A review of Offline Payment, a key feature & challenge for Central Bank Digital Currencies

EESTEL – European Network of Experts in Digital Transactions (eestel.org)

What's offline payment?

- Offline payment: between 2 devices, both permanently or temporary without internet access
- Instantaneous, final and irrevocable, allowing immediate re-spend
- Subject to compliance requirements but maximizing privacy of holdings and transactions
- Any device: smartphone, feature phone, smartcard, dedicated tag/fob, POS, wearable…
- Any D2D technology: NFC, BLE, QR code, sound modulation...

What's the Demand for it?

- Historically not a priority topic for the payment industry focused on online payment development
- Now globally researched and promoted as part of the development of retail Central Bank Digital Currency (rCBDC)
- Mostly as a way to foster financial inclusion (of undercovered population) and payments resilience (massive network failures)

What's rCBDC?

- A digital version of cash (banknotes and coins), issued by the Central Bank as a means of payment for potentially any use case
- A global concept, but local projects and designs (e.g. digital euro)
- A public initiative involving the banking and payment industry and targeting all consumers and enterprises
- A new type of payment account, a new payment rail and a new payment scheme

Online/offline A dual design

- Separate holdings: online rCBDC accounts vs specific offline wallets locked to devices
- Different systems for online and offline holdings and payments, but closely integrated
- Online procedures: on/offboarding, funding (top-up)/defunding from/to the online rCBDC account
- Offline procedures: discovery, mutual authentication, compliance enforcement & payment

Design challenges

- Device: multiplicity of architectures for secure storage & processing, lifecycle management, cloning
- App & protocol: double spending, replay attack, counterfeiting CBDC units, limited data storage
- Upgradability and crypto-agility for sustainable compliance & security

A nascent market

- Only 14 CBDC pilots/launches and no large-scale return of experience on offline payments
- 2024 ECB issued calls for an offline "component" of the digital euro and associated consulting services
- A few companies have invested in developing solutions and are longing for more rCBDC deployments.
- Large companies from the security and payment industry (Thales, Worldline, Idemia, G+D...), and a few technology SMEs

What is an "offline payment"?

A digital "offline payment" occurs when, at the time of the transaction, neither the payer's device nor the payee's device have any connection to any remote payment system, only they share a peer-to-peer connection. Such a scenario occurs when, locally, network is permanently or temporarily unavailable or when the online payment system has failed.

What is the demand for offline payments?

Until recently, offline payments were mostly off the roadmap of the payment industry, despite the actual needs of a large part of the world population. The payment industry was (is) busy building and expanding online payments and public authorities were not pushing the offline topic. This changed about 5 years ago when offline payments became a key objective of the public effort to deploy **retail Central Bank Digital Currency (rCBDC)**.

History : offline means delayed payment

Historically, offline payment scenarios, e.g. for card payments, have been developed to help merchants securing sales in situations where no communication network is available at the PoS. The solutions (typically EMV one) are based on a store-and-sync-later principle: the transfer of transaction data is simply delayed until connectivity of at least one of the parties (usually the receiver/merchant) with a central payment system is again available. The merchant may accept to deliver the goods even without having confirmation of a fully completed payment, therefore he/she is taking a counterparty risk (possibly covered by insurance). In any cases, until the sync with the central system is complete, the merchant cannot spend the received funds.

Enters retail CBDC

For the last 12 years, CBDC has been an active field of studies and pilots for Central Banks across the world, with the support of international organizations like IMF, World Bank and BIS. Retail CBDC is a digital equivalent of cash, that is banknotes and coins, that every economic agent (consumer, enterprise, association, government…) would be able to use for any payment. There is also a "wholesale CBDC" but it has no link with offline payments, so we won't touch it here: the rest of this document is about retail CBDC or rCBDC.

As cash, rCBDC is issued by the Central Bank, meaning it is "public money": this is, by nature, different from bank accounts which are "private" or "commercial" money issued by financial institutions when we deposit or get a loan from them. Or from e-money accounts that are also "private money". rCBDC is a public service enabling every citizen to pay with a money with the supposedly highest possible level of security (contrary to commercial banks, CB cannot fail… or the whole banking system fails with it).

As cash, rCBDC is supposed to be **available to all citizens and everywhere in the jurisdiction… even when connectivity is not available**: hence the requirements for supporting offline payment.

In addition, Central Banks see in offline payment support a way to achieve some of the other objectives of rCBDC:

- **Resilience**: maintaining payment capabilities in case of disaster and emergency situations
- **Privacy**: meeting people's expectations to keep, with rCBDC, the full privacy of holdings and transactions they enjoy with cash
- **Inclusion**: serving the part of the population that is not served by the private sector because of the lack of business incentives
- **Lower transaction cost**, thanks to less resources engaged by the online system

To support these objectives, the rCBDC version of offline payments has more ambitious requirements than previously known solutions:

- the receiver does not take a counterparty risk
- the receiver can immediately spend the received funds
- sync with an online system (either centralized or decentralized) is not mandatory for completing a transaction (some other procedure, e.g. onboarding the payment system, may require connectivity to a central platform)

rCBDC design

The description hereafter reflects the general model promoted by international organizations like the Bank for International Settlements (BIS), and largely adopted by European Central Bank for digital euro. Other countries, like China, have partly different models, but the separation between bank accounts and rCBDC accounts applies anyway.

Designing rCBDC is about designing:

1. a new payment rail, with the associated scheme ruling the relationships between all participants
2. a new concept and system for holding value in the form of rCBDC, in parallel with the traditional bank and e-money accounts.

rCBDC Accounts & Intermediaries

rCBDC units can only be held, by consumers and enterprises, in a **new type of account** serviced by **authorized/regulated "Intermediaries"**. Such account is **different from a bank account or e-money account**, because the rCBDC holdings are a liability of the Central Bank, unlike your bank (resp. e-money) account's balance is a liability of your bank (resp. e-money Service Provider).

rCBDC accounts are closer to a digital equivalent of a safe deposit box at a bank: the Intermediaries provide security of holdings but, because it is digital, they can also provide convenient digital payment instruments to spend and receive rCBDC from and to the "safe".

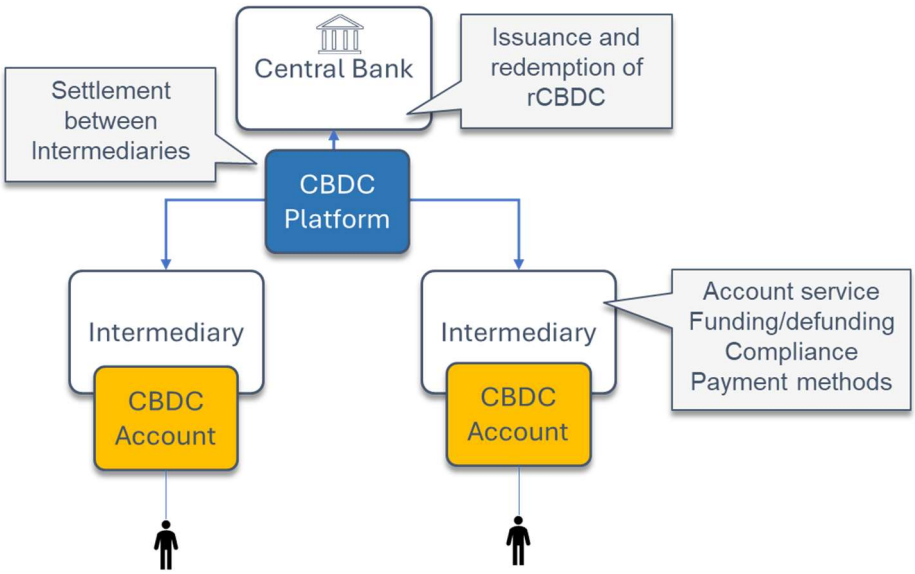
An Intermediary also provides you with means to "**fund/defund**" (ECB's naming) your rCBDC account, i.e. exchange other monies (cash, bank account, e-money…) for rCBDC and vice-versa. Any means is theoretically possible: **ATM, Over-The-Counter cash deposit, card, credit transfer, direct debit, instant payment…**

Privacy & compliance

rCBDC accounts and transactions are subject to compliance checks, information collection, legal measures and reporting, e.g. for KYC and AML/CFT, but **adapted to the feasibility limits in devices**. On the other hand, Central Banks are facing **concerns about the privacy of holdings and payment in rCBDC** : with physical cash the public enjoys full privacy of holdings and transactions and expects that rCBDC will offer the same. Central Banks are trying hard to find the acceptable balance between the 2 objectives, so that privacy is a driver, not a brake, of rCBDC's adoption by the public.

The role of the Central Bank

At the top of the rCBDC payment system, there is obviously the Central Bank which must ensure the right liquidity level by creating (**issuance**) and "burning" (**redemption**) rCBDC units, based on the demand (as they currently do for cash): this implies that CB is controlling (and possibly directly operating) the back-end part of the rCBDC system. Central Bank is also the **anchor of trust** for the whole system and the holders/users of rCBDC: obviously the CB is the only one that can **authenticate its own liabilities** (rCBDC units).



A new payment rail and scheme

The deployment of rCBDC involves multiple parties, public and private, and it requires some form of **technical standards, compensation model and governance**: that is a payment scheme. ECB is in the process of designing such a scheme for digital euro with private stakeholders. At this stage, ECB has proposed a quite simple compensation model:

1. Intermediaries would provide for **free "basic services"** to individuals: rCBDC account with at least one payment instrument
2. **Merchants would be charged** by their serving Intermediary for acquisition (with some « legislative safeguards »)
3. Intermediaries would pay **interchange fees** to each other

Work is ongoing for digital euro, but **the challenge to create a viable business model** is one of the biggest for rCBDC in each and every country, along with **adoption by consumers and businesses**.

rCBDC Offline Payment System

Yet Another Account : offline purse

Offline payment requires that some rCBDC **funds are stored in the parties' devices**: these holdings are identified via an account, sometimes called purse or wallet, **distinct from the online rCBDC account** which links a holder with holdings recorded in a ledger. The offline purse running on a given device is a bearer instrument, meaning that 1 purse = 1 device.

Note : at the current and "early" stage of development of rCBDC, the topic of multi-currency wallets is not yet a subject.

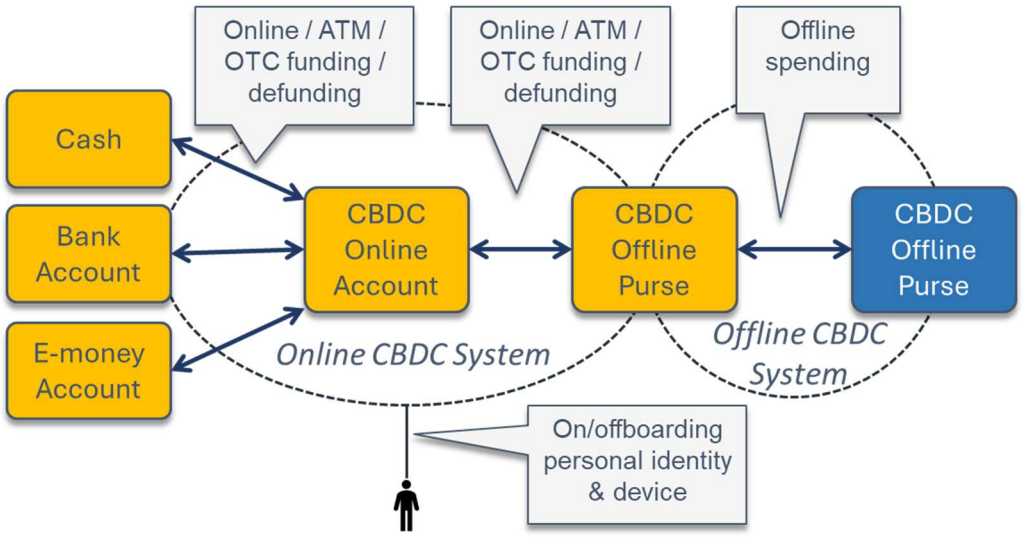
Finality and Sync

Offline payments are considered **final and irrevocable** with no need for a sync with the rCBDC online system. This allows for **immediate re-spend** by the receiver. A sync is an exchange of data between the device/purse the online rCBDC system, obviously requiring some return of the user's device under coverage at some point in time. Sync may be required from time to time to maintain the mid-/long-term offline payment capabilities at the device (security upgrades, offload of reporting data, updates of compliance policies…), but the short-term payment capabilities shall not be dependent on such procedure. Yet sync may be (indirectly) forced by the purse application which suspend the payment capabilities.

Online-Offline: a Dual System

Technically, a rCBDC Offline Payment System is quite different from an online payment system, even if both share functional requirements and some . It could operate completely in parallel to the rCBDC Online system, with its own means and procedures for on/offboarding and funding/defunding. For instance, some rCBDC pilots have considered pre-paid rCBDC cards working 100% offline. Then funding is replaced by the provisioning of the pre-loaded cards, e.g. through an agent network… which would be facing similar security issues as an ATM network.

Other designs (e.g. digital euro) consider that both systems should be functionally integrated, as in the diagram below.



Use cases: proximity payments

The dominant use cases of offline payment are proximity payments of all sorts, person-to-person or person-to-business. This is due to the limited resources and reach of individual devices to communicate with each other (NFC, BLE, QR codes, manual text entry or sound modulation) and support the discovery and payment protocols.

Note that some also consider as “offline” scenarios where:

- Internet is not available (possibly because the user’s equipment is a simple “feature phone”), but other non-data mobile communication services are: then SMS or USSD can be used to support protocols (see UPI in India)
- Internet is available but the payment system is not: email communication can be used between devices

In both cases, “proximity” is no more a limitation to possible use cases. However, the limited data rate and

A variety of supporting devices

Many different types of devices are considered for supporting offline payments: smartphones, feature phones, smartcards (optionally with battery, keyboard and display), dedicated tag/fob, POS and wearables. A new type of device, so-called “Bridge Device”, is considered to enable card-to-card transactions, when the cards have no internal batteries. This wide range of form factors is considered to support a wide range of payment use cases, but also to allow for very cheap equipment of poor population (also public subsidies are considered to foster adoption). The key point is that, whatever the form factor, the device, hardware and software, must provide the foundation for securing the rCBDC holdings and transactions. So, some tamper-resistant HW/SW technologies like Secure Elements, Secure Enclaves or inserted SIMs are required. And, of course, lifecycle and upgrade management is required to maintain the security level during the whole life of the device.

Core Features of a rCBDC Offline Payment System

The core features of an offline payment system are the same as the ones of an online payment system, but with some specificities.

Feature	Offline Payment specifics
On/offboarding	Onboarding for offline payment is likely to happen online, as part of a single rCBDC onboarding procedure. Offline support adds requirements on verification and registration of the account holder's device(s)
Funding/defunding	It shall be possible to move rCBDC from/to the online rCBDC account to/from the rCBDC offline purse of the same person, via the internet, ATM, an agent's counter…
Sending/receiving payment	Any device-to-device technology can be used to support the payment protocol: NFC, BLE, QR code, sound modulation
Compliance (AML/CFT, KYC/KYB)	Can only be enforced locally when offline, based on pre-loaded policies, so highly dependent on secure storage and online upgrade. Given these constraints, Central Banks are considering specific limits and thresholds for offline transactions. Reporting relies on sync.
Technical limits	Limited storage in the device imposes some functional limits, e.g. in terms of number of transactions between 2 syncs with the online system
Interoperability	As for online rCBDC payments, it shall be possible to exchange payment between purses serviced by different rCBDC intermediaries. This implies standards protocol for discovery and payment
Counterfeiting / cloning	The design must ensure it is not possible to create fake rCBDC holdings in the device, by tampering, cloning or double spending/replay.
Double spending/replay attack	The design must ensure it is not possible for a payer to double spend the same funds or a payee to replay the same payment
Upgradability/crypto-agility	Upgrade of the purse application, for security reasons, policy updates…
Loss of value	As value is attached to the device, the loss of the latter is an issue for the funds' holder (like loosing your physical wallet). Implementation of (some) recovery of funds (via the online system) is an open point in many rCBDC projects
Control of monetary mass	rCBDC being a liability of the CB, it is supposed to be under control of the latter. It is not about individual spendings but issuance, loss and redemption
Support of multiple device platforms	Smartphone OS, cardlets, Secure Elements, eSIMs, Secure Enclaves…
Device's lifecycle management	Upgrades, jailbreaks, factory resets, deprecation, theft/loss
Liquidity management (online system)	For the intermediary to support the flow of offline wallets' funding/defunding with no friction but an optimal financial situation

A pre-Market Situation

A global view of retail rCBDC deployment

As of May 2025, 104 Central Banks have launched, piloted, experimented with and/or researched retail rCBDC. Among them, 13 have reached the pilot stage and 2 have launched rCBDC (Nigeria and Bahamas). Note that the scope of "pilot" varies a lot between Central Banks: the e-CNY "pilot" in China is many orders of magnitude greater than any other pilots or even launches.

Offline payment capabilities are always part of the requirements set by a Central Bank for its national or regional rCBDC, but with a different emphasis and priority depending on the country's situation. For instance, Ghana's e-cedi has strong needs for financial inclusion while 47% of their population still have no internet connection. East Caribbean Central Bank is looking at offline capabilities to enable payments when networks are down after hurricanes.

China is, by far, the largest deployment of rCBDC (180M wallets, about 1 trillion $ transactions in 1st half of 2024) although it is still only a "pilot" in the official communication. The digital yuan (or e-CNY) project claims full support of offline payments, based on smartphones with Secure Elements and pre-loaded NFC smartcards, but the extent of use is unclear in the absence of official data.

With regard to Europe, the ECB has included the requirement for offline payment capabilities since the preparation phase of the digital euro. The recent and massive power outages in Spain and Portugal seems to have increase the priority of the topic, offline payments potentially being a key resilience factor.

Available Solutions for rCBDC Offline Payments

The Bank for International Settlements (BIS) and other Central Banks (Bank of England, Riksbank, ECB) have conducted surveys of solutions and vendors. BIS summarizes its findings as:

- There is no one-size-fits-all solution for offline payments
- There is no return of experience from large-scale deployments
- An offline payment solution cannot be designed in isolation from the online system
- Solution vendors are seeking guidance from CBs for further investment

The BIS survey dates from 2023, but we have not seen more large-scale deployment since then. The Bank of England acknowledged technical feasibility but identifies difficult UX trade-offs and a large dependency on policy and legal choices, confirming the no-one-size-fits-all finding of BIS. Solution vendor list includes large companies from the security and payment industry like Thales, Idemia and G+D, and technology SMEs like Crunchfish or Whispercash. Some of them supply both online and offline rCBDC systems, others focus on offline systems to be integrated with online platforms. Some Central Banks (China, ECB) develop their own technology for all or part of the online rCBDC system, but none seems to step in the offline technology.

The business case for Offline Payments

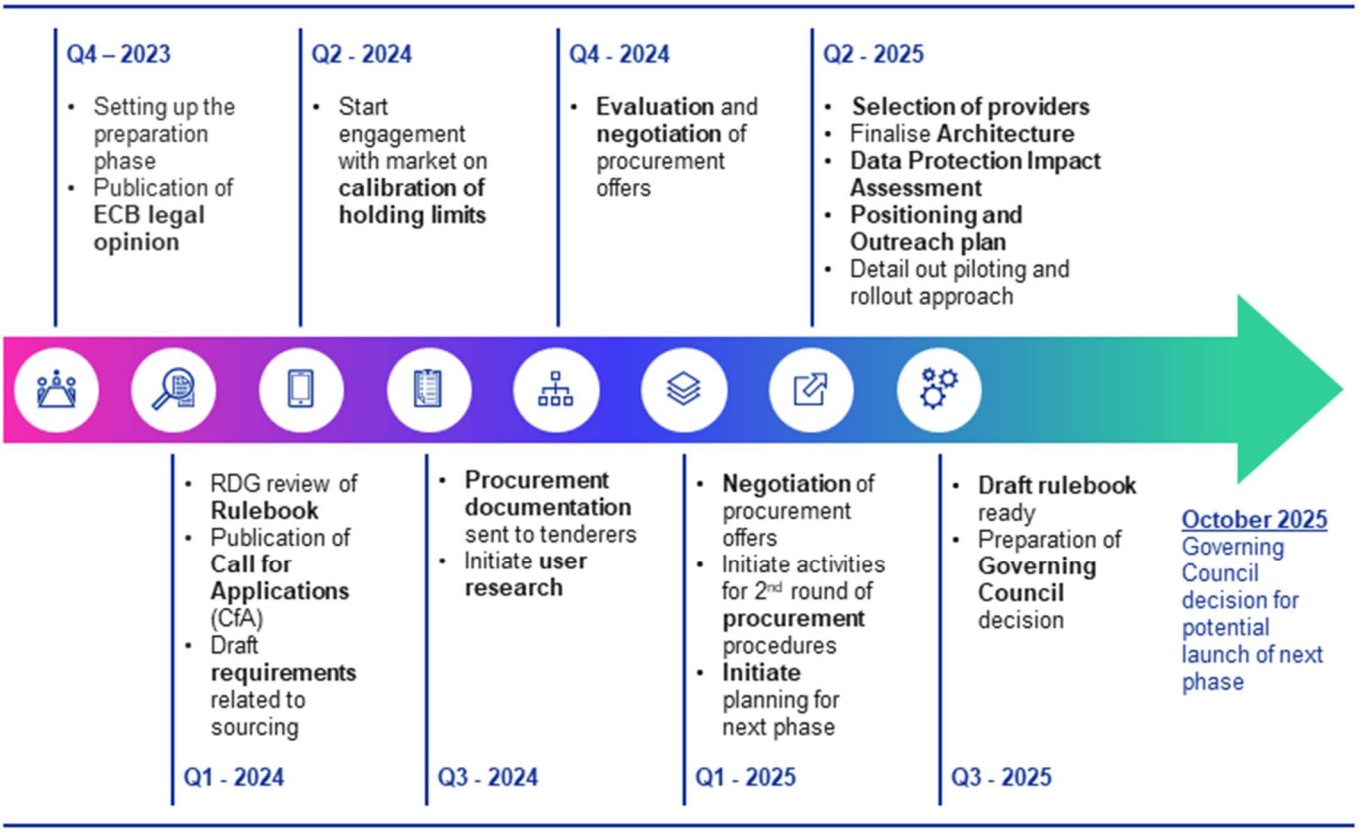
There is a need for rCBDC's business model, where intermediaries have a clear business interest to participate in and help develop the adoption of rCBDC by the general public without competing unfairly with the existing banking and payment business. The equation is not yet solved, and the likes of ECB are still working on an effective scheme with private stakeholders. Offline payments are not helping on the subject as:

1. The collection of fees is technically challenging
2. More importantly, consumers are very unlikely to accept pay fees for what looks like a cash-like transaction, with no 3rd-party's resources involved

The digital euro case

Support of offline payments has progressively become an important requirement for digital euro and ECB has issued over time. From 2022-2023, ECB selected Worldline to work on the prototyping of offline P2P payment use cases, based on smartphones with secure elements or eSIMs (prototypes of this phase of the digital euro project were only designed for research). In January 2024 ECB issued a call for vendors applications for services related to digital euro components, one of the "components" being an offline solution. In October 2024, another call was issued for consulting services on offline solutions. As of today, the results of the 2024 calls have not been made public.

Below the ECB roadmap for digital euro: the current phase, called "Preparation" will be completed by November 2025. The next phase should be about a launch of digital euro, but the legislative phase, with "trilogues" between the Commission, the Council and the Parliament, and then votes, does not have yet a clear date objective.



Contributors

- *Author : Christian Mouton, Founder/Consultant, AEMAA*
- *Reviewer : Robert Fargier, Director, Istium*
- *Reviewer : Eric Nizard, CEO, LIC*
- *Reviewer : Pierre Crégo, Director, Mercury Technologies*
- *Reviewer : Arnaud Crouzet, Vice President - Strategy & Business Consulting, Fime*

Sources & Read List

1. *Banque of Canada - "A central bank digital currency for offline payments"* *https://www.banqueducanada.ca/2023/02/note-analytique-personnel-2023-2/*
2. *BIS – « A high-level design guide for offline payments with CBDC" -* *https://www.bis.org/publ/othp79.pdf*
3. A short document with key concepts about CBDC *https://medium.com/@mouton_christian/central-bank-digital-currencies-and-digital-euro-why-should-i-care-cb66b3cf1f00*
4. A live tracker of the CBDC projects cross the world *https://cbdctracker.org/*
5. *ECB - Progress on the preparation phase of a digital euro (July 2025)* *https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202507.en.html*
6. *Digital euro – Prototype summary and lessons learned* *https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf*
7. *Riksbank (Swedish Central Bank) study of secure offline payments* *https://www.riksbank.se/globalassets/media/rapporter/e-krona/2024/e-krona-pilot-phase-4.pdf*
8. *Bank of England - Digital pound experiment report: Offline payments* *https://www.bankofengland.co.uk/report/2025/digital-pound-experiment-report-offline-payments*