deposits.

However, this also leads to an increase in complexity. To some extent, this can be alleviated by leveraging existing standards (e.g., EMV for authentication mode), which are suitable for online CBDC payments. QR codes can also be offered unobtrusively by integrating CBDC wallet addresses into domestic or international QR code standards.

The remaining challenge is the user experience for offline payments. I have presented an approach based on the existing Application Selection mechanism of POS terminals to automatically select the source of funds, depending on static and dynamic factors. This does not prevent tech-savvy users from defining their preferences. On the merchant side, smartphones could also serve as acceptance devices, lowering the barrier to conduct business.

The burden is on central banks and technology providers to adequately weigh technological trade-offs and provide reasonable defaults. However, more research is needed to understand user behavior when confronted with new payment methods. This is necessary to foster user adoption and to ensure that retail CBDC becomes successful.

Acknowledgements I thank my colleagues Nicole Saleh, Charalampos Karagiannis, Vratul Kapur, and Raoul-Thomas Herborg for their comments on an early draft of this paper. Special thanks go to John Kiff, who has contributed numerous suggestions for improvement. I appreciate the comments from the anonymous referees at JPSS, which greatly improved the paper. This work has been partially supported by the Federal Ministry of Education and Research (BMBF), Verbundprojekt CONTAIN (13N16582).

References

[1] Svetlana Abramova et al. "What can CBDC designers learn from asking potential users? Results from a survey of Austrian residents." In: *OeNB Working Paper* 241 (2022). ISSN: 2310-5321. URL: https://hdl.handle.net/10419/264833.

[2] Bank of England. *Point-of-sale proof of concept*. May 2024. URL: https://www.bankofengland.co.uk/-/media/boe/files/report/2024/point-of-sale-proof-of-concept-digital-pound-experiment-report.pdf.

[3] Bank of Ghana. *Design paper of the digital Cedi (eCedi)*. Mar. 2022. URL: https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf.

[4] Bank of Japan. *Central Bank Digital Currency Experiments: Results and Findings from "Proof of Concept Phase 2"*. May 2023. URL: https://www.boj.or.jp/en/paym/digital/dig230529a.pdf.

[5] Bank of Thailand. *Retail CBDC Conclusion Report*. Mar. 2024. URL: https://www.bot.or.th/content/dam/bot/documents/en/financial-innovation/cbdc-digital-currency/Update_Release_ENrCBDC%20Conclusion%20Report.pdf.

[6] Ulrich Bindseil. "Tiered CBDC and the financial system." In: *Working Paper Series* (Jan. 2020). DOI: 10.2866/134524. URL: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf.

[7] David Birch. *CBDCs must work offline if they are to be rolled out successfully*. July 2024. URL: https://www.linkedin.com/feed/update/urn:li:activity:7216403081738022913/.

[8] BIS Innovation Hub. *A handbook for offline payments with CBDC*. May 2023. URL: https://www.bis.org/publ/othp64.pdf.

[9] Clifford Chance. *Central Bank Digital Currencies: A new type of intermediary*. Sept. 2023. URL: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/09/cbdcs-a-new-type-of-intermediary.pdf.

[10] Maria Demertzis and Catarina Martins. "Progress with the Digital Euro." In: *Intereconomics* 58.4 (July 2023), pp. 195–200. ISSN: 1613-964X. DOI: 10.2478/ie-2023-0041.

[11] Alberto Di Iorio, Anneke Kosse, and Ilaria Mattei. "Embracing diversity, advancing together – results of the 2023 BIS survey on central bank digital currencies and crypto." In: *BIS Papers* 147 (June 2024). URL: https://www.bis.org/publ/bppdf/bispap147.pdf.

[12] Andy Dresner and Amit Gandhi. *The role of US open banking in catalyzing the adoption of A2A payments*. Jan. 2024. URL: https://www.mckinsey.com/industries/financial-services/our-insights/the-role-of-us-open-banking-in-catalyzing-the-adoption-of-a2a-payments.

[13] EMVCo. *EMV® QR Codes*. URL: https://www.emvco.com/emv-technologies/qr-codes/.

[14] Shayan Eskandari et al. “A First Look at the Usability of Bitcoin Key Management.” In: *Network and Distributed System Security (NDSS) Symposium*. USEC 2015. 2015. DOI: 10.14722/usec.2015.23015.

[15] European Central Bank. *Digital euro - Secure Exchange of Payment Information*. Jan. 2024. URL: https://www.ecb.europa.eu/ecb/jobsproc/proc/pdf/pro-009486_digital_euro__secure_exchange_of_payment_information_-_cn_4400-2024.pdf.

[16] European Central Bank. *End-user on-boarding and digital euro access & holdings*. Dec. 2022. URL: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov221208_item2onboardingaccessmag.en.pdf.

[17] Michael Fröhlich, Felix Gutjahr, and Florian Alt. “Don’t lose your coin! Investigating Security Practices of Cryptocurrency Users.” In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. ACM, July 2020. DOI: 10.1145/3357236.3395535.

[18] GoCardless. *Push vs Pull Payments: What’s the Difference?* Aug. 2023. URL: https://gocardless.com/guides/posts/push-vs-pull-payments-whats-the-difference/.

[19] Monika Hartmann et al. “Are instant payments becoming the new normal? A comparative study.” In: *Occasional Paper Series* 229 (Aug. 2019). DOI: 10.2866/845816.

[20] Lars Hupel. “Interoperability aspects of CBDC across ecosystems and borders.” In: *Journal of Payments Strategy & Systems* 17.4 (2023), pp. 422–432. ISSN: 1750-1814. DOI: 10.69554/MBDJ6710. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4636197.

[21] IMF. “Measuring the Digital Economy.” In: *IMF Policy Papers* (Apr. 2018). URL: https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy.

[22] Charles M. Kahn, Maarten van Oordt, and Yu Zhu. “Best Before? Expiring Central Bank Digital Currency and Loss Recovery.” In: *Bank of Canada Staff Working Paper* (2021). DOI: 10.34989/SWP-2021-67. URL: https://www.bankofcanada.ca/2021/12/staff-working-paper-2021-67/.

[23] John Kiff. “Taking Digital Currencies Offline.” In: *Finance & Development Magazine* (Sept. 2022). URL: https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline.

[24] Zhongzhen Lin and Chien-Hsiung Chen. “Interaction Design and Research for User Interfaces of Central Bank Digital Currency: An Empirical Study.” In: *International Journal of Human–Computer Interaction* (Nov. 2023), pp. 1–17. ISSN: 1532-7590. DOI: 10.1080/10447318.2023.2285651.

[25] Zhongzhen Lin and Chien-Hsiung Chen. "The influence of dynamic page interaction and multimodal operation feedback on the user experience of central bank digital currency." In: *Displays* 80 (2023), p. 102516. ISSN: 0141-9382. DOI: 10.1016/j.displa.2023.102516.

[26] Zhongzhen Lin, Chien-Hsiung Chen, and Shasha Li. "The User Interface Interaction Design of Central Bank Digital Currency: An Empirical Study." In: *Human-Centered Design and User Experience*. AHFE 114 (2023). ISSN: 2771-0718. DOI: 10.54941/ahfe1004223.

[27] Sigurd Næss-Schmidt et al. *Standardising QR Code Payments in Europe*. Jan. 2022. URL: https://copenhageneconomics.com/wp-content/uploads/2022/03/ce-publication-standardising-qr-code-payments-in-europe.pdf.

[28] Fabio Panetta. "A digital euro to meet the expectations of Europeans." In: *SUERF Policy Brief* 95 (May 2021). URL: https://www.suerf.org/publications/suerf-policy-notes-and-briefs/a-digital-euro-to-meet-the-expectations-of-europeans/.

[29] Gerard P. Presto et al. *Retail & Wholesale Central Bank Digital Currencies: Comparison of Select Models, Use Case Analysis & Exploration of Potential Technical Features*. 2023. DOI: 10.2139/ssrn.4448351.

[30] Mark de Reuver and Jan Ondrus. "When technological superiority is not enough: The struggle to impose the SIM card as the NFC Secure Element for mobile payment platforms." In: *Telecommunications Policy* 41.4 (May 2017), pp. 253–262. ISSN: 0308-5961. DOI: 10.1016/j.telpol.2017.01.004.

[31] Mustafa Saiyid. "Pix: Brazil's Successful Instant Payment System." In: *IMF Staff Country Reports* 2023.289 (July 2023), p. 1. ISSN: 1934-7685. DOI: 10.5089/9798400249266.002.

[32] Bruno M. Struif. "Smartcard standardization: Inter-industry commands and application selection." In: *Computer Standards & Interfaces* 17.1 (Jan. 1995), pp. 81–87. ISSN: 0920-5489. DOI: 10.1016/0920-5489(93)e0073-b.

[33] Tao Sun and Ryan Rizaldy. "Some Lessons from Asian E-Money Schemes for the Adoption of Central Bank Digital Currency." In: *IMF Working Papers* 2023/123 (June 2023). ISSN: 1018-5941. URL: https://www.imf.org/en/Publications/WP/Issues/2023/06/09/Some-Lessons-from-Asian-E-Money-Schemes-for-the-Adoption-of-Central-Bank-Digital-Currency-534452.

[34] Thales. *Host Card Emulation (HCE)*. URL: https://cpl.thalesgroup.com/encryption/host-card-emulation.

[35] Assad Umar, Keith Mayes, and Konstantinos Markantonakis. "Performance variation in host-based card emulation compared to a hardware security element." In: *Conference on Mobile and Secure Services (MOBISECSERV)*. IEEE, Feb. 2015. DOI: 10.1109/mobisecserv.2015.7072872.

[36] Mikko Vahter and Sami Nurmi. *Digital Euro: Functionality of the new digital cash will focus on effortless consumer use*. 2024. URL: https://qvik.com/news/digital-euro-functionality-of-the-new-digital-cash-will-focus-on-effortless-consumer-use/.

[37] Xin Wang and Xiaoxiong Hu. *Financial Development, Non-Bank E-Money, and Central Bank Digital Currency*. Mar. 2022. DOI: 10.2139/ssrn.4052603.

[38] World Bank Group. *The use of Quick-Response Codes in payments*. Sept. 2021. URL: https://fastpayments.worldbank.org/sites/default/files/2021-10/QR_Codes_in_Payments_Final.pdf.

[39] Yaman Yu et al. "“Don’t put all your eggs in one basket”: How Cryptocurrency Users Choose and Secure Their Wallets." In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, May 2024. DOI: 10.1145/3613904.3642534.

[40] Yao Zhao. *Balance sheet analysis for two-tier operating central bank digital currency under different settlement framework*. 2023. DOI: 10.2139/ssrn.4647825.