



IMMEDIATE VS. DEFERRED OFFLINE MODE

**A COMPARATIVE ANALYSIS FOR CBDC AND
DIGITAL PAYMENT ECOSYSTEMS**

Immediate vs. Deferred Offline Modes

A Comparative Analysis for CBDC and Digital Payment Ecosystems

December 4, 2025

Joachim Samuelsson, Crunchfish CEO

Abstract

Offline payment capability has become a foundational requirement for modern digital money systems. As societies reduce their use of physical cash, payment systems must continue functioning during connectivity disruptions, power outages, rural coverage gaps, and crisis scenarios. This paper compares the two dominant architectural approaches for offline digital payments: **Immediate** Offline Mode, which transfer digital value tokens like “digital banknotes,” vs. **Deferred** Offline Mode, which transfer digitally signed instructions (digital checks/IOUs) for later settlement.

Drawing on perspectives from the Bank for International Settlements (BIS), Bank of England (BoE), BIS Project Polaris, International Monetary Fund (IMF), Bank of Canada (BoC), Bank Negara Malaysia (BMN), and industry experience from Crunchfish, this whitepaper shows that the deferred offline mode provides a more secure, scalable, and interoperable foundation for national and international deployment.

The immediate offline mode remains constrained by hardware requirements, double-spending risks, and operational complexity. Deferred offline mode leverages decades of EMVCo experience and align naturally with existing digital payment paradigms. The paper concludes with policy recommendations for central banks and payments regulators, advocating for a layered, instruction-based deferred offline architecture as the global standard.

Executive Summary

Offline digital payments are necessary for ensuring resilience, inclusion, and continuity in an increasingly cashless world. Two modes dominate global discussions:

Immediate Offline Mode (Digital Value Tokens)

These systems transfer digital monetary value between devices offline, similar to handing over a banknote. While conceptually close to physical cash, immediate offline mode are operationally challenging and security-intensive. They require secure elements, tamper-resistant hardware, and robust protection against double spending. Global authorities, including BIS and leading central banks, BoE, IMF, and BMN identify this approach as high-risk and difficult to scale.

Deferred Offline Mode (Digital Checks / IOUs)

These systems transfer signed payment instructions, not value. The ledger remains authoritative; offline transfers are provisional until settlement. Deferred offline mode avoids the security burden of managing and transferring value tokens and can scale across diverse devices using software-based virtual secure elements (vSE). Consecutive offline payments are supported provided that the payee's wallet credits the balance with received offline payments securely.

Across global research, a clear consensus has emerged:

- **BIS and leading central banks:** Immediate offline mode is high-risk; deferred offline mode is more practical.
- **BOE:** Deferred offline mode will be implemented first; immediate offline mode will be "under review."
- **BIS Project Polaris:** Immediate offline mode requires complex secure hardware ecosystems.
- **BoC:** Deferred offline mode align conceptually with 2PC ledger integrity.
- **BMN:** Deferred offline mode aligns conceptually with modern money, including CBDC as it fundamentally is a credit relation.
- **IMF:** Deferred offline mode is more realistic and safer.
- **Crunchfish:** Layer-2 architecture with deferred offline mode supports domestic and global interoperability.

Deferred offline mode should serve as the baseline for national digital money systems. Immediate offline mode may be explored later as optional enhancements but are not necessary for initial deployment and currently lack scalable, safe implementations.

1. Introduction

As digital payments increasingly replace physical cash, societies require robust mechanisms for conducting transactions when connectivity is unavailable. Network disruptions, whether caused by infrastructure failures, congestion, rural coverage gaps, natural disasters, or cyberattacks, pose a serious risk to payment continuity. Offline payments offer a way to maintain resilience under such conditions.

Leading authorities, including BIS, BoE, BIS Project Polaris, and IMF consistently stress the need for offline payment capability. Yet these institutions also note that not all offline designs are equal: they differ drastically in their security models, risk characteristics, operational requirements, and scalability. Two dominant architectural modes have emerged:

1. **Immediate offline mode**, where value tokens moves between devices offline
2. **Deferred offline mode**, where payment instructions or IOUs move offline but settlement remains online

The purpose of this whitepaper is to provide a comprehensive comparison of these modes, with a particular focus on security, scalability, hardware dependencies, reconciliation, interoperability, merchant readiness, and policy implications. Across global perspectives, a consistent message emerges: Deferred offline mode offer a safer, more scalable, and more interoperable pathway to national deployment, while immediate offline mode are high-risk and operationally immature.

2. Two Conceptual Modes for Offline Payments

Offline digital payments can be built using two fundamentally different architectural approaches. These reflect two different starting assumptions:

- **Start from physical cash and make it digital:** Immediate offline mode (value tokens / digital banknotes)
- **Start from digital payment and make it offline-capable:** Deferred offline mode (payment instructions / IOUs / digital checks)

Understanding the distinction is essential because it shapes the entire security model, risk exposure, hardware requirements, and interoperability potential of a national offline payment system.

2.1. *Immediate Offline Mode: Transfers Digital Value Tokens (Digital Banknotes)*

In the immediate offline mode, the payer's device holds cryptographic value tokens representing real monetary value. When a payment occurs offline:

1. The token is transferred directly to the payee.
2. The payee gains immediate economic finality—as with physical cash.
3. The payee may reuse the token offline.
4. The central ledger updates only after connectivity returns.

This design attempts to preserve the fundamental property of cash: value moves directly between users, offline, without referencing the central ledger during the transaction. However, this design introduces significant operational risks:

- **Hardware dependence:** Devices must store digital value securely using tamper-resistant hardware (secure elements).
- **Double-spending risk:** Preventing duplication without a live ledger is extremely difficult.
- **Device lifecycle management:** Lost or compromised devices can cause systemic risk.
- **Reconciliation complexity:** Offline token chains must be validated retroactively.
- **Scalability limitations:** Ensuring uniform hardware security across millions of devices is impractical.

As a result, global authorities classify immediate offline mode as high risk.

2.2. *Deferred Offline Mode: Transfers Payment Instructions (Digital Checks / IOUs)*

Deferred offline mode uses a different approach: only instructions move offline, not value itself. In this mode:

1. The payer creates a signed payment instruction (digital check / IOU).
2. The instruction is transferred offline to the payee.
3. The payee stores it as a provisional claim.
4. Settlement occurs when either party reconnects to the network.

This design mirrors how digital payments work today—through the exchange of payment instructions—extended into offline contexts.

Consecutive Offline Payments

A major advantage is the ability to support multiple offline hops, provided the payee uses a secure offline wallet capable of:

- Storing incoming offline payments
- Crediting a offline balance
- Spending that balance offline

Integrity is maintained because the ledger remains authoritative, validating every offline payment once online.

Strengths:

- Minimizes offline double-spending risks
- Does not require hardware-based secure elements
- Scales across heterogeneous devices
- Integrates naturally with EMV, ISO 20022, bank systems, and PSP infrastructure
- Aligns with global recommendations from BIS, BoE, BIS Project Polaris, and IMF

This explains why most central banks consider deferred offline mode as the most realistic starting point.

3. Implementation Complexity

The viability of any offline payment system depends on its security, device requirements, operational feasibility, and ability to scale. This chapter provides a detailed evaluation of the two offline modes across seven dimensions: security complexity, device requirements, reconciliation, ecosystem integration, scalability, interoperability, and overall feasibility.

3.1. Security Challenges

Immediate Offline Mode

Immediate offline mode requires that digital value tokens be stored and transferred securely offline. Because offline transfers are considered economically final, the system must enforce:

- Token uniqueness and non-repudiation
- Protection against device cloning
- Offline double-spend controls

- Secure cryptographic value storage
- Sophisticated fraud detection after reconnection

Security must function without a connection to the central ledger, relying solely on the integrity of the device. If a device is compromised, the attacker may extract or clone digital value tokens, creating systemic risk. BIS, BoE, BIS Polaris, and the IMF all highlight this as a major challenge.

Deferred Offline Mode









Deferred offline mode transfers only signed payment instructions, not value. The central ledger remains the source of truth. This reduces risks substantially:

- A compromised device does not generate real value.
- Double-spending attempts are caught during online settlement.
- Instruction collisions or invalid signatures are easily rejected.
- Tamper-resistant isolated runtime and offline caps limit exposure.

Security is significantly strengthened by online validation of the payment instructions. Offline security relies on tamper-resistant runtime isolation of the trusted application.

















Comparison tables: Security Challenges and Overall Risks

Below are two tables that details and compares security challenges and risk categories between immediate and deferred offline modes.

Security Challenges	Immediate Offline Mode (Digital Value Token)	Deferred Offline Mode (Digital Check / IOU)
Monetary creation / counterfeit risk	 Very High: compromised SE or wallet can duplicate CBDC tokens; catastrophic system-wide risk	 None: offline wallets cannot mint or create money; only IOUs, settlement controlled by bank
Value duplication (double-spend)	 Very High: tokens can be spent many times before reconnection, settlement is final	 Low: only IOUs; double spends collapse at settlement; risk bounded by offline limit
Multi-hop P2P propagation of fraud	 Very High: fake tokens propagate exponentially offline	 Medium: operational risk only, fake IOU propagation possible, but risk is bounded by offline limit
Secure Element compromise	 Very High: entire currency supply threatened; tokens cloneable	 Minimal: only IOU issuance compromised; risk bounded by offline limit

Security Challenges	Immediate Offline Mode (Digital Value Token)	Deferred Offline Mode (Digital Check / IOU)
Settlement irreversibility	■ High: immediate finality; cannot reverse fraudulent offline transfers	■ Low: settlement happens online; fraudulent IOUs are rejected
Replay attacks	■ High: same token reused offline until detected	■ Medium: replaying IOUs can possibly happen offline, but always rejected at settlement
Device cloning attack	■ Very High: cloned device means duplicated funds	■ Low: cloned device means duplicated IOUs, but risk bounded by offline limit
Merchant exposure	■ High: merchants accept fake tokens that cannot be reversed	■ Medium: merchants may accept bad IOUs, but loss bounded by offline limit
Systemic liquidity impact	■ High: offline loading drains bank deposits immediately	■ None: reserved funds stay in bank until settlement
Impact of device loss / damage	■ Medium: value permanently lost	■ None: only IOUs stored; value retained in bank
Fraud during long network outages	■ Very High: large-scale counterfeit values circulate	■ Medium: operational trust issues possible; financial loss capped
Supply chain compromise risk	■ High: compromised SE manufacturer undermines entire ecosystem	■ Low: no SE-based trust root needed; CA compromise manageable
Officer/agent cash-out fraud	■ High: offline bearer value can be cashed out	■ Low: settlement with bank always required
Backend reconciliation failures	■ Medium: reconciling multiple offline tokens is fragile	■ Low: IOUs have simple deterministic settlement

Risk / Challenge: ■ High / Significant ■ Medium / Manageable ■ Low / Bounded

Risk categories	Immediate Offline Mode (Digital Value Token)	Deferred Offline Mode (Digital Check / IOU)
Financial risk	 Systemic, unlimited	 Low (bounded)
Operational risk	 High	 Medium
Monetary integrity risk	 High	 None
User/merchant trust risk	 Medium (financial risk)	 Medium (operational risk)
Banking system liquidity	 Negative impact	 Safe
CBDC integrity	 Vulnerable	 Protected
Overall risk rating	  High-Medium	  Low-Medium

Risk / Challenge:  High / Significant  Medium / Manageable  Low / Bounded

Conclusion:

- **Immediate offline mode:** Behaves like digital cash, which is inherently vulnerable to cloning, duplication, and systemic risks.
- **Deferred offline mode:** Behaves like a digital cheque / IOU, where settlement is controlled centrally. Only payment instructions are created and transferred offline.

3.2. Device Requirements & Hardware Dependencies

Immediate Offline Mode

To safely hold digital money offline, devices must include:

- Tamper-resistant secure elements (SEs)
- Trusted hardware execution zones
- Secure counters, clocks, monotonic timers
- Hardware lifecycle management (factory → replacement → revocation)
- Firmware attestation and anti-tamper features

This requires national-level coordination with hardware vendors, mobile OS providers, and terminal manufacturers.

Deferred Offline Mode

Deferred offline mode can rely on software-based virtual Secure Elements (vSE) allowing:

- Secure key storage
- Secure signing operations
- Anti-tampering protections
- Uniform deployment through software updates

No mandatory need for secure elements across the entire population of devices.

Conclusion:

- **Immediate offline mode:** Hardware-heavy, expensive, slow to deploy
- **Deferred offline mode:** Software-driven, scalable across all devices

3.3. Ledger Synchronisation & Reconciliation

Immediate Offline Mode

Offline value-token transfers produce chains of transfers that must be reconciled retroactively once devices reconnect. This process is complex, slow, and error-prone and requires:

- Token lineage reconstruction
- Conflict resolution for double spends
- Fraud detection across offline hops
- Potential rollback or rejection of transactions

Deferred Offline Mode

Deferred offline mode simplifies reconciliation:

- Instructions queue offline.
- Upon reconnection, the ledger validates each instruction.
- Invalid instructions are rejected.
- Exposure is bounded by offline spending limits.

Reconciliation mirrors existing financial clearing processes, using standard settlement logic.

Conclusion:

- **Immediate offline mode:** Complex, fragile reconciliation
- **Deferred offline mode:** Simple, deterministic settlement

3.4. *Ecosystem Integration*

Immediate Offline Mode

Value tokens must be universally recognized. This is extremely difficult in heterogeneous device ecosystems. The ecosystem must align on:

- Token formats
- Hardware security profiles
- Wallet behavior
- Device lifecycle processes
- Token revocation rules

Deferred Offline Mode

Deferred offline mode is simply an extension of mainstream digital payment logic. Deferred offline mode align naturally with today's payment infrastructure:

- EMV terminals already handle offline payment instructions
- PSPs understand deferred authorization flows
- Banks handle reconciliation and settlement
- ISO 20022 messaging can carry offline instructions
- Merchants adopt offline capability with minimal friction

Conclusion:

- **Immediate offline mode:** Requires entirely new infrastructure
- **Deferred offline mode:** Integrates smoothly with existing systems

3.5. *Scalability*

Immediate Offline Mode

Scaling immediate offline mode is limited by:

- Global secure hardware availability
- Testing and certification pipelines
- Device replacement challenges
- Fraud risk scaling with user base
- Complex token lifecycle management

Even advanced economies struggle with such requirements.

Deferred Offline Mode

Deferred offline mode relies on:

- Software deployment

- Existing merchant terminals
- Secure wallets with vSE
- Ledger validation at settlement

They inherit the scalability benefits of digital payments, with no hardware requirements.

Conclusion:

- **Immediate offline mode:** Hardware-limited scalability
- **Deferred offline mode:** Software-driven. Highly scalable.

3.6. *Interoperability (Domestic and International)*

Immediate Offline Mode

Token formats must be standardized across:

- Devices, vendors, and OS platforms
- Countries and regulatory frameworks
- Hardware secure elements

This is highly unlikely and would take decades.

Deferred Offline Mode

Deferred offline mode is inherently interoperable because:

- Instructions can follow ISO 20022
- Merchant-side acceptance aligns with EMV
- Cross-border flows can settle using existing clearing systems
- Layer-2 architectures enable wallets from different PSPs to interoperate
- Global CBDC networks like mBridge can incorporate instruction-based flows

Deferred offline mode can bridge CBDCs with:

- Domestic bank money
- Card payments
- Mobile money
- International CBDCs

Conclusion:

- **Immediate offline mode:** Difficult to standardize
- **Deferred offline mode:** Naturally interoperable

3.7. Impact on the Banking System: Liquidity, Lending Capacity, and Monetary Stability

A critical but often overlooked distinction between immediate and deferred offline modes lies in their impact on banking-system liquidity. Immediate-finality offline payments mirrors the macroeconomic implications of withdrawing physical cash: money is removed from deposit accounts and therefore from the bank's liquidity pool. This is in contrast to deferred offline payment mode where money reserved for offline use does not reduce the bank's liquidity pool. This makes the deferred offline mode fundamentally more compatible with bank-based financial systems.

Immediate Offline Mode

- A user transfers digital value tokens offline.
- These tokens function like digital cash, moving outside the banking system until they are redeemed.
- During this period, the funds are no longer available as bank deposits.

Consequences:

- Reduced deposit base for banks
- Lower lending capacity, as banks cannot use these funds for credit creation
- Potential liquidity fragmentation, especially if large sums migrate into offline wallets
- Higher systemic risk during prolonged offline periods

Deferred Offline Mode

Deferred offline mode is fundamentally more compatible with bank-based financial systems.

- The payer's funds remain locked or reserved in their bank or PSP account.
- Only a signed instruction (IOU) is exchanged offline.
- The bank or PSP still holds the funds and can continue using them for lending.

Benefits:











- No loss of deposits—funds remain with account-holding institutions.
- Lending capacity preserved, supporting the credit-generating function of the banking sector.
- Lower liquidity risk for the financial system.
- Better alignment with monetary policies, which relies on stable deposit bases.

Conclusion:

- **Immediate offline mode:** Money used offline leaves the banking system
- **Deferred offline mode:** Money reserved offline remains in the banking system

3.8. Summary Table

The summary table below highlights a decisive structural advantage for the Deferred Offline Mode (Digital Check / IOU) across all key technical, operational, and economic dimensions. In contrast, the Immediate Offline Mode (Digital Value Token) consistently exhibits high systemic risk, high implementation complexity, and poor scalability. This comparison shows that deferred offline mode is overwhelmingly superior as the baseline mode for offline functionality, with immediate offline mode possibly suitable for narrow, hardware-backed niche use cases.

Dimension	Immediate Offline Mode (Digital Value Token)	Deferred Offline Mode (Digital Check / IOU)
Security Challenge	 Very high. Requires tamper-resistant hardware SE, token integrity, double-spend controls	 Moderate. Offline runtime isolation of cryptographic signing with online validation and ledger-based finality
Device Requirements	 Requires hardware secure elements and lifecycle processes	 Software-based vSE; no hardware reliance
Risk Exposure	 High risk. Device compromise can lead to money compromise	 Limited risk. Ledger authoritative; offline runtime isolation and caps
Reconciliation	 Complex. Token chains, reconstructed offline	 Simple. Settle or reject payment instructions upon reconnection
Ecosystem Integration	 Difficult. Requires new token ecosystem	 Natural. Aligns with EMV and digital payments

Scalability	■ Low. Hardware-limited	■ Very high. Software-driven
Interoperability	■ Low. Hard to standardize tokens globally	■ High. Possibly ISO 20022 or EMV-compatible
Merchant Adoption	■ Challenging. Requires new hardware logic	■ Easy. Similar to offline card transactions
Deployment Cost	■ High	■ Low
Impact on banking system	■ Money exits banking system; reduces lending capacity	■ Money stays in banking system; supports lending and stability

Alignment / Risk: ■ Weak / High ■ Moderate / Medium ■ Strong / Low

Immediate offline mode resembles a digital cash token stored on devices. This imposes very high security requirements, including tamper-resistant hardware, secure elements, token lineage tracking, and sophisticated offline fraud controls. Device compromise equates to value compromise, producing high-risk exposure. It is hard to integrate into existing payment ecosystems, demands new hardware logic and certification flows, and scales poorly because deployments depend on OEM-controlled secure elements. It carries high deployment costs and reduces banking-system liquidity because value leaves bank balance sheets.

- **Immediate offlinemode:** high risk, hardware-heavy, costly, difficult to scale, poorly interoperable, and risk of destabilizing to the banking system.

Conversely, deferred offline mode relies on software-based cryptographic instructions rather than device-held value. This provides predictable, ledger-centric security, low hardware dependency, and simple reconciliation: payments settle or reject when connectivity returns. Risk exposure is tightly bounded by configurable spending caps. This mode aligns naturally with existing EMV, ISO 20022, and digital-payment infrastructures, enabling immediate merchant adoption and high interoperability. It is highly scalable, incurring vastly lower deployment and lifecycle

costs, and preserves bank deposits because funds remain with PSPs, supporting financial stability and lending capacity.

- **Deferred offline mode:** low-risk, software-driven, interoperable, easy to deploy, compatible with existing payment standards, and preserves banking-sector liquidity.

4. EMVCo and Mobile Card Precedents

The global payment card industry implemented offline-capable payments decades before CBDCs were conceived. EMVCo specifications provide a mature, proven system for deferred offline mode operating at massive international scale.

4.1. *EMV Smartcard Offline Capabilities*

Smartcards support offline authorization when a terminal lacks connectivity. The process:

1. Terminal performs Offline Data Authentication (ODA).
2. Card generates an EMV cryptogram, a signed payment instruction.
3. Terminal applies issuer-defined offline limits.
4. The terminal stores the transaction.
5. It forwards the instruction when online.

Critically:

- Cards do not move value offline.
- Offline approvals are provisional.
- Issuers remain authoritative.
- Settlement always occurs online.

This mode is directly analogous to deferred offline mode CBDC payments.

4.2. *Offline Mobile Card Payments*

Smartphones extend EMV offline capabilities using:

- Embedded Secure Elements
- SIM/eSIM secure elements
- Trusted Execution Environments (TEE)
- Virtual Secure Elements (vSE)

When offline, mobile wallets can:

- Generate EMV cryptograms offline
- Validate cardholder authentication locally
- Apply risk controls

Again, only payment instructions are transmitted offline—not monetary value.

4.3. *Deferred Offline Systems as an Extension*

Deferred offline mode CBDC payments extend EMV logic into wallet-to-wallet and wallet-to-merchant flows. This preserves:

- Cryptographic authentication
- Local approval
- Stored instructions
- Deferred online settlement

CBDCs generalize these capabilities beyond card systems into the broader digital money ecosystem.

4.4. *Implications for CBDCs and Digital Wallets*

Merchant Familiarity

Merchants already handle offline card transactions; CBDC deferred offline mode payments feel similar.

Low Incremental Cost

Existing terminals often need only software updates.

Global Scalability

EMV offline logic already operates across billions of devices.

Interoperability

Deferred instructions align with ISO 20022 and EMV, enabling domestic and cross-border compatibility.

5. Global Perspectives on Offline Payments

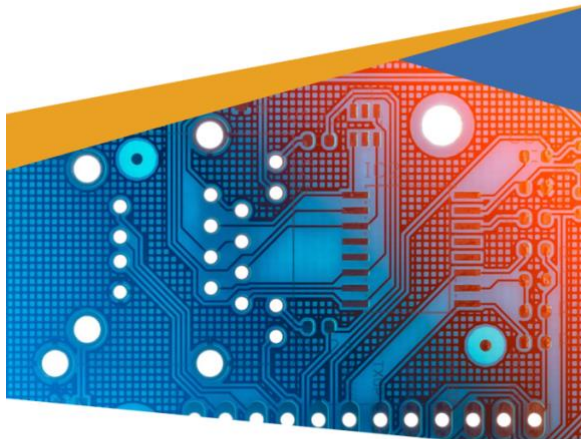
Offline payment research has expanded significantly across central banks and international institutions. Despite diverse objectives, there is strong convergence in global findings: instruction-based deferred offline mode offers a safer, more scalable, and more interoperable solution than digital value-token modes.

Below is a summary of key perspectives. Click on the images to get to the research papers.

BIS and Seven Leading Central Banks

The BIS and its partner central banks emphasize that offline capability is essential for resilience. They point out that for Offline CBDC two operating modes are possible:

- **immediate**, where there is immediate settlement between devices in a transaction; and
- **deferred**, where the settlement takes place after a device connects to the network.”



▶ Central bank digital currencies:

System design

November 2024

Bank of Canada
European Central Bank
Bank of Japan
Sveriges Riksbank

Swiss National Bank
Bank of England
Board of Governors Federal Reserve System
Bank for International Settlements

The BIS and its partnering central banks argue:

- Immediate offline mode systems introduce high systemic risk due to potential double spending and hardware compromise.
- Hardware-driven designs suffer from device lifecycle and operational complexity.
- Deferred offline mode are practical, more secure, and easier to supervise.

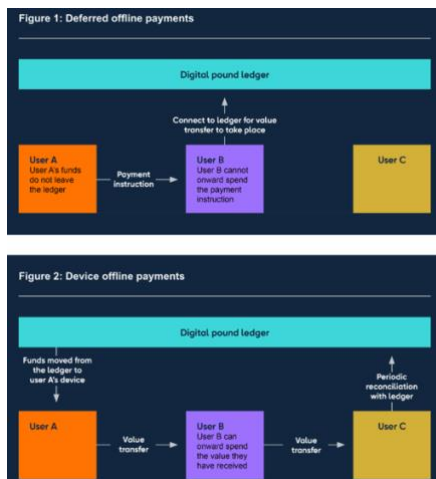
Bank of England

The BoE distinguishes between:

- **Device Offline Payments** → immediate offline mode with value tokens transferred offline
- **Deferred Offline Payments** → deferred offline mode with instruction transferred offline.

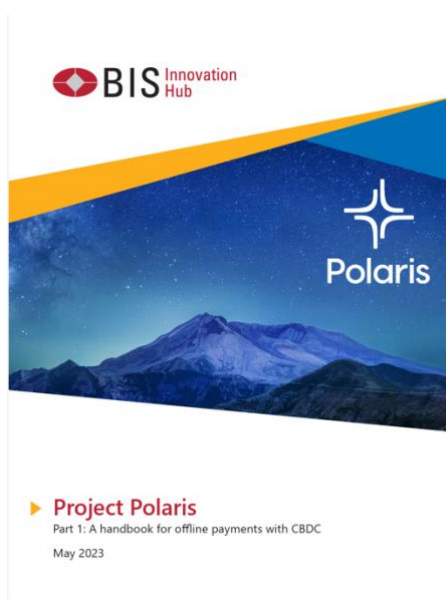
BoE concludes:

- Device offline payments, i.e. immediate offline mode, remain “under review” due to risk, complexity, and hardware requirements.
- Deferred offline mode payments aligns with the Bank’s roadmap for safe, incremental CBDC deployment.
- Deferred offline mode payments will be implemented first.



BIS Project Polaris

Project Polaris provides detailed technical and operational insights for building offline-capable CBDC systems.



BIS Project Polaris findings:

- Immediate offline payments demand secure elements on consumer devices.
- Device lifecycle management—including provisioning, replacement, and deactivation—is complex and expensive.
- Layered, modular architectures are strongly preferred.
- Deferred offline mode aligns with realistic constraints and modern digital payment patterns.

Bank of Canada

The Bank of Canada references MIT's OpenCBDC 2PC architecture for online CBDC settlement integrity. It conceptually supports layer-2 deferred offline mode rather than immediate offline mode.

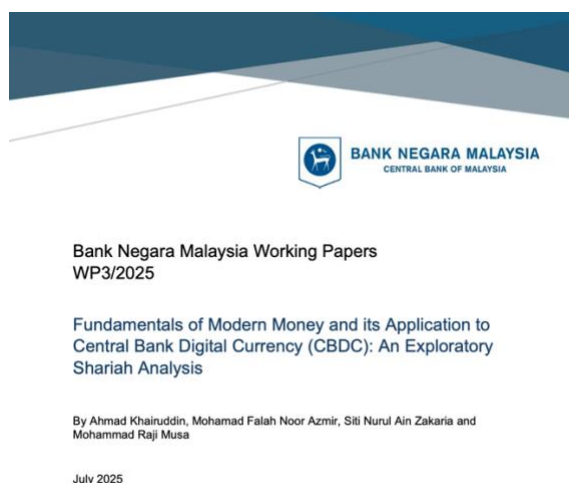


Although designed for online CBDC, there is alignment with deferred offline mode:

- Prepare phase resembles creation of an offline IOU.
- Commit phase resembles online settlement.
- Strong atomicity prevents double spending at the point of ledger update.

Bank Negara Malaysia (BMN)

BNM reinforces the rationale for the deferred offline mode conceptually in its working paper on the Fundamentals of Modern money and its Application to CBDC: An Exploratory Shariah Analysis from July 2025.



Modern money, including CBDC, is fundamentally a credit relation:

- It aligns with the deferred offline mode as funds remain with the issuing bank until online settlement, when obligations are discharged on the issuer's balance sheet.
- In contrast, the immediate offline mode, mimics commodity money, and introduces higher systemic risk and liquidity leakage from the banking system.

International Monetary Fund (IMF)

The IMF's 2025 Fintech Note underscores CBDC systems must balance security, usability, and feasibility and that offline is essential for inclusion and resilience.



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

The IMF's guidance aligns closely with deferred offline mode:

- Immediate offline mode is conceptually appealing but carries significant operational risk.
- Deferred offline mode is a more realistic for early adoption.
- Final settlement should occur online, preserving ledger authority.

Kiffmeister Chronicles

A note presents the Crunchfish Digital Cash (CDC) Layer-2 solution as a viable augmentation to a central bank digital currency (CBDC) payment system.



CBDC STABLECOINS CRYPTO ASSETS SPECIAL MONTHLY MONITOR INTELLIGENCE

Rethinking CBDC Retail Payments with
Crunchfish Digital Cash Layer-2
Architecture



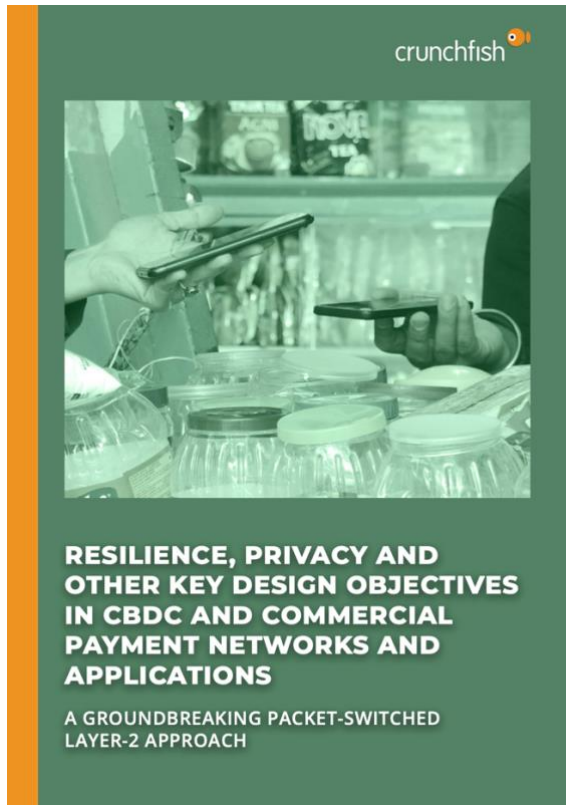
SEPTEMBER 2, 2025 - KIFFMEISTER

The note argues that deferred offline mode as the superior design choice:

- Immediate offline mode introduces unnecessary risk without adding functional advantages.
- IOU-based offline payments are safer, more scalable, and more interoperable than value tokens.
- Layer-2 architectures allow deferred offline mode to coexist seamlessly with both CBDC and commercial bank systems.

Crunchfish

Crunchfish contributes practical, implementation-ready expertise through its Digital Cash Layer-2 architecture.



Crunchfish's approach is an example of a deployable, real-world deferred offline mode solution:

- IOU-based instruction flows
- Support for consecutive offline payments via secure provisional balances
- Software-based vSE security
- Interoperability across CBDC, bank money, and commercial wallets
- Scalable deployment in national systems

6. Comparison across key design dimensions

An additional comparison between immediate and deferred offline mode across key design dimensions has been proposed by Crunchfish.

- | | |
|----------------|------------------------|
| 1. Security | 5. Interoperability |
| 2. Scalability | 6. Universality |
| 3. Resilience | 7. Seamlessness |
| 4. Privacy | 8. Cost Effectiveness. |

It underscores also why deferred offline mode is a safer, more scalable, and more future-proof foundation, with immediate offline mode reserved for niche, hardware-backed use cases.

Category	Immediate Offline Mode (Digital Value Token)	Deferred Offline Mode (Digital Check / IOU)
Security	<p>■ High-security burden; device compromise risks token cloning; offline-final transactions amplify systemic exposure.</p>	<p>■ Ledger-based security; double-spend constrained by online settlement; uses mature cryptographic flows.</p>
Scalability	<p>■ Scaling tied to secure-element penetration, OEM cooperation, and hardware certification.</p>	<p>■ Software-only scaling across all smartphones and terminals; avoids hardware bottlenecks.</p>
Resilience	<p>■ Strong local resilience but higher systemic fragility due to token lineage and SE compromise recovery risks.</p>	<p>■ High systemic resilience; offline payments continue while finality remains controlled at settlement.</p>
Privacy	<p>■ Natural cash-like privacy; device-to-device value transfer shares almost no data online.</p>	<p>■ Configurable. Can achieve strong privacy via local pseudonymisation and minimal settlement data.</p>
Interoperability	<p>■ Requires harmonised token formats and hardware profiles; global standardisation extremely challenging.</p>	<p>■ Fits ISO 20022, EMV-style flows and multiple settlement rails (CBDC, A2A, cards).</p>
Universality	<p>■ Constrained by hardware availability and secure-element access; less universal across user groups and devices.</p>	<p>■ Works on all modern devices; supports all payment rails and use cases, including transit and offline public services.</p>
Seamlessness	<p>■ Cash-like for users but complex for PSP back offices; creates a parallel "mini-ledger" paradigm.</p>	<p>■ Familiar EMV-style flow for PSPs and merchants; easy to integrate; smooth UX for users.</p>
Cost Effectiveness	<p>■ High CapEx/OpEx due to hardware rollout, certification, SE lifecycle, and incident management.</p>	<p>■ Low marginal cost; software-driven; uses existing infrastructure; minimal certification overhead.</p>

Alignment / Risk: ■ Weak / High ■ Moderate / Medium ■ Strong / Low

The immediate offline mode excels primarily in privacy and cash-like user experience, but displays significant weaknesses in security, scale, interoperability, universality, and cost. Its dependency on secure hardware and its offline-finality risks make it far more complex to deploy and govern at euro-area scale. While immediate offline mode offers a strong cash-like privacy experience, it introduces high operational and systemic risk, depends heavily on secure hardware availability, and scales poorly in diverse device environments.

The analysis shows that the deferred offline mode based on signed payment instructions and online settlement consistently delivers superior alignment with system-wide requirements, achieving strong performance in security, scalability, resilience, interoperability, and cost. The deferred offline mode demonstrates strong alignment across nearly all eight design dimensions. It offers a scalable, secure, device-agnostic, and cost-efficient approach suitable for broad adoption, while maintaining compatibility with existing PSP infrastructures and preserving banking-system liquidity.

7. Evolution Toward Deferred Offline Mode

1990s–2000s:	EMV Smartcards <ul style="list-style-type: none"> • Introduce cryptographic offline authorization • Deferred clearing becomes standard
2010s:	Mobile Secure Hardware <ul style="list-style-type: none"> • SE/eSIM/TEE architectures enable offline EMV on mobile devices • Billions of mobile devices gain offline capability
2020–2024:	CBDC Exploration <ul style="list-style-type: none"> • Immediate offline mode is explored (value tokens) • Risks and hardware limits become evident
2024–2027:	Shift Toward Deferred Offline Mode <ul style="list-style-type: none"> • BIS, BoE, IMF: deferred is safer and more realistic • Crunchfish demonstrates deployable Layer-2 architecture

Future:	Interoperable Layer-2 Systems <ul style="list-style-type: none"> • CBDC + bank money + PSP wallets interoperable offline • Cross-border settlement through mBridge-like platforms • ISO 20022 and EMV alignment.
----------------	--

8. Policy Implications

Based on the synthesis of global perspectives, several key policy recommendations emerge for governments, regulators, and central banks:

8.1. *Adopt Deferred Offline Mode as the Baseline*

Deferred offline mode provides the best balance of:

- Operational feasibility
- Risk mitigation
- Consumer usability
- Merchant acceptance
- Regulatory clarity
- Scalability and interoperability

Immediate offline mode should be optional future enhancements, not a prerequisite.

8.2. *Establish a Layer-2 Architecture*

A separate Layer-2 solution allows offline capability to operate above:

- CBDC
- Commercial bank money
- E-money
- Private wallets
- PSP ecosystems

This enhances flexibility and future-proofs the system.

8.3. *Deploy Software-Based Security (vSE)*

Virtual secure elements provide:

- Strong tamper protection
- Wide device compatibility
- Cost-effective national deployment
- Rapid rollout to diverse populations

This avoids the hardware burden of immediate-mode systems.

8.4. *Support Consecutive Offline Payments*

Offline capability should allow:

- Receivers to store instructions securely
- Wallets to credit a provisional offline balance
- Users to make additional offline payments

This ensures cash-like usability in offline environments without sacrificing ledger integrity.

8.5. *Implement Risk Controls and Tiered Limits*

To maintain safety:

- Offline spending caps
- Velocity limits
- Authentication requirements
- Maximum consecutive offline hops
- Revocation mechanisms

These controls ensure systemic stability even in large-scale rollout.

8.6. *Use Standardized Messaging (ISO 20022 & EMV)*

Using global payment standards ensures:

- Domestic interoperability
- International interoperability
- Compatibility with bank and PSP systems
- Compatibility with cross-border CBDC networks (e.g., mBridge)

9. Conclusion

Offline payment capability is essential for resilient and inclusive digital payment ecosystems. While two modes exist across BIS, BoE, IMF, and Crunchfish analyses, the conclusion is clear:

- **Immediate offline mode**, based on offline value transfer, are limited by hardware requirements, operational fragility, and high systemic risk.
- **Deferred offline mode**, based on signed payment instruction transferred offline and online settlement, are safer, more scalable, and more interoperable.

Deferred offline mode is the sound approach for enabling offline digital transactions at national and international scale. It avoid the pitfalls of immediate-mode systems while offering nearly the same cash-like user experience and far stronger operational viability.

crunchfish 