INTERNATIONAL MONETARY FUND

FINTECH

NOTES

Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity

A Review of Existing Approaches

Herve Tourpe, John Kiff, Majid Malaika, and Chris Ostrowski

NOTE/2025/005

FINTECH NOTE

Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity

A Review of Existing Approaches

Prepared by Herve Tourpe, John Kiff, Majid Malaika, and Chris Ostrowski

August 2025

Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity: Review of Existing Approaches

Note 2025/005

Prepared by Herve Tourpe, John Kiff[+], Majid Malaika, Chris Ostrowski[*]

Cataloging-in-Publication Data
IMF Library

Names: Tourpe, Herve, author. | Kiff, John, author. | Malaika, Majid, author. | Ostrowski, Christopher Michael, author. | International Monetary Fund, publisher.
Title: Technology solutions to support central bank digital currency with limited connectivity : review of existing approaches / Herve Tourpe, John Kiff, Majid Malaika, and Chris Ostrowski.
Other titles: Technology solutions to support CBDC with limited connectivity. | Fintech note.
Description: Washington, DC : International Monetary Fund, 2025. | Aug. 2025. | NOTE/2025/005. | Includes bibliographical references.
Identifiers: ISBN:
9798229017435 (paper)
9798229018838 (ePub)
9798229018951 (WebPDF)
Subjects: LCSH: Digital currency—Case studies. | Digital currency—Technological innovations.
Classification: HG1710.T6 2025

DISCLAIMER: Fintech Notes offer practical advice from IMF staff members to policymakers on important issues. The views expressed in Fintech Notes are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

RECOMMENDED CITATION: Tourpe, Herve, John Kiff, Majid Malaika, and Chris Ostrowski. 2025. “Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity: Review of Existing Approaches.” IMF Fintech Note 2025/005, International Monetary Fund, Washington, DC.

Publication orders may be placed online or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430
publications@IMF.org
IMFbookstore.org
elibrary.IMF.org

[+] Both John Kiff and Chris Ostrowski are from SODA Services Ltd, a UK-based consultancy specializing in digital money.

[*] This note benefited from comments and contributions from Jérôme Ajdenbaum, Andrea Alvarez, Elli Androulaki, Shiri Band, David Birch, Asaf David-Margalit, Lauren Del Giudice, Ben Dovey, Jérôme Duperrut, Razvan Dragomirescu, Jerome Duperrut, John Fagan, Bertrand Foing, Judith Garcia, Lars Hupel, Thomas Kudrycki, Hugues Marie, Alain Martin, Cyrus Minwalla, Frederic Rebours, Jeff Rubon, Gabe Ruhan, Danny Russell, Joachim Samuelsson, Leon Schumacher, Beju Shah, Yoav Soffer, Emerson Tan, Cedric Wahl, Nir Yaacobi, and William Zhang.

Contents

BOXES

FIGURES

TABLES

Abbreviations

API	Application Programming Interface
AML/CFT	Anti-money laundering/countering the financing of terrorism
BIS	Bank for International Settlements
BLE	Bluetooth Low Energy
BOG	Bank of Ghana
BOK	Bank of Korea
BOT	Bank of Thailand
CA	Certificate authority
CBDC	Central Bank Digital Currency
CPU	Central processing unit
EAL	Evaluation Assurance Level
ECB	European Central Bank
EMV	Europay, Mastercard, and Visa
G+D	Giesecke+Devrient
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile Communications Association
HSE	Hardware secure elements
NFC	Near Field Communication
P2B	Person to business
P2P	Person to person
PIN	Personal identification number
POS	Point of Sale
PSP	Payment Service Provider
PUF	Physical Unclonable Function
SE	Secure Element
SMS	Short Message Service
STK	SIM Application Toolkit
TEE	Trusted Execution Environment
USSD	Unstructured Supplementary Service Data
VaR	Value-at-risk
VSE	Virtual Secure Element
ZKP	Zero-knowledge proof

Introduction

Central banks worldwide are exploring various approaches to design retail central bank digital currencies (CBDCs) which can provide universal access and operate under all conditions.[1] According to the Bank for International Settlements (BIS), almost all central banks surveyed in 2023 were considering offline payments to be vital or at least advantageous (BIS 2023a). The challenge of ensuring accessibility in environments with limited or no connectivity is particularly evident in emerging market and developing economies, remote regions, and areas prone to natural disasters where internet infrastructure may be unreliable, intermittent, or entirely absent. In advanced economies, such as the euro area, offline functionality is often prioritized to ensure operational resilience, support cash-like usability, and uphold privacy. Therefore, the ability to function in limited connectivity environments is not merely a technical consideration but a key requirement for CBDCs to fulfill their policy objectives.[2]

This note builds on the foundational work conducted by the BIS through Project Polaris (BIS 2023a), which provides comprehensive insights into the technological environment involved in supporting offline CBDC systems, as well as other work such as the Bank of England's recent publication (Bank of England 2025). To further explore this domain, the authors conducted a series of interviews in early 2025 with key stakeholders, including representatives of payment platforms and central banks, and industry experts. Notably, most of the payment platforms with interviewed representatives have participated in CBDC pilot projects that tested offline functionalities.

This note aims to help policymakers understand the practical implications of each technological option, while providing technical teams with insights into each trade-off (Bechara and others, forthcoming).[3] It categorizes connectivity challenges along a spectrum, from no connectivity to cellular-only connectivity where internet is not available or affordable, and which allows for payment solutions based on short message service (SMS) and unstructured supplementary service data (USSD) protocols.[4] The note also considers fallback options for periods of temporary disconnection, for example, during natural disasters.

The note takes a neutral approach to the technology options available, and is structured around the analysis of the usability, accessibility, and functionality considerations of the offline CBDC solutions, followed by an examination of cybersecurity risks and privacy. In all areas, the maturity and track record of the technology is assessed to help inform this research. The note concludes by offering key takeaways for policymakers, drawn from the interviews and the authors' research.

[1] This note does not cover wholesale CBDC (wCBDC). WCBDC is limited to a set of predefined user groups, typically banks and other members of national payment systems, whereas a retail CBDC is widely accessible to the public.

[2] This note focuses on CBDCs, but many observations also apply to other forms of offline payments where central banks play a key role, such as stablecoins. For instance, Sveriges Riksbank is coordinating with banks, nonbank payment service providers, and merchants to enable offline purchases of essential goods during disruptions lasting up to seven days by mid-2026. Similar efforts exist or are underway in Denmark, Estonia, and Norway (Sveriges Riksbank 2025).

[3] This note does not cover legal and regulatory aspects, geopolitical, or trends in technology lifecycles. However, a forthcoming paper from the IMF's Legal Department will cover financial integrity considerations (Schwarz and others 2025). Likewise, macroeconomic considerations and the economic perspective, while critical to inform the solution decision, are out of scope. Finally, while this note can inform a cost analysis of various solutions, it is not meant to cover a fully-fledged cost-benefit analysis.

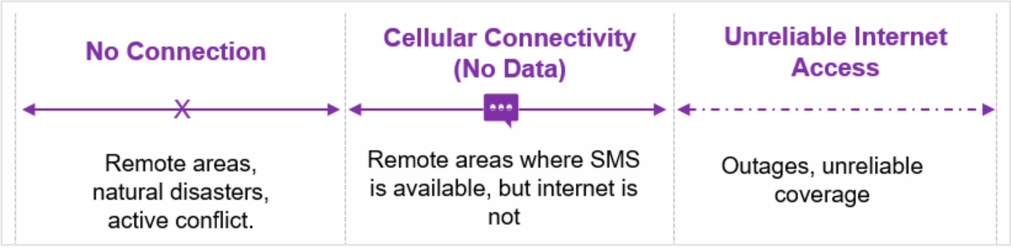
[4] SMS lets basic phones exchange messages with a server without internet access. USSD creates a real-time, session-based connection between a mobile device and the mobile network, enabling two-way data exchange. USSD enables applications like mobile banking and CBDC access menus on feature phones.

I. Connectivity Scenarios and Case Studies

The connectivity scenarios considered in this note range from zero connectivity, often found in rural areas or during extraordinary events, to intermittent or unreliable internet connectivity. In between, some environments may be able to leverage cellular connectivity for text messages via SMS and USSD protocols, which can run on most feature phones, and even on smart phones. One SMS-based payment solution provider noted that "*in rural areas, most users did have smart phones, but as they were old or low-cost models, users are not using apps. They are just using voice and SMS services.*" Also considered are scenarios that are temporary in nature, have patchy connectivity that can vary by location, and are hard to predict, such as natural disasters or outages that disrupt connectivity infrastructure (Figure 1).

Figure 1. Connectivity-Challenged Environments

The scope of this note goes beyond complete offline scenarios, to include low-connectivity and intermittent, unreliable connections.


No Connection
Cellular Connectivity (No Data)
Unreliable Internet Access
Remote areas, natural disasters, active conflict.
Remote areas where SMS is available, but internet is not
Outages, unreliable coverage

Source: Authors.

Additionally, CBDC design and policy decisions must consider whether a payment solution can be kept completely offline for certain scenarios—as long as sufficient funds remain available—or whether a connection is required after either a certain number of payments "hops," a cumulative number of transactions, or a given duration. Offline payment scenarios generally fall into three categories: staged offline, intermittently offline, and fully offline. Each case leads to a different approach to payment transitivity—the ability of a payee to immediately spend the funds without requiring reconciliation with an online ledger (Table 1). For example, staged offline architectures require reconciliation before the payee can onward spend funds received. Several solution providers interviewed for this paper stated that technically speaking, fully offline wallets can safely execute transactions without such reconciliation. However, most recognized that it could be useful for auditability, risk management, or financial integrity purposes.[5]

[5] In the BIS (2023a) description of the reconciliation process on intermittently offline platforms, they describe "settlement" as occurring offline. However, they are careful to point out that they mean "settlement" only from a technical point of view (that is, allowing the transferred value to be onward spent), which may differ from the legal definition (when the transfer is irrevocable and unconditional). Also, see BIS (2023a) and Bank of Israel (2025) for technical discussions of different reconciliation models.

While this note does not examine the reconciliation process in detail, Crunchfish's "reserve, pay, and settle" scheme was mentioned during the interviews (Samuelsson 2025). In this scheme, users' offline wallets are assigned a value that is reserved on the online ledger that limits the amount they can pay offline. To initiate an offline payment, the payer's offline wallet generates and transmits a cryptographically signed digital IOU ("I owe you") to the payee's offline wallet or terminal for an accumulated amount that may not

Table 1. High-Level Offline Architecture Types

Offline payment architecture generally falls into three categories depending on whether reconciliation to a central ledger is required before onward spending.

MODE	ABILITY FOR PAYEE TO SPEND FUNDS RECEIVED
Staged	The payee cannot spend any further until they are connected to the database for reconciliation.
Intermittently	The payee can spend the amount received, although limits set by the issuer and/or payment service providers (PSPs) determine the value and/or volume of transactions that can occur before a connection is required.
Fully offline	No limits to the number or amounts of transactions.

Source: BIS (2023a) and authors.

Experimentation with payment solutions suited to no or low connectivity environments is not new. It dates back decades, beginning with pioneering initiatives such as the Mondex offline payment platform, and early mobile money systems like M-Pesa, which operated effectively in low-connectivity conditions. Modern experiments are exploring a variety of approaches, from custom-built devices and embedded secure elements to sophisticated smartphone applications capable of peer-to-peer transactions without real-time connectivity. Drawing on these cases, the following subsections illustrate the evolution of payment technologies developed to operate across a full range of connectivity-constrained environments. These examples are illustrative rather than exhaustive and provide context for understanding the technical diversity underpinning today's CBDC design strategies.[6]

No Connectivity Environments

Zero connectivity scenarios occur when there is a complete absence or a prolonged breakdown of connectivity infrastructure (for example, during a natural disaster, active conflicts, or in remote areas with no coverage). Several technological approaches have been explored to facilitate digital payments under such conditions, none of which are mutually exclusive:

- One commonly discussed option involves low-cost stored-value card solutions, which can be used to make payments without relying on connectivity. These solutions rely on preloaded balances, secure hardware elements to authenticate transactions locally, and an intermediary device to transfer funds from one card to another.
- Where smartphones are widely available, device-to-device (for example, smartphone-to-smartphone) offline payment solutions have been proposed as viable alternatives. These rely on the short-range transmission of payment instructions using communication technologies such as Bluetooth Low Energy (BLE) near-field communication (NFC), or quick response (QR) codes. For

exceed the reservation online. The digital IOU can be validated by the payee in offline mode, and the digital IOU's credit amount may be used by the payee to make further offline payments, without synchronizing online. The digital IOUs are also validated when either party goes online and reconciles with their offline ledger. This triggers a transfer of value on the online ledger from the payer's reserved amount to the payee's online ledger. The transferred amount would be reserved on the online ledger until the payee synchronizes their online ledger.

[6] The note does not cover closed-system person-to-business (P2B) stored-value card platforms such as the Eagle Cash system that the US Department of the Treasury runs for the US Armed Forces (https://fiscal.treasury.gov/eaglecash).

example, Crunchfish has implemented pilots using these approaches, using NFC technology and QR codes (RBI 2023).

- Unlike in fully connected environments where wallets function primarily as message conduits between users and central databases, offline scenarios require wallets to temporarily act as local ledgers. In such cases, payment execution is based on the exchange of cryptographically signed, time-sequenced payment instructions between devices. For example, Giesecke+Devrient (G+D) has successfully piloted offline CBDC payments in Ghana and Thailand (BOG 2024; BOT 2024).

Stored-Value Card-Based Offline Payments

Stored-value cards can transfer funds via NFC using intermediary devices like point of sale (POS) terminals or smartphones, both of which can operate offline. Card-based payments, introduced in the United States in the 1950s, have become widespread due to standardized features (for example, Europay, Mastercard, and Visa [EMV]), strong merchant acceptance, and innovations like chip-and-personal identification number (PIN) and contactless payments (EMVco 2022).[7]

Two main card types exist: bank-linked debit/credit cards and stored-value cards, which hold funds directly. The latter are common in P2B contexts like transit or prepaid calling, offering ease of use without requiring a bank account.[8]

Historical examples include the Mondex project (UK 1995), which was technically sound but failed due to low merchant adoption and limited person-to-person (P2P) usability, partly due to the need for special devices (Bátiz-Lazo and Moretta 2016). Finland’s Avant card (1993) had offline capabilities but never activated them and was later discontinued (Grym 2020).

More recently, several CBDC pilots have explored card-based offline payment platforms:[9]

- The Reserve Bank of Australia piloted offline P2B CBDC transactions at two universities. Participating students used pre-loaded stored value cards to make purchases at on-campus merchants who accepted the payments via secure apps installed on NFC-enabled smartphones while remaining offline. The technology was provided by Secretarium and Thales (RBA 2023).
- G+D conducted CBDC pilots in Ghana and Thailand. In Ghana, a dedicated POS terminal was used, while in Thailand, smartphones served as SoftPOS devices. Transactions were conducted using NFC and BLE features (BOG 2024 and BOT 2024).
- Not strictly speaking a CBDC project, Payala trialed a digital cash aid distribution system in Timor Leste with World Vision International under the observation of the central bank (Payala 2019).

[7] Chip and PIN is a payment method where a credit or debit card with an embedded microchip is inserted into a terminal, and the cardholder enters a PIN to authorize the transaction. "Tap-to-pay" is a contactless payment method where a card or mobile device is held near a payment terminal to wirelessly transmit payment information.

[8] Examples of stored-value card schemes include Chipknip in the Netherlands, Geldkarte in Germany, Quick in Austria, Moneo in France, Proton in Belgium, Octopus in Hong Kong, and the US Treasury Department's EZpay.

[9] Although this note focuses on payment platform pilots, several central banks have conducted proof-of-concept experiments with offline payment systems (for example, Bank of England 2025). IDEMIAhas demonstrated card-based offline payments for multiple central banks, including the Bank of Israel, using smart cards with fingerprint sensors to enhance security and prevent electronic pickpocketing (Bank of Isreal 2024).

Interviews with Paycode and G+D indicate that stored-value cards are viable in many African markets where they are already in use. In Ghana, G+D highlighted battery-powered POS devices enabling fully offline P2P card payments. However, Thales and the Bank of Canada pointed to limitations, such as the risk of “torn” transactions, where a card is removed mid-transfer, causing imbalances. Mitigations include secure sessions, retransmission, and claim/compensation mechanisms.

Many countries have introduced offline payment cards, often for distributing government benefits. These are usually backed by commercial bank money and may not fully meet CBDC requirements. While technically mature and reliable in controlled settings, stored-value cards are generally better suited for P2B than P2P transactions.

Device-to-Device Offline Payment Solutions

Direct device-to-device offline payment solutions enable the transfer of funds between dedicated devices, typically smartphones, via NFC or BLE connections, QR codes, or by manually typing in the payment instructions.[10] These methods do not require connectivity to a central ledger at the time of transaction execution. Several pilot projects have explored this approach:[11]

- Crunchfish has piloted smartphone NFC-based offline payments in India since 2022 through its “On Tap” solution, initially under the Reserve Bank of India’s regulatory sandbox. Approved for adoption by regulated entities in December 2023 (RBI 2023), Crunchfish began collaborating with Tata Consultancy Services in July 2024 on an offline CBDC solution (Crunchfish 2024).
- Bank of Korea (BOK) experimented with smartphone NFC-based offline CBDC payments in 2022, reportedly in partnership with Samsung Electronics (BOK 2023).
- DigiTally created a Java card applet for feature phones that runs on a mobile operator’s SIM or an overlay SIM, bypassing network restrictions. A pilot at Strathmore University in Kenya enabled users to input wallet IDs and amounts via phone keypads (Baqer and others 2017).[12]

Most smartphones with NFC capability also support BLE and are equipped with cameras for QR code scanning. However, to date, there have been no known CBDC pilots relying solely on BLE or QR codes. Devices used in these pilots have either relied on NFC or custom hardware utilizing manual entry. IDEMIA has experimented with QR codes but found that the limitations outpaced the benefits, therefore confirming the benefit of NFC, the limit in the amount of data stored in a QR code may also hamper their potential to be used with quantum safe algorithms.

[10] QR is a static or dynamic code displayed by the merchant, which payers can scan with their phone. Alternatively, the payer can generate their own QR code for the merchant to scan. This method is widely adopted in mobile payment ecosystems and requires minimal infrastructure, making it highly effective in cashless economies.

[11] IDEMIA has demonstrated offline CBDC exchanges between two smartphones using the NFC channel for the Bank of Israel (Bank of Isreal 2024).

[12] On DigiTally, the payee enters the amount and payer’s wallet ID to generate a transaction code. The payer then inputs this code, the amount, and the payee’s ID. If the details match, the payer’s wallet deducts the funds and generates a second code, which the payee enters to receive the credit (Baqer and others 2017).

Cellular Connectivity Environments (No Data)

In scenarios where some internet connectivity is available, users' holdings are recorded in ledgers, and users' wallets can initiate direct transfers. The payer's wallet sends cryptographically secured payment instructions (such as account identifiers, the amount to be transferred, a verification code, and so on) to the ledger maintenance mechanism instructing the payer's account provider to transfer value from the payer's account to the payee's account.[13]

[13] This is a "push" transaction. In a "pull" transaction, by contrast, the payee's wallet—based on prior payer authorization—initiates the request to debit the payer's account and transfer funds.

Box 1. Insights from Technology Providers and Experts

In early 2025, interviews with representatives of payment platforms and central banks, and industry experts, confirmed a key principle of this note: **no single CBDC solution fits all contexts**. Offline capability requires trade-offs between **form factor availability**, **security architecture**, and **operational feasibility**, all of which are shaped by local infrastructure and user expectations.

On **form factors**, experts emphasized the need for jurisdiction-specific strategies:

- "*There is no one-size-fits-all form factor. In some jurisdictions, feature phones are the baseline. In others, even the most remote users are connected through smartphones and mobile money ecosystems.*"
- "*Cards are more viable in markets where they are already widely used. But in other jurisdictions, people expect CBDC access through smartphones*."

Experience from past deployments underscores that **technical feasibility alone is not enough:**

- "*We've learned from Mondex and Avant. The tech worked. The problem was merchant readiness and user trust. Without a clear rollout strategy and training, even perfect tech fails*."
- "*The problem isn't technology—it's distribution, cost, and user trust. Most of the failures we've seen [of offline payment projects] have been for business reasons*."
- "*We've seen that the most secure architecture might not be adopted if it's clunky or requires unfamiliar hardware. Good user experience is therefore critical.*"

On **security and privacy**, the consensus was pragmatic: while perfect solutions may be out of reach, well-calibrated mitigations exist.

- "*Complete secure systems will probably never exist. But you can make it harder to break, more expensive, less impactful, less scalable, and more visible. In many cases this will be secure enough.*"
- "*Anonymity is possible. Wallet caps and holding limits are enough to manage risks without requiring user IDs in every case*."

Finally, experts reflected on **technology maturity** and the evolving role of cryptography and secure elements:

- "*Secure hardware is expensive and slow to scale. That's why we're investing in virtual secure elements and using trusted execution environments on consumer devices*."
- "*Quantum-safe cryptography exists, but it's slow. You'd need a new chip generation to make it feasible in the field*."

Environments where only basic telecommunications services like SMS and USSD are available can still support some payment scenarios. SMS, which began rolling out in 1993, is a basic text messaging service that enables users to interact with remote services by sending commands via simple numeric codes. USSD, which followed shortly after, is a more advanced protocol that facilitates real-time sessions with mobile network operator (MNO) servers. When supported by the MNO and associated application servers, and if the phone includes a SIM Application Toolkit (STK), USSD can offer interactive menus.[14] These allow users to navigate payment interfaces, input commands via the keypad, and receive feedback in real time. However, because most basic feature phones lack NFC and smartphone capabilities, user input is typically limited to numeric keypad interactions.

While not a CBDC platform, M-Pesa started out as an SMS-based mobile money platform in 2007 in Kenya, and has since expanded to Afghanistan, the Democratic Republic of Congo, Egypt, Ethiopia, Ghana, Lesotho, Mozambique, South Africa, and Tanzania. M-Pesa allows users to deposit, withdraw, and transfer money to other users and pay for goods and services by sending PIN-secured SMS messages. In 2020, it added a USSD interface to improve the user experience (Madegwa 2020).[15]

Several CBDC projects have incorporated or piloted USSD-based mobile access:

- **Ecuador**: In 2014, the Banco Central del Ecuador launched the Dinero Electrónico mobile payment system, enabling USSD-based real-time US dollar transfers via basic phones. Despite functional technology and a wide cash-in/out network, it failed to gain traction and was discontinued in 2018 (Arauz and others 2021).
- **Uruguay**: The Central Bank of Uruguay piloted e-Peso from November 2017 to April 2018 using USSD for mobile Peso transfers. The system—supported by Antel, INSwitch, and RedPagos—ran smoothly and was deemed a technical success (Sarmiento 2022).
- **Nigeria**: The Central Bank of Nigeria launched eNaira in 2021 via a smartphone app. In 2022, USSD access was added for unbanked users. Wallets can be opened with a national ID, and balances loaded through agent networks (Mohammed and Yusuf 2023).
- **Peru**: Since 2024, the Central Bank of Peru has piloted a USSD-based digital Sol limited to BiTel users. It supports P2P, P2B, and utility payments, with cash-out restricted to BiTel stores. Merchants can transfer funds to bank accounts (BCRP 2024).

When considering the lessons learned from all USSD-based and all the secure element-based pilots, it is apparent there is no single solution for any one country, and each country’s distinct digital habitat requires a bespoke response. The USSD-based systems are generally less cash-like and as such some users in USSD-based pilots associated digital money more with the telecommunication companies than the sovereign issuer. Some users that participated in offline secure element-based CBDC pilots reported that the biggest barrier to workability was the need for an intermediary device in those circumstances where such a device was required. All pilots reported positive feedback from users for some elements of the digital money experience.

[14] STK is a standard that enables SIM cards to initiate actions on the mobile device, allowing applications to be run and services to be provided directly from the SIM card.

[15] It is technically possible to link a USSD-based payment platform to other “web 3” forms of digital money. In Kenya, Kotani Pay bridged the gap between blockchain wallets and the M-Pesa mobile money platform (Ishida and Yoshida 2024). This allowed users to access Celo stablecoin loans and other DeFi services using their mobile phones, even those without smartphones (Celo Foundation 2022).

II. Assessment Criteria #1: Form Factor

Building on the understanding gained from the review of existing examples and pilots, this section and the next two describe a structured framework to support central banks' assessment of relevant solutions for their jurisdiction. It aims to bring greater analytical clarity by looking at technological options along three dimensions: i) the payment instrument form factor and user experience, which includes accessibility, and usability; ii) the cyber and operational risks of each approach; and iii) the control of privacy. These three sections examine a dimension, using concrete examples to illustrate key trade-offs and practical considerations.

Understanding the role and importance of each form factor—the device or devices in people's hands—for the targeted use case, can strengthen the deployment strategy. Most stakeholders agree that no single form factor can meet the needs of all users or use cases. An effective offline CBDC strategy must therefore account for multiple form factors, selected based on the specific realities of the jurisdiction, including device penetration, network connectivity, implementation costs, and end-user preferences. This section considers four broad categories of form factors: smartphones, feature phones, custom-made devices, and stored-value cards (Figure 2).[16]

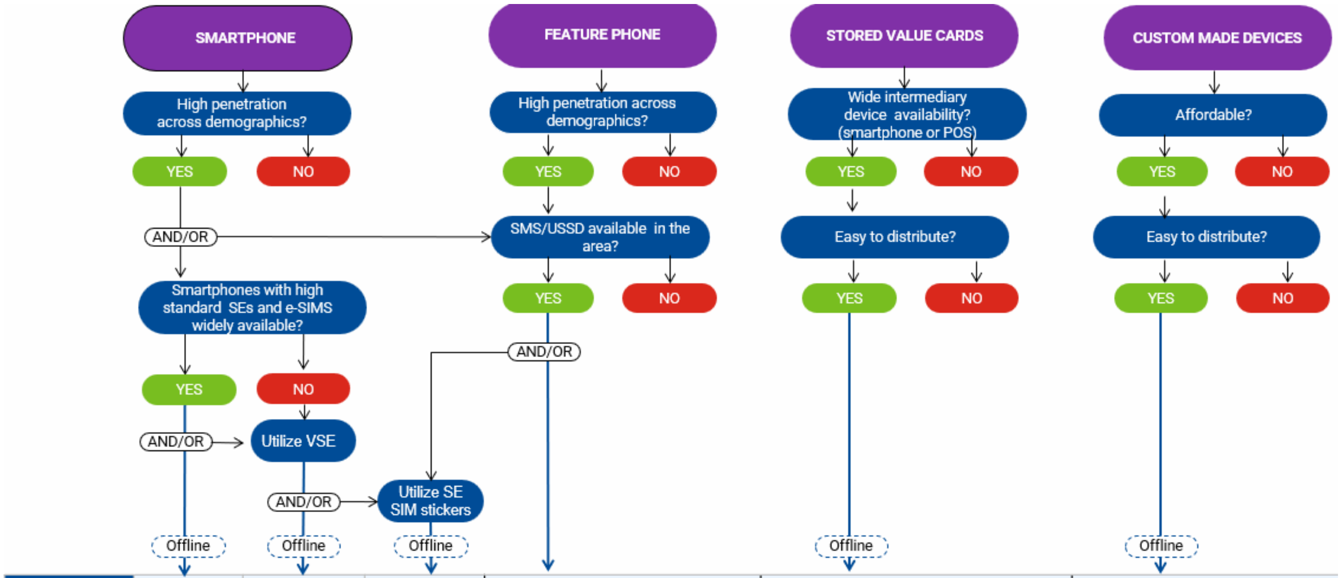
Many payment platforms can support several form factors simultaneously to enhance accessibility and address a broader range of use cases. Nonetheless, some take the view that there should be a single type of device that provides primary functionality, with other form factors reserved for contingencies or specific inclusion use cases.

This section assesses each form factor by considering accessibility and usability. Accessibility refers to how widely adopted a device is or how broadly it can be distributed, ensuring that even the most remote of under-connected areas are served. Availability also relies on the maturity of the technology and resilience of the solution. Usability relates to the ease and convenience of making everyday P2P and P2B payments. Figure 2 offers a structured flow analysis to understand the conditions for different form factors to play a role for a given jurisdiction.

[16] An example of a "custom-made device" would be a credit card-sized device that has an e-ink screen to display menus and data, a keypad for data input, and possibly NFC functionality (see whispercash.com). These devices are used for P2P payments. Some vendors have also designed and built "merchant devices" to be used only by merchants to receive P2B payments from card holder payers.

Figure 2. Understanding Feasibility and Role of Each Form Factor in a Given Jurisdiction

Flow diagram to understand the optimal mix of form factor options



P2P/P2B	✓	✓	✓	✓	With intermediary device (POS or smartphone)	✓
NFC	✓	✓	✗	✗	With intermediary device (POS or smartphone)	✓
BLE	✓	✓	✗	✗	✗	✓
QR Code	✓	✓	✗	✗	✗	With intermediary device (POS/ smartpho
Keypad Input	✓	✓	✓	✓	With intermediary device (POS or smartphone)	✓

Source: Authors.

Accessibility

Device accessibility is closely linked to the type of connectivity available in any given geography, as well as the cost and practicality of manufacturing and distributing devices (custom-made devices or stored-value cards). This is particularly true when such devices are not already in people's hands.

In extreme situations, for example, after natural disasters that disable telecommunications infrastructure, even feature phone-based solutions become unusable. In such cases, SMS networks may still operate when data networks are down, making SMS/USSD-based payment platforms an important backup solution.[17] If power is cut off, all of the payment platforms discussed in this note will eventually fail, leaving physical cash as the ultimate fallback. Some of these risks can be mitigated, or at least delayed, through measures such as stored-value card-based systems and intermediary devices with high-capacity batteries.[18] Such unusual events aside, SMS/USSD technology is a mature and reliable option The 2G/3G networks that support these protocols are still widely operational in many countries, especially

[17] Wireless networks often prioritize voice and text over data during emergencies, as they require less bandwidth and are more resilient under congestion. However, if physical infrastructure like towers are damaged, both services become unavailable.

[18] In extreme circumstances, cash itself has limited effectiveness. Cash already in circulation can be used when there is no electricity at all, but new notes and coins cannot be distributed if ATMs cannot function and other civic organizations, such as post offices, cannot operate.

those with limited broadband or smartphone penetration.[19] However, as 2G/3G networks are being phased out in some countries, strategies relying on SMS/USSD must assess whether these services will continue to be supported over 4G/5G in their jurisdiction. If not, policymakers should anticipate this transition and plan for a timely migration to alternative technologies.

Given these considerations, SMS/USSD-based access continues to offer a practical solution for extending CBDC functionality to remote or low-connectivity areas, especially in areas such as sub-Saharan Africa, where this technology is already widely used. In such contexts, feature phones offer a practical and widely available and cost-effective form factor.

SIM sticker-based wallets can enhance resilience by enabling fully offline payments when all connectivity is down. However, usability challenges, such as navigating an extra menu or maintaining sticker balances, may confuse users. Physical durability is another concern, as stickers may degrade due to heat or wear over time. These factors should be carefully weighed when assessing the role of SIM stickers within an offline solution strategy.

Usability

Usability is primarily determined by the device form factor and how easily it supports both P2P and P2B transactions. The interviewed experts agree that the most seamless user experiences typically rely on technologies like NFC, BLE, or QR codes, which are generally limited to smartphones. In contrast, feature phones and SMS/USSD-based platforms rely on keypad input, which is more error-prone, less intuitive, and considerably less “cash-like” than smartphone-based tap-to-pay functionality.[20] Stored-value card-based solutions also face usability constraints, as they require an intermediary device to complete certain transactions. This device could be an unconnected smartphone equipped with NFC/BLE or a merchant POS terminal. Unlike smartphones, feature phones, or custom offline devices, stored-value cards cannot independently execute direct P2P or P2B payments. Introducing new or custom intermediary devices can increase costs, add deployment complexity, and raise compatibility concerns, especially in under-resourced environments. In contrast, leveraging existing merchant POS infrastructure, as illustrated in Figure 2, can ease integration and lower rollout barriers.[21]

Integrating new or custom intermediary devices into payment systems can pose significant barriers to adoption and rollout, primarily due to increased costs, complexity, and potential compatibility issues. Conversely, utilizing existing POS devices, as depicted in Figure 2, leverages the current infrastructure already employed by merchants, facilitating a smoother and more cost-effective implementation process.

[19] According to the Global System for Mobile Communications Association (GSMA) (2025), in advanced economy countries, 2G/3G networks have been phased out or are being phased out to reallocate spectrum for 4G/5G. However, in Africa, parts of Asia, and Latin America, 2G is still a critical backbone for voice and low-bandwidth services due to its cost-effectiveness and wide coverage.

[20] Though NFC is the most cash-like experience, some vendors made the point that even those phones that are NFC enabled are not necessarily as functional as the most up-to-date smart phones. Finding the NFC antennae or operating BLE can be functionally challenging, which is why a variety of value transmission options is advisable.

[21] Vendors that participated in CBDC pilots where cards were used as the main form factor, report that user feedback included the desire for any card to have a display showing how much money was left on the card at any time.

III. Assessment Criteria #2: Operational and Cybersecurity Risks

CBDC offline capabilities vary significantly based on the system's design, architecture and underlying algorithms, even when the systems conform to common characteristics. Additionally, as exploration of distributed ledger technology, tokenized assets and offline transactions evolve in the CBDC field, the emphasis on security has become more crucial, demanding more involvement and scrutiny from central banks and all service providers and participants within the ecosystem.

While SMS and USSD-based systems are relatively mature and well-understood technologies, they are inherently insecure. These systems primarily rely on Global System for Mobile Communications (GSM) channel cryptography (A5/1 stream cipher)[22] which has been deemed weak in modern cryptanalysis studies (Zhang 2019). Therefore, any payment system relying exclusively on the SMS and USSD-based GSM security for transaction security is insecure for financial transactions. However, to mitigate this weakness, platform providers are offering application-layer encryption on top of the GSM channel encryption. This approach helps compensate for the inherent GSM security weaknesses and repositions SMS and USSD-based systems as a viable option especially for digital inclusion purposes.

Even with modern cryptography and smart phones, offline payment solutions remain vulnerable to a wider range of risks. These include interrupted inter-device connections, device loss or tampering, exposure to rollback risks, double spending, side-channel, fault-injection, and cryptography compromises (BIS 2023a). These vulnerabilities are compounded by traditional threats such as software vulnerabilities, third-party and supply-chain dependencies, and gaps in secure system design.[23]

This section focuses on the most critical cybersecurity and operational risks specific to offline CBDC functionality, informed by expert interviews and field experience. It also highlights emerging mitigation strategies and raises key policy questions that are further elaborated in later chapters.

Risk Exposure

Offline capabilities broaden the attack surface beyond that of conventional digital payment systems amplifying risks such as:

- **Financial risks**, including fraud and theft from unauthorized reuse of value.
- **Security risks**, including cryptographic integrity, data leakage, key management, and device-level vulnerabilities.
- **Operational risks**, involving system failures, recovery limitations, and user-device dependencies.
- **Regulatory risks** (outside this section’s scope), including gaps in anti-money laundering/countering the financing of terrorism (AML/CFT) and know-your-customer compliance.

[22] The GSM encryption algorithm relies on three algorithms: 1) A3 for authentication, 2) A5 (Stream cipher) for data encryption, and 3) A8 for generating cipher keys.

[23] Third-party and supply-chain dependencies can introduce a class of vulnerabilities and threats similar to the CrowdStrike Falcon outage. Although that incident was caused by an unintentional error, it highlights the potential impact of such disruptions on supply chains and the trust placed in platform providers.

The degree of exposure varies with system design, the underlying technologies and cryptographic algorithms, and the architecture of value storage and transfer. While offline capability offers significant promises for enhancing payment system resilience and inclusion, the experts interviewed for this note recognize that these technologies have yet to undergo extensive, scalable, and long-term testing under real-world conditions, the kind of validation that only time can provide.

The risks associated with offline transaction platforms are correlated with the offline duration and/or the number of consecutive offline "hops" (Sveriges Riksbank 2024). Hops are defined as the sequential transfers of digital value from one user to another without re-synchronization with the central ledger. In practice, offline payment platforms mitigate these risks by limiting offline duration and/or number of hops, before reconciliation with a central ledger is required.

Interviews revealed that risk tolerance and thresholds vary across providers. This variability emphasizes the need for the central bank to exercise their role to conduct a thorough scrutiny of the design and underlying algorithms of the CBDC solution. This includes what platform providers refer to as their "secret sauce" schemes and underlying algorithms. Such scrutiny is critical to ensuring alignment with policy objectives while accurately assessing the exposure risk to make informed decisions as described in the best practices section below.

Quantum computing represents an evolving threat to modern cryptography which threatens the entire financial sector (Deodoro and others 2021). All representatives of payment platforms interviewed for this note take quantum computing threats to their offline platforms very seriously. Most saw the quantum horizon as similar to the CBDC horizon (approximately five years) based on the latest work of National Institute of Standards and Technology (NIST) (2022 and 2024). As such, the prevailing sentiment was that watchful preparation is critical. Some thought that current quantum-resistant algorithms are too large and slow for existing hardware-based secure elements and trusted environments that most platforms run on, implying that current technology is not ready to face the threat of quantum computing. However, IDEMIA has announced that it has demonstrated offline payments incorporating enhanced security against quantum threats, using quantum-resistant public key cryptography endorsed by NIST (IDEMIA 2024).

Most of the offline platform providers highlighted the strong requirement for hardware-based secure and trusted environments. Some providers offered a hybrid solution with optional software-based trusted and secure environments for scalability and inclusiveness. Each approach has advantages and disadvantages, but it is important to note that the secure and trusted environment is paramount to the development and security of any offline capabilities. Interviewees from Thales and Bank of Canada emphasized the importance of tamper resistance and the challenges posed by torn transactions or hardware attacks. The Bank of Canada also cited physical unclonable functions (PUFs) as a promising mitigation (Calhoun and others 2019), and G+D emphasized card trust elements such as holograms and biometric consent features.

Box 2. The Right Security Mindset Among Platform Providers

None of the representatives of the offline platforms interviewed for this note claimed that their hardware and software are tamperproof. There is ample evidence of successful secure element hacks in lab environments.[24] Nevertheless, payment platforms continuously work to stay ahead of potential hacks, under the assumption that they are inevitable.

Offline payment platforms work to ensure that their platforms are resistant to tampering at the highest attack potential parameters, for example, by those defined by the Common Criteria standard as an attack by very skilled attackers with almost unlimited funding (Mead 2006). In most cases, security evaluations are performed by independent laboratories to detect potential exploitable vulnerabilities.

Software Security and Software-Based Secure Environment

Software security is foundational to the integrity of any payment platform, especially for supporting offline functionality. This responsibility extends well beyond the core ledger to encompass every layer of the software stack—from central bank servers to end-user devices. Offline capability introduces specific software-related challenges, such as wallet synchronization errors, duplicate transactions, double spending, and reconciliation failures. These risks could arise across various components, including server operating systems, databases, Application Programming Interface (API) integrations, and mobile applications.

The diversity of end-user devices and operating system versions further expands the attack surface. Supporting offline functionality across a fragmented landscape of feature phones, smartphones, and custom hardware introduces additional vulnerabilities and complicates system updates and maintenance.

The management of cryptographic keys is also more complex in offline scenarios, as they must be securely generated, stored, and managed across multiple devices, potentially without real-time access to central validation servers. This introduces new risks of key leakage, loss, or misuse, particularly when wallets are in the user’s custody, implemented as mobile apps or embedded in general-purpose devices.

To address these challenges, several payment platforms offer software-based secure environments such as virtual secure elements (VSEs). Although VSEs are more scalable and cost-effective than hardware-based solutions, they are inherently more exposed to cyber threats. As noted in interviews, the VSEs typically share hardware resources with the main device and are thus considered to offer less resistance to physical attacks. They are also more susceptible to rollback risks, where an attacker could restore a previous wallet state and reuse funds. Crunchfish maintains that VSEs are important for financial inclusion, since they enable secure offline payments on consumer-grade smartphones without needing dedicated hardware. Updates can also be deployed remotely, reducing logistical burdens associated with hardware distribution.

[24] For references to such successful secure element attacks in lab environments, see Grothoff and Dold (2021) and Schumacher (2024).

Table 2. Comparison of Hardware- and Software-Based Secure Elements

HARDWARE SECURE ELEMENT (SE)	TRUSTED EXECUTION ENVIRONMENT (TEE)	VIRTUAL SECURE ELEMENT (VSE)
Dedicated chip designed to securely store sensitive data and execute secure applications	Isolated execution environment that runs alongside the main operating system, providing a secure area to store sensitive data and execute applications.	Software implementation that emulates hardware-based SE functionality.
Used in offline payment solutions like cards, EMV, chips, wearable devices, and so on	Used in offline payment solutions requiring a smartphone	Used in offline payment solutions requiring a smartphone.
Challenging to scale and upgrade across multiple phone models or multiple mobile network operators, although eSIMs on all recent iPhones and most high-end Android phones can support SE-level secure offline payments.[25]	Challenging to scale and upgrade across multiple phone models or multiple mobile network operators, although eSIMs on all recent iPhones and most high-end Android phones can support TEE-level secure offline payments.	Cost and ease of scaling is low because it is app-based and distributed and upgraded using the existing app store ecosystems.
All use JavaCard and the security level is uniform	Security levels may not be uniform or interoperable across phone brands	The security level is homogeneous across phone brands but depends on the level of security of the separating layer (that is, hypervisor) and the hosting software.

Source: Brodsky, Dubey, and Lucas (2023)

Hardware Security and Hardware Secure Environment

Hardware security also plays a vital role in securing the offline capability of any payment platform. While hardware-related risks threaten both online and offline transactions, as noted earlier, the risk increases for offline transactions. Furthermore, almost all of the offline platforms reviewed for this note are based on hardware-based secure and trusted environments, including hardware secure elements (HSEs) and TEEs, but one was based purely on software.

HSEs are standalone hardware components, typically on a separate chip, designed to resist both physical and software attacks (that is, “tamper resistant”). They include a central processing unit (CPU), secure memory, and the ability to perform cryptographic operations, which provides a strong security boundary. TEEs are protected areas within a device’s processor that isolate sensitive code and data from the main operating system. These components isolate cryptographic keys and transaction logic from the main device, making it significantly harder for attackers to extract sensitive data or manipulate the wallet state. Unlike software-based approaches, they do not rely on the device's main processor, reducing the risk of system-wide compromise.

Several payment platforms also emphasized the potential for PUFs to further protect sensitive key material. PUF encryption ties an encryption key to the imperfections of the physical structure of the chip—

[25] Apple stopped selling iPhones in the United States with physical SIM trays in 2022, and most new medium- and high-end Samsung phones ship with eSIMs only (Hupel 2024c).

physically attacking the chip modifies this structure and destroys the ability to decrypt the sensitive data the attacker is after.

When designing offline payments capability, considering compliance frameworks for TEE, SE, and VSE like the Common Criteria,[26] among others, ensures a standardized and robust security evaluation. Table 2 shows a high-level comparison between SE, TEE, and VSE. However, requiring minimum assurance like the Evaluation Assurance Level (EAL) may exclude certain minorities and populations because devices with a higher level of assurance are more expensive. Therefore, central banks will have to evaluate and decide on device security requirements, and acceptable levels of risk, while maintaining a high level of inclusion.

Hardware obsolescence is another risk. If vulnerabilities are discovered after deployment, replacing hardware in the field is costly and slow.[27] This makes forward-compatibility and modularity important considerations when selecting HSE and TEE architectures.

Box 3. Other Types of Attacks Threatening a Secure and Trusted Environment Leveraged for Offline Payment Wallets

Other types of attacks and their mitigation are covered in BIS (2023a), such as counterfeiting via physical breaches, man-in-the-middle, side-channel, fault-inducing attacks, and third-party device compromises. In addition, other attacks target the TEE vulnerabilities and deficiencies. These vulnerabilities stem from missing or erroneous input validation, architecture and design gaps, and the lack of memory protection mechanisms. These targeted exploits are used to escalate privileges for malicious users to compromise the entire device or otherwise force the secure element to leak data and sensitive information like extracting the encryption keys. The root causes for these issues are weak operational hygiene and lack of security best practices during the design and development phases. However, countermeasure design and operational best practices exist, such as layered security architecture and strong and continuous monitoring and fraud detection.

In addition to the security exposures and risks mentioned above, and those highlighted in Box 3, double-spending or “rollback” attacks are considered among the highest security threat for offline transactions. In such attacks, an adversary creates a snapshot of the wallet’s state, executes a transaction, and then restores the original state, enabling the same funds to be spent again. As noted by Schumacher (2024), it is mathematically impossible to eliminate this risk in a fully offline system. Mitigating rollback attacks therefore begins with the deployment of tamper-resistant environments, which can help detect or prevent unauthorized state restoration (Hupel 2024a and 2024b).

[26] The Common Criteria framework defines EALs, ranging from EAL1 to EAL7, to indicate the rigor of a system's security evaluation. Each level builds on the previous one, adding stricter design requirements, testing depth, and vulnerability analysis.

[27] Meltdown and Spectre raised the alarm over vulnerabilities that attackers can exploit in popular hardware. This list, though not comprehensive, presents discovered vulnerabilities in Intel SGX, a TEE built into the CPU (Constantin 2024).

Best Practices for Offline Transactions Capability

Design Considerations

The design and architecture of a payment platform fundamentally shapes the security of its offline transaction capabilities. Sound design must align with a jurisdiction's legal frameworks, risk appetite, and inclusion goals.[28] Early integration of cybersecurity principles, such as secure-by-design, defense-in-depth, and default fail-safe, can significantly reduce exposure throughout the system's lifecycle.

Offline transaction features require additional precautions. Principles like complete mediation and compartmentalization are essential to ensure that access to value is tightly controlled and that compromise in one component does not propagate to others (OWASP 2025). Ensuring transaction integrity and authenticity is also paramount, particularly for detecting replay attacks and tampering attempts.[29]

These high-level principles must be implemented through robust development practices. Adopting a secure software development lifecycle, including threat modeling, secure coding, supply-chain vetting, and secure API integration, is critical.[30] Embedding security early in the development cycle—a so-called "shift-left" approach—helps mitigate risk before it scales.

Offline-specific risks can be addressed through policy-driven countermeasures embedded in hardware and software. For instance, imposing transaction and balance caps can limit financial exposure even if a device is compromised.[31] Platforms like Thales and Paycode view placing checks on the receiving wallet (payee) is just as important as controls on the payer's wallet. This ensures that even if one device is hacked, fraud cannot scale.

The offline payment platform design should incorporate the economics of security aiming to make attacks economically prohibitive, ensuring that the cost of executing an attack far outweighs the gains.[32] For example, the enforcement of limits and the frequent synchronization makes certain types of offline attacks very expensive. However, residual risks will remain, especially for small-value fraud.[33] These include the possibility of automating attacks that replicate small payments to many recipients. Also, attacks may be aimed at undermining the central bank's reputation, even if they are inconsequential from a financial perspective. Design mitigants might include proximity-only communications (for example, NFC)

[28] The implications of "losing" the singleness of money (whereby the CBDC deviates from cash at par) are far reaching and should also be considered as a macroeconomic risk. A large-scale security breach, where a large volume of the CBDC is stolen from end users, may cause the CBDC to lose value if the central bank is unable to guarantee redemption.

[29] Replay attack is a type of network or protocol-level attack where an adversary would intercept and retransmit valid data, in full or partially, to impersonate a legitimate sender to force the receiver to reveal information or executing an unauthorized action.

[30] API security practices include using secure gateways to enforce limits and strong authentication and authorization mechanisms.

[31] Holding and transaction limits would also play a role in offline CBDC compliance legislation and regulations on illicit activities, such as money laundering, terrorist financing, sanctions avoidance, and tax evasion.

[32] Economics of security is a core principle in securing systems by making successful attacks resource-intensive and economically infeasible for attackers. This approach acts as a deterrent to adversaries by increasing the cost and effort required to breach the system.

[33] Some vendors also advocated a "consent to pay" principle for enhanced security. With an offline CBDC, anyone could tap their CBDC device (for example, phone) on another one (for example, card) and steal money immediately offline, if payment is not protected by a user verification method. As is the case with cash today, it would be difficult to prove the absence of consent as there would be no detectable fraud. Some sort of consent mechanism on a card, phone, or other device would enhance consumer protection, but make the experience less cash-like.

to slow such attacks and increase operational burden. For platforms using software-based secure environments, rollback risk can be partially mitigated by anchoring state changes using transaction counters stored in a separate secure area (for example, TEE) or synchronizing them with the backend in staged or intermittent offline models. As recommended in BIS (2023a), limiting or delaying “cash-out” options further reduce exploitability.

In summary, a hardware-based trusted and secure environment remains foundational to ensuring the security and reliability of offline transactions. While software-based secure environments may enhance accessibility and inclusion, they inherently carry higher security risks. Regardless of the approach, offline functionality must be supported by a comprehensive risk mitigation framework. This includes the enforcement of transaction and balance limits, reconciliation frequency requirements, and continuous ecosystem monitoring. Strong detective controls must be embedded across the payment platform lifecycle, along with robust incident response capabilities to swiftly and effectively address any detected breaches.

Mitigating Operational Risks

Operational risks in offline payment systems go beyond cybersecurity, affecting continuity, reliability, and trust in the system. A relevant question is whether policymakers should plan for disruptions such as device loss, transaction interruption, or reconciliation failures. Some payment platforms adopt a strict “cash-like” approach—lost device means lost funds—while others could permit recovery if no outgoing transactions occurred before reconnection. Recoverability depends on architecture choices and policy decisions. Recoverability approaches are still emerging. Kahn and others (2024) suggest expiration mechanisms where offline balances auto-return to the ledger after a time threshold. However, time-based mechanisms are susceptible to internal clock tampering attacks and require leveraging secure elements and certain cryptographic techniques to mitigate clock-tampering attacks.[34] Torn transactions, where payments are interrupted mid-process (for example, NFC disconnection or device power loss), are another real-life risk. These can result in one wallet being debited without the other credited. Most payment platforms mitigate this with secure sessions that complete only after both devices confirm the transaction or by allowing retransmissions. Push-based models often wait for receipt acknowledgements to ensure atomicity: either the transaction fully succeeds or fails. Some platforms recognize that this scenario has to be thoroughly tested to avoid impacting trust and adoption.

Secure-by-design principles can reduce such risks from the outset. Adopting a secure software development lifecycle and the IMF’s “5P framework” (preparation, proof-of-concept, prototype, pilot, production) allows early identification of edge cases and iterative design improvements (Tourpe and others 2023).[35]

Continuous monitoring and responsive incident management are vital. Offline transaction capabilities remain relatively new and untested at scale. This makes it essential to embed fraud detection mechanisms into the synchronization process and empower security operations centers to act on

[34] Malicious users can tamper with the internal clock within mobile phones to manipulate the expiration mechanism. However, smart cards require more sophisticated designs and battery reliance to accurately track time.

[35] The 5P methodology “emphasizes a phased approach to CBDC research and development, with strong focus on research preparation, experimentation and testing, risk management, stakeholder engagement, and cyber resilience.”

anomalies. For instance, IBM proposes a protocol that allows tracing of transaction chains during reconnection to identify and resolve potential double-spends (Androulaki and others 2024). Once anomalies are flagged, additional measures such as wallet freezing and transaction flagging can be employed to prevent misuse or financial loss, as suggested by Bharath and others (2024).

Another key challenge for offline transaction operations is ensuring wallet funding and synchronization during sudden blackouts caused by network or infrastructure failures such as the widespread power outage in Spain in April 2025. These scenarios highlight the need for pre-offline mechanisms that prepare CBDC offline wallets to remain functional even when connectivity is lost. Some central banks are exploring solutions like pre-funding offline wallets via ATMs or implementing automated pre-funding mechanisms that push CBDCs to wallets during online periods. However, many of these approaches assume prior knowledge of the connectivity loss, which may not always be feasible in unexpected emergencies.

Finally, offline payment functionality introduces unique risks that demand ongoing testing and validation. Its complexity, variability across payment platforms, and limited real-world deployment make continuous scrutiny essential. Threat modeling and Architecture Risk Analysis should be applied early, especially as offline designs are often proprietary. Many payment platforms require legal safeguards for independent review of their algorithms and protocols. Testing must reflect the diversity of supported devices and edge cases. Inconsistent behavior across platforms increases the likelihood of undetected vulnerabilities. Throughout the CBDC lifecycle, robust risk management and assessment practices should be consistently applied. Cyber value-at-risk (VaR) modeling should be integrated to enhance quantifying the threats and their impacts (World Economic Forum 2015).[36] This is particularly important for the offline functionality, which is exposed to unique attack vectors that traditional real-time monitoring mechanisms cannot detect.

Just like online payment systems, security audits and penetration tests should be routine for offline payment platforms, especially when extending offline transaction limits or offline durations. Any design change should prompt renewed verification. In addition, continuous assurances for the quantum computing threat must be in place with a post-quantum plan for at-risk algorithms. This also requires early cryptographic agility design techniques to ensure that upgrades can be executed smoothly and safely (Harishankar and others 2024).

Monitoring does not end at deployment. As several interviewees stressed, synchronization events must be used to detect rollback, double-spending, or tampering by tracing transaction chains and checking for anomalies (Androulaki and others 2024).

[36] VaR is a quantitative risk modeling widely used in the financial services industry. Cyber VaR aims to quantify the potential loss and impact of cyber incidents to a specific system or organization.

IV. Assessment Criteria #3: Privacy Considerations

Though privacy requirements vary markedly between jurisdictions, the protection of data privacy is generally a desired feature. Offline platform providers claim to offer “complete privacy” to end users, and to design tailored solutions to suit the privacy requirements of the central bank. However, platform providers admit that regulatory and legal requirements present challenges to privacy. This is particularly true when identifying information must be stored in transaction logs for fraud detection and compliance with AML/CFT requirements.

Platform providers are eager to share how much time and effort they spend to ensure, and even mathematically prove, that end users’ privacy is protected. This is of acute importance as both vendors and central banks need to convince critics who believe that any CBDC transactions will be accessible by the government.

It is important to understand that privacy cannot be designed without robust security measures. This underscores the necessity of strong security protocols to design, develop, and maintain a secure CBDC ecosystem, along with the offline functionality and the necessary verification and scrutiny to ensure privacy and verify the proposed privacy schemes.

Privacy on SMS and USSD

Since SMS- and USSD-based payment platforms are online systems that report transactions back to a ledger, the owner or controller of the ledger will have access to transaction data. In such circumstances, privacy is best protected through legislation, the civic rights of users, and a robust and transparent relationship between the central bank, the government, and the telcos. Other telco-based digital money (such as M-Pesa) can provide instructive information on how privacy is regarded by the users and handled by the government. As a general rule, the SMS and USSD system is no more or less private than any other online system.

Privacy on Offline Platforms

Representatives from offline payment platforms argued that there is no technical need to ever connect to a server to settle offline transactions. However, most central banks have opted for intermittently offline models that batch and upload transaction data after a set number of transactions or when value thresholds are met. This allows for the detection of double spending, irregular patterns, and device tampering, while supporting financial integrity requirements. It is at this upload stage that cash-like privacy may be lost, especially if data can be linked to individuals.

The European Central Bank (ECB), for instance, is adopting such an intermittently offline model for the digital euro. The proposed regulation includes a modified AML/CFT framework to allow greater privacy for offline payments.[37] The central bank is currently assessing how to balance high privacy with robust security and is procuring a technical platform accordingly. In this process, platform providers must demonstrate that the ECB's end-user privacy standards, comparable to cash, are met. Some propose only sharing device-level balances (not transaction histories) to allow reconciliation while protecting privacy.[38]

Another model, used by several central banks, is tiered privacy, where transaction thresholds determine what identifying information is required (ECB 2019; Darbha and Arora 2020). While effective in preserving privacy, this model may pose AML/CFT challenges.

Several platform providers noted that rich transactional data could benefit macroeconomic monitoring (for example, velocity of money, inflation signals). Some even offer services to "color" wallets by merchant category. While such features can aid policymaking, they raise important privacy trade-offs. The perception that privacy is being compromised, even if merchant-level only, may reduce trust and adoption.

Most platforms distinguish between ordinary users and merchants: end-user privacy is prioritized, while merchant/agent data may be accessible to authorities. However, this distinction must be clearly communicated. If users believe others' data is being accessed, they may question the integrity of their own privacy and disengage from the CBDC system.

The technical requirements needed to generate a privacy-enhancing CBDC outline the design of the CBDC with four key components:

1. Leveraging privacy-enhancing technologies: these include specific cryptographic techniques as described in Box 4.
2. Design patterns focused on preserving user privacy: these design patterns are focused on preserving user privacy while still allowing for necessary regulatory oversight.
3. Privacy regulation and tier-models: these regulatory frameworks would establish the legal rules and guidelines for transaction/data privacy. This should include the definition of the level of privacy and the required identifying information based on the transaction amount.
4. Security frameworks: without security there's no privacy. This emphasizes the recommendations in section 2 to design, implement, and deploy a secure CBDC with offline capabilities aimed at preserving the privacy of users.

"Proving" privacy is challenging to payment platform providers, as mathematical and technical proof is harder to follow and more complex than organizational proof. In other words, demonstrating that there is no ledger is not simple, while demonstrating that a particular person does not have access to a ledger is easier. There are innovative mechanisms to prove privacy within the device itself. For example, Apple has

[37] Article 37 of the proposed regulation specifies that transaction data shall not be retained by payment service providers, the ECB, and the national central banks for offline digital euro payment transactions. Payment service providers will only access funding and defunding data related, among other things, to the identity of the user and the amount funded and defunded. See "Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro."

[38] Narula and others (2018) and Stuewe and others (2024) describe such privacy-preserving reconciliation frameworks, albeit not specifically focused on offline payments.

showed how the phone's data load would behave in the cloud if data was being removed in a way which compromised the identity of the user.[39]

Box 4. Privacy-Enhancing Technologies

Privacy-enhancing technologies can be broadly categorized into two types: input-preserving and output-preserving technologies (Bains and Gaidosh 2025). Input-preserving technologies, such as homomorphic encryption, offer a robust mechanism for safeguarding data privacy. However, they are computationally intensive and significantly slower than traditional encryption methods. Similarly, zero-knowledge proofs (ZKPs)—an output-preserving technology—hold substantial promise for privacy protection in financial applications such as CBDCs (Murphy and others 2024). Yet, ZKPs remain complex to implement and resource-intensive. Both homomorphic encryption and ZKPs are considered promising, but their scalability and efficiency limitations suggest that they still require further technological maturation.

In contrast, blind signatures provide a cryptographic method for entities such as central banks to sign messages without accessing the underlying content or revealing user identities. Anonymous credentials similarly support user anonymity by enabling the verification of specific attributes (for example, proof of age or citizenship registration) without disclosing personally identifiable information. Depending on the CBDC system's architecture and design choices, blind signatures and anonymous credentials may offer a practical path toward achieving privacy and anonymity.

Furthermore, for those payment platform providers and central banks that wish to integrate the CBDC into a commercial bank account with accessibility through existing banking apps, the levels of privacy tend to be determined by the privacy requirements set in the banking sector. This usually means that only the payer's bank sees the identity of both parties in the transaction.

Preserving privacy in offline CBDC transactions requires integrating key architectural techniques into the overall CBDC design. This includes the use of privacy-enhancing technologies—such as blind signatures and anonymous credentials—combined with tamper-resistant hardware and TEEs. These safeguards must rest on strong cybersecurity practices and operational resilience across all CBDC participants, including central banks and PSPs. Equally critical is a clear governance and oversight framework to define roles, accountability, and fallback or revocation protocols, particularly for offline scenarios

[39] Apple Security Research (2024) covers how the phone would behave if data was being removed. The data load then proves that it has not behaved that way.

V. How Current Progress Informs Policy Decisions

This section suggests a set of emerging policy takeaways from the current state of experimentation and implementation of offline-capable CBDC solutions. The interviews that anchor this note have surfaced recurring themes and practical insights that can guide decision-making. Therefore, the section does not aim to be exhaustive, nor to replace in-depth technical or legal analysis. Rather, it complements existing work by institutions such as the BIS (2023a), the Bank of England (2025), and others, by providing a snapshot, based on the perspectives gathered through these interviews, of where technology stands today and what questions are coming into sharper focus for policymakers.

Creating a digital currency system that works effectively in a connectivity challenged environment will require policymaking agility and ongoing trade-offs.[40] There is no "off-the-shelf" solution for any environment and the conditions on the ground are different in every country.

Analysis of current progress, by reviewing experimental use case deployments and analyzing the technology solutions, offers key policy takeaways.

Policy Takeaway 1: Diversity of access channels and devices is essential to strengthen CBDC accessibility and usability across different scenarios and demographics. Multiple technology solutions may increase initial complexity and cost but are critical to widespread adoption and resilience.

Any CBDC roll-out that includes multiple technology solutions will inevitably require more investment and be more complex than one that uses a single solution or single channel. As the BiTel experiment in Peru shows, using a preexisting telco infrastructure and a single channel technology solution can work effectively with pre-selected users (telco customers) and in a selected geographic area. However, for a CBDC to be a fully comprehensive, cash-like solution, that can be used organically by self-selecting members of the public, more device options and more technology solutions may be required.

Running technology solutions that can be used on different devices is essential, and "nudging" the CBDC onto devices that are as easy to use for P2P payments as possible is important if the CBDC is to become analogous to cash. Any solution that always requires an intermediary device or that can only work on new devices or custom-made devices will insert barriers into the user experience. However, there are some scenarios and demographics where such solutions will be the only option aside from cash, so deploying these more complex and less cash-like solutions is necessary and indeed fundamental if the CBDC is to be universal and usable in a connectivity challenged environment.

Policy Takeaway 2: Fully secure offline solutions do not exist; therefore, risk mitigation is critical.

Rolling out a CBDC will involve some level of risk. Technology never stands still and each innovation represents a new opportunity for hackers, fraudsters, and bad actors. An online system, such as an

[40] The regulatory agility and automation focus here on the system's ability to enforce regulatory changes rapidly. This has been introduced as a resilience practice in the forthcoming paper titled "Payment Resilience in Fragile and Conflict-Affected States: Lessons for CBDC." (Zhabska and others, forthcoming)

SMS/USSD solution, can be subject to centrally controlled checks and balances, even in a connectivity challenged situation, whereas the secure elements and TEEs on smart phones will remain open to potential exploitation, so setting key parameters and objectives to reflect risk appetite is important.

Establishing a holding limit, and a “hop” limit are not mere details in CBDC design, but essential considerations in any CBDC decision framework. Similarly, there should be clarity upfront whether users should be able to recover funds in the event of a device being lost.

Policy Takeaway 3: With the notion that fully secure offline solutions are evolving and do not yet exist, technological and regulatory agility is needed to enable changes later. This approach ensures that the offline functionalities can be introduced progressively, after meeting certain assurances, and rapidly, so they can be used effectively during outages or catastrophic events.

With such regulatory agility, the CBDC solution can more easily enforce different regulatory updates, such as changing transaction limits and offline hops. Therefore, phasing the introduction of the offline functionalities and increased limits and hops should be based on assurance thresholds. This phased introduction ensures security and privacy while providing a resilience mechanism to rapidly enforce regulatory updates during unforeseen challenges.

Policy Takeaway 4: Regulatory constraints on privacy prevent full cash-likeness, but an analogous experience is feasible in small-value use cases

Though there is no technical need for a central ledger in an offline CBDC, it is expected that all central banks will want the offline solution configured in such a way that allows for intermittent batches of transaction data to be sent to the central bank to test for patterns of double spending, counterfeiting, and fraud. It is important for the central bank to be transparent upfront about what type of data will be included in these intermittent checks, and how the levels of privacy differ for individuals and merchants. In summary, and as noted by Sveriges Riksbank (2024), with the current state of offline technology, it should be possible to develop a secure and usable offline solution.[41]

[41] As noted by the Sveriges Riksbank (2024) Phase 4 report on the e-krona pilot, “with the right boundaries and regulatory framework, it should be possible to develop a secure and usable offline solution.”

VI. Conclusion

This note reviewed a range of technology solutions (SMS/USSD, stored-value cards, custom hardware, and smartphone apps) that support CBDC use in low- or no-connectivity environments. These insights, drawn from interviews with central banks, vendors, and experts suggest that designing policies to support offline capabilities is not only a technical challenge but also a matter of assessing trade-offs among access, usability, security, and privacy.

This analysis revealed that no single architecture or device meets all needs. Instead, effective CBDC or digital money deployment, will require tailored combinations of technologies based on local infrastructure, regulation, and user habits.

Four core takeaways emerged in this study:

- No solution is fully secure, but mitigation strategies (for example, value caps, secure elements, and staged reconciliation) have been successfully tested in pilot environments.
- Technology is still maturing, with ongoing innovation in areas such as secure elements, virtual execution environments, post-quantum cryptography, and privacy-enhancing mechanisms. It is therefore important for stakeholders to adopt a posture of continuous engagement, monitoring, and iterative risk assessment.
- No single solution is capable of meeting all CBDC use cases. Design decisions, such as form factor, security model, and levels of privacy, should be mapped to specific scenarios and user segments.
- Offline user experience will always lag behind online systems, due to limitations in transaction speed, user interfaces, the separation of offline and online wallets, and limited recovery mechanisms.

Offline solutions are maturing, but continued engagement among stakeholders is vital. As future technologies advance and change the connectivity environment (such as low Earth orbit satellites, decentralized architectures, quantum-resistant software, and mesh networks), policymakers can stay ahead of the technology curve by closely monitoring these developments, fostering experimentation, engaging with stakeholders, and considering long-term strategies that can incorporate or adapt to future breakthroughs.

References

Androulaki, E., A. De Caro, K. El Khiyaoui, R. Gay, R. Mercer, and A. Sorniotti. 2024. "Secure and Privacy-preserving CBDC Offline Payments using a secure element." Cryptology ePrint Archive.

Armelius, H., C.-A. Claussen, and I. Hull. 2021. "Can Digital Central Bank Currencies Function as Cash?" Sveriges Riksbank Staff Memo, February.

Arauz, A., R. Garratt, and D.F. Ramos. 2021. "Dinero Electrónico: The Rise and Fall of Ecuador's Central Bank Digital Currency." *Latin American Journal of Central Banking*2 (2), June.

Apple Security Research. 2024. "Private Cloud Compute: A New Frontier for AI Privacy in the Cloud." June 10.

Bains, P. and T. Gaidosh. 2025. "Privacy Technologies & The Digital Economy." IMF Working Paper No. 2025/060, International Monetary Fund, Washington, DC.

Banco Central de Reserva del Peru. 2024. "BCRP Seleccionó a la Empressa Participante en el Primer Piloto de Innovación de Dinero Digital." July 16.

Bank for International Settlements (BIS). 2023a. "A Handbook for Offline Payments with CBDC." BIS Innovation Hub, May.

Bank for International Settlements (BIS). 2023b. "A High-Level Design Guide for Offline Payment," BIS Innovation Hub, October.

Bank of England. 2025. "Digital Pound Experiment Report: Offline Payments." April 10.

Bank of Ghana (BOG). 2024. "The eCedi Report: Bank of Ghana's Central Bank Digital Currency Pilot Project." October 22.

Bank of Israel. 2024. "Demonstration IDEMIA Secure Offline Payments Digital Shekel Challenge," November 27.

Bank of Israel. 2025. "Preliminary Design for the Digital Shekel System." March 3.

Bank of Korea (BOK). 2023. "Current Status of CBDC Technology Research at the BOK." In "Payment and Settlement Systems Report 2022," July 19.

Bank of Thailand (BOT). 2024. "CBDC Offline Testing." In "Pilot Program: Retail CBDC Conclusion Report," March.

Baqer, K., R. Anderson, J.A. Payne, L. Mutegi, and J. Sevilla. 2017. "DigiTally: Piloting Offline Payments for Phones," Paper presented at the Third Symposium on Usable Privacy and Security, 2017.

Bátiz-Lazo, B., and T. Moretta. 2016. "Mondex and VisaCash: A First (Failed) Attempt at an Electronic Purse." In *The Book of Payments: Historical and Contemporary Views on the Cashless Society*. London: Palgrave Macmillan.

Bechara, M., A. Dumitrescu-Pasecinic,, and T. Kubota. Forthcoming. “Selected Legal Considerations for Central Bank Digital Currencies”. International Monetary Fund, Washington, DC.

Bharath, A., A. Paduraru, and T. Gaidosch. 2024. "Cyber Resilience of the Central Bank Digital Currency Ecosystem." IMF Fintech Note 2024/003, International Monetary Fund, Washington, DC.

Bharathan, V. 2020. “Cash Like Features of Central Bank Digital Currencies Can Enhance Financial Inclusion, and Disaster Readiness.” *Forbes*, December 31.

Brodsky, B., A. Dubey, and D.T. Lucas. 2023. “Enabling Offline Payments in an Offline World: A Practical Guide to Offline Payment Security.” Lipis Advisors.

Calhoun, J., C. Minwalla, C. Helmich, F. Saqib, W. Che, and J. Plusquellic. 2019. "Physical Unclonable Function (PUF)-Based e-Cash Transaction Protocol (PUF-Cash) " *Cryptography* 3(18).

Celo Foundation. 2022. "Celo-Mercy Corps Ventures Pilot Highlights How DeFi on Celo Empowers Farmers in Kenya." *The Celo Blog*, June 8.

Cepeda, R. Jr. 2023. "NFC vs BLE Credentials: Determine Which is Right For You." *IDEAS Blog*, May 5.

Christodorescu, M., W.C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu, and M. Zamani. 2020. "Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies." Posted on ArXiv, December 14.

Common Criteria Recognition Arrangement. 2012 *“*Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Components, Version 3.1 Revision 4.*”* CCRA Standard, 2012. Common Criteria Portal, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf.

Constantin, L. 2024. "39 Hardware Vulnerabilities: A Guide to the Threats" *CSO*, July 15.

Crunchfish. 2023. “Crunchfish Receives Clean IPRP for Key Digital Cash Application.”

Chrunchfish. 2024. “Crunchfish and Tata Consultancy Services Enter Alliance Agreement to Offer Offline Payments for CBDCs.” July 1.

Deodoro, J., M. Gorbanyov, M. Malaika, and T. S. Tahsin. 2021. *“Quantum Computing and the Financial System: Spooky Action at a Distance?”* IMF Working Paper 2021/071, International Monetary Fund, Washington, DC.

EMVCo. 2022. "EMV Chip-at-a-Glance: Enabling Seamless and Secure Contact and Contactless Payments Around the World."

Eun-byel, I. 2023. "BOK, Samsung Join Hands for Offline Payment Using CBDC." *The Korea Herald*, May 15.

Groupe Spécial Mobile Association (GSMA). 2025. “The Mobile Economy 2025.”

Grothoff, C., and F. Dold. 2021. “Why a Digital Euro Should be Online-First and Bearer-Based.” Taler.

Grym, Aleksi. 2020. “Lessons Learned from the World’s First CBDC.” *Bank of Finland Review,* August.

Harishankar, R., M. Osborne, J. S. Arun, J. Buselli, and J. Janechek. 2024. "Crypto-Agility and Quantum-Safe Readiness." *IBM Quantum Research Blog*, June 19.

Hupel, L. 2024a. "Secure Wallets for CBDC: How Do They Work?" *The Paypers*, February 6.

Hupel, L. 2024b. "Why Accounts Do Not Solve Double-Spending." *The Paypers*, March 13.

Hupel, L. 2024c. "The eSIM is Becoming the Global Standard: Great News for CBDC." LinkedIn, August 10.

Hupel, L. 2024d. "A Conceptual Model for Point-of-Sale Payment with Retail CBDC" *Journal of Payments Strategy & Systems*18(4).

IDEMIA. 2024. "IDEMIA Secure Transactions Demonstrates the World's First Offline CBDC Payment Transaction Resistant to Quantum Computers." June 20.

International Telecommunications Union (ITU). 2025. "Central Bank Digital Currency Reference Architecture." Digital Currency Global Initiative, January.

Ishida, S., and Y. Yoshida. 2024. "5 Startups Transforming Kenya's Web3 Scene," *Emergo Africa Blog*, November 7.

Kahn, C.M., M.R.C. Van Oordt, and Y. Zhu. Forthcoming. "Best Before? Expiring Central Bank Digital Currency and Loss Recovery" *Journal of Money, Credit and Banking*.

Kieran, M., S. Tao, S. Y. S. Zhou, N. Tsuda, N. Zhang, V. Budau, F. Solomon, K. Kao, M. Vucinic, and K. Miggiani. 2024. "Central Bank Digital Currency Data Use and Privacy Protection." IMF Fintech Note 2024/004, International Monetary Fund, Washington, DC.

Madegwa, C. 2020. "You Can Now Access M-PESA via *334# USSD: Here's What You Need to Know" *Dignited*, October 9.

Mead, N. 2006. "The Common Criteria." Carnegie Mellon University Software Engineering Institute, August.

Minwalla, C. 2020. "Security of a CBDC." Bank of Canada Staff Analytical Note 2020-11, June.

Minwalla, C., J. Miedema, S. Hernandez, and A. Sutton-Lalani. 2023. "A Central Bank Digital Currency for Offline Payments." Bank of Canada Staff Analytical Note 2023-2, February.

Mohammed, R.S., and A.O. Yusuf. 2023. "eNaira—The Journey So Far." In Obiora, K.I.(ed.). 2023. *Economics of Digital Currencies: A Book of Readings*, Central Bank of Nigeria Research Department: 21–41.

Narula, N., W. Vasquez, and M. Virza. 2018. "zkLedger: Privacy-Preserving Auditing for Distributed Ledgers." *Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation.* NSDI, Renton, WA.

Open Worldwide Application Security Project (OWASP). 2025. "Principles of Security." In the OWASP Developers Guide.

Payala. 2019. "Field Trial: World Vision International: East Timor."

Reserve Bank of Australia (RBA). 2023. "Reserve Bank and Digital Finance CRC Complete CBDC Research Project." RBA and Digital Finance Cooperative Research Centre joint press release, August 23.

Reserve Bank of India (RBI). 2023. “Regulatory Sandbox: On Tap application on theme ‘Retail Payments’ – Completion of Test Phase.” December 11.

Samuelsson, J. 2025. "Rethinking Offline Payments: A Groundbreaking Ecosystem Approach," Crunchfish white paper presented at the Digital Currency Conference, Bangkok, May 28-29.

Sarmiento, A. 2022. "Seven Lessons from the e-Peso Pilot Plan: The Possibility of a Central Bank Digital Currency." *Latin American Journal of Central Banking* 3(2), June.

Schumacher, L. 2024. “Decoding Digital Assets.” Palgrave Macmillan Cham.

Schwarz, N., K. Kao, K. Chen, and S. Forte. Forthcoming. "Financial Integrity Implications of CBDCs." IMF Fintech Note, International Monetary Fund, Washington, DC.

Stuewe, S., M. Virza, M. Maurer, J. Lovejoy, R. Böhme, and N. Narula. 2024. "Beware the Weak Sentinel: Making OpenCBDC Auditable Without Compromising Privacy." MIT Media Lab Digital Currency Initiative, November 25.

Sveriges Riksbank. 2024. “E-Krona Pilot Phase 4.”

Sveriges Riksbank. 2025. “The Public’s Ability to Pay in Times of Crisis and States of Heightened Alert Needs to be Strengthened.” In “Payments Report 2025,” March 10.

Tourpe, H., A. Lannquist, and G. Soderberg. 2023. "A Guide to Central Bank Digital Currency Product Development." IMF Fintech Note 2023/007, International Monetary Fund, Washington, DC.

US National Institute of Standards and Technology (NIST). 2022. “NIST Announces First Four Quantum-Resistant Cryptographic Algorithms.” July 5.

US National Institute of Standards and Technology (NIST). 2024. “NIST Releases First 3 Finalized Post-Quantum Encryption Standards.” August 13.

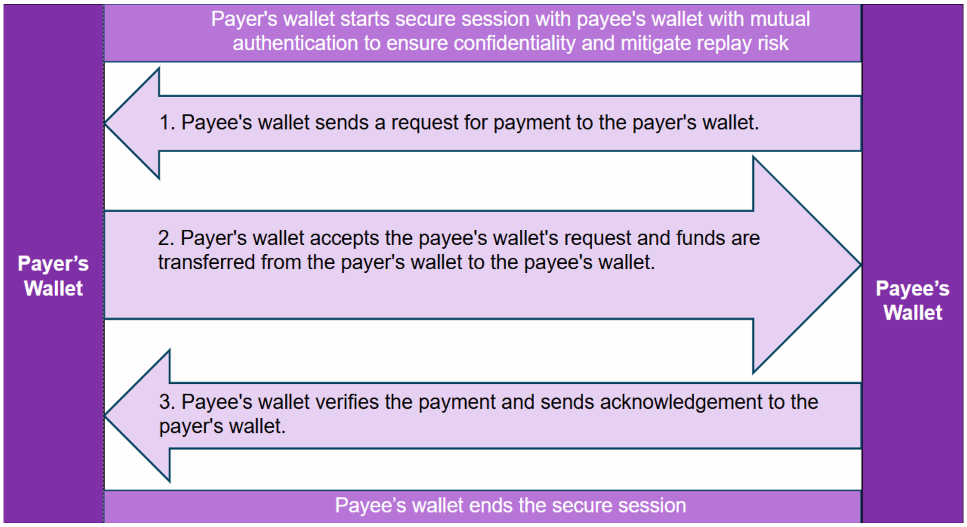
World Economic Forum. 2015. “*Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*.” World Economic Forum, Geneva.

Zhabska, K., G. Soderberg, and M. Malaika. Forthcoming. “Payment Resilience in Fragile and Conflict-Affected States: Lessons for CBDC.” IMF Fintech Note, International Monetary Fund, Washington, DC.

Zhang, B. 2019. "Cryptanalysis of GSM Encryption in 2G/3G Networks without Rainbow Tables." In Galbraith, S.D. and S. Moriai (Eds.). 2019. *Advances in Cryptology ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security: Proceedings, Part III.* Kobe, Japan, December: 428–456.

Annex: Value Transmission in an Offline System

The figure below shows a typical offline payment sequence that starts with the opening of a secure session with mutual authentication to ensure confidentiality and the mitigation of transaction replay risk. The payee's device or app then (1) sends its identity coordinates to the payer's device or app, after which (2) the payer's device/app decrements its balance by the payment amount, generates a multi-digit code based on the amount and the two identification coordinates, which it sends to the payee's device or app. After successful receipt of the multi-digit code (3) the payee's device or app increments its balance by the payment amount and closes the secure session.


Payer's wallet starts secure session with payee's wallet with mutual authentication to ensure confidentiality and mitigate replay risk
1. Payee's wallet sends a request for payment to the payer's wallet.
2. Payer's wallet accepts the payee's wallet's request and funds are transferred from the payer's wallet to the payee's wallet.
3. Payee's wallet verifies the payment and sends acknowledgement to the payer's wallet.
Payee's wallet ends the secure session
Payer's Wallet
Payee's Wallet

SOURCE: Authors and Bank of England (2025)

Bank of England (2025) suggests an alternative flow that does not require the payee's wallet to take part in the transaction in real time, which does away with the secure session and allows the payee's payment verification (step 3 above) on a delayed basis. Such an asynchronous verification could be generated and sent as a QR code, printed, or sent by email, SMS message or even regular mail. However, this increases the risk of torn transactions.

To trust value transfers from sender wallets, the offline payment platform must either be a closed-loop system where values are trusted as they are transferred between payment applications executing in HSEs or TEEs, or alternatively rely on public key infrastructure.[42]

[42] Christodorescu and others (2020) shows how trust can be established offline by issuers acting as certificate authority (CA) by signing certificates with wallets' public keys. Using public key infrastructure and sender signatures, only the sender wallet needs to be secured by a tamper resistant element. By verifying the sender signature using the CA root certificate receivers or any node may trust the sender and accept the value transfer. The Crunchfish offline platform allows for multiple payment schemes to become interoperable when sender wallets are authenticated by the same CA (Crunchfish, 2023). This is beneficial for CBDC rollouts as the service may become interoperable with existing payment services or to support cross-border payments with other CBDCs, even in offline mode.

The functionality and usability of offline payment platforms will vary by configuration. Staged and intermittently offline platforms allow users to continue to transact when/where connectivity is temporarily unavailable, like during natural disasters. Fully offline platforms allow users to transact where connectivity is persistently unavailable, although such usability requires that devices be loaded up with funds (Minwalla and others, 2023).

Token versus Value

A further consideration which applies to an offline system, but not an SMS/USSD system is whether the system itself is underpinned by a token- or value-based platform. Though this distinction may not be obvious to an end user, there are some policy implications in using one system over another.

Token-based offline platforms are based on transferring individual units of digital currency that have specific denominations, and even unique identifiers like physical banknotes with their unique serial numbers. This method makes it hard to transfer values that are not multiples of one of the denominations held by the sender, resulting in “change” needing to be paid back to the payer from the payee. Value-based offline payment platforms represent the balance as a numeric amount, without a unit token, allowing transfers without identifying the individual tokens or their history.

Value-based platforms reduce the need for frequent and large data transfers by relying more on the hardware security of the wallet. Value is created by the central bank and injected into the system, but subsequent transfers between users do not carry a proof of origin or a history, relying on the "transitivity of trust" principle. The "transitivity of trust" simply means that wallets verify the attestation presented by other wallets they interact with to determine that they are genuine and follow the same rules as their own. A payee will accept a transfer from a payer because it trusts the sender wallet and accepts the value transferred as genuine. However, online checks may still be necessary to verify the integrity and trustworthiness of wallets.

PUBLICATIONS

Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity

NOTE/2025/005