crunchfish
RETHINKING PAYMENTS

OFFLINE PAYMENTS AT SCALE AS DIGITAL MONEY

Architectural Requirements for Resilient Payment Systems

BANKABLE

IMPLEMENTABLE

GOVERNED

Executive Whitepaper
March 2026

FOREWORD

Digital payments are evolving from convenience infrastructure into critical societal infrastructure. Retail commerce, public services and financial inclusion increasingly depend on continuous payment availability. Payment system resilience is therefore no longer merely a technical consideration. It is an institutional responsibility.

Offline capability is often described as a contingency feature. Structurally, however, offline functionality is an architectural design choice. That choice determines where ledger authority resides, how payment obligations behave, and whether liquidity remains anchored within regulated institutions when real-time validation or underlying system availability is disrupted.

This executive whitepaper introduces a structured institutional BIG Analytical Framework for evaluating offline architecture. It examines whether offline capability can scale without distorting funding structures, fragmenting interoperability, or altering governance continuity.

Resilience at scale is ultimately a governance question. Architecture determines whether governance remains intact.

Joachim Samuelsson
Crunchfish CEO

Understanding the Traffic Light

The cover of this whitepaper presents three green lights: This is not a claim of perfection. It is a structured signal. The traffic light is used deliberately as an analogy. When a traffic light turns green, it does not mean that driving is risk-free. Roads remain complex. Other vehicles move unpredictably. Weather changes. Human error exists. A green light does not remove risk. It indicates that the structural conditions to proceed are aligned. It signals that movement is permitted within a governed framework. The same principle applies here.

The traffic light in this whitepaper does not suggest that governed offline payments eliminate all operational, technical, or policy risks. No payment architecture can do that. What it signals is that, relative to alternative offline models, the structural conditions for institutional alignment are satisfied.

Three green lights represent alignment across three institutional constituencies:

Bankable	**Friendly to banking economics.** Liquidity remains anchored within regulated institutions. Exposure is predefined and bounded. Funding efficiency is preserved.
Implementable	**Friendly to service providers and ecosystems.** Architecture scales across heterogeneous devices and acceptance environments without vendor lock-in or scheme fragmentation.
Governed	**Friendly to system operators and regulators.** Central ledger authority remains intact. Exposure does not expand unpredictably during disruption. Governance continuity is preserved.

A green light (🟢) therefore signals structural compatibility with institutional incentives. It does not imply the absence of risk. It indicates that known systemic distortions are not introduced by design.

Green does not mean risk-free. It means structurally aligned.

By contrast, a yellow light (🟡) signals that known systemic risks are embedded in the architecture in addition to ordinary operational risk. For example, deferred offline models accumulate temporary unmanaged credit exposure during disruption. That exposure must be supervised and absorbed. It is a structural feature, not a residual risk.

A red light (🔴) signals that severe known systemic risks are structurally introduced that alter governance boundaries. For example, immediate offline models relocate monetary representation to devices and assert local finality. This creates a parallel monetary form at device level and partially externalises monetary integrity.

In road traffic, passing a red light introduces predictable systemic danger beyond normal driving risk. The same logic applies architecturally. The traffic light framework is therefore comparative and institutional. It evaluates whether an offline architecture introduces structural distortions in liquidity anchoring, exposure behaviour, or governance continuity.

Governed offline receives three green lights not because it is risk-free, but because it does not introduce additional systemic distortions beyond those inherent in operating digital payments at scale. All green means proceed with institutional discipline.

A green signal therefore indicates that an architecture satisfies institutional compatibility conditions. It does not imply absence of risk, but that risks remain governable within the structure of the payment system.

The traffic light evaluates structural risk, not operational incidents.

EXECUTIVE SUMMARY

crunchfish
RETHINKING PAYMENTS

Retail payment systems must remain operational during connectivity interruptions, operational incidents, cyber events, and periods when the underlying payment system is temporarily unavailable. Offline capability is therefore increasingly examined in central bank, instant payment, CBDC and mobile-money payment ecosystems. Such ecosystems are often central to financial inclusion in emerging and developing economies.

Retail payment systems must remain operational during connectivity interruptions, operational incidents, cyber events, and temporary unavailability of underlying infrastructure. Offline capability is therefore increasingly examined in central bank, instant payment, and CBDC contexts.

Offline architectures influence governance boundaries in materially different ways. The architectural choice determines how ledger authority, exposure, and liquidity behave under disruption and whether resilience reinforces the payment system or unintentionally reshapes it.

This whitepaper introduces the **BIG Analytical Framework (Bankable, Implementable, Governed)** as an institutional lens for evaluating offline payment architectures:[1]

Bankable Liquidity, Exposure & Funding Efficiency	Liquidity remains anchored within regulated institutions. Exposure is predefined and bounded. Funding efficiency is preserved even when transactions occur without real-time connectivity.
Implementable Scalable, Interoperable & Vendor Neutral	Architecture scales across heterogeneous devices, acceptance environments, and payment ecosystems without embedding vendor-specific logic into the payment system.
Governed Risk, Privacy & Authority Continuity	Central ledger authority remains intact, systemic exposure remains bounded, and privacy can be preserved in a way that remains consistent with supervisory and AML/CFT obligations.

The objective is coherence: enabling offline payments at scale as digital money by preserving governance continuity rather than redefining it. Implementability at scale also requires vendor neutrality, so offline capability can be adopted across an ecosystem without creating structural vendor lock-in.

Privacy is not delivered by being offline. It is delivered by architecture, and by how settlement and reconciliation are designed under the chosen governance model.

1. The BIG Analytical Framework is presented as an analytical framework for evaluating offline payment architectures. The framework does not depend on a specific technology or vendor implementation.

Offline is an Architectural Decision

Offline capability is increasingly considered essential for payment systems that function as societal infrastructure. The central question is therefore no longer whether offline functionality is required, but how it should be architected so that resilience strengthens rather than alters the institutional structure of digital money. The analysis presented in this paper leads to several architectural observations.

Offline capability is often described as a contingency feature. In practice it is an architectural design choice that determines how digital money behaves when real-time validation or connectivity is unavailable. Architectural design determines where authority resides, how exposure emerges during disruption, and whether liquidity remains anchored within regulated institutions.

Three Structural Offline Architectures

Three principal architectural approaches are observed in practice.

• **Immediate offline** replicates physical cash behaviour digitally by transferring stored value at the device level.
• **Deferred offline** replicates cheque-style authorisation by allowing transactions that are verified later once connectivity returns.
• **Governed offline** structures offline capacity as policy-defined reserved limits derived from existing balances or approved credit allocations while preserving central settlement authority. This capacity is created through a backend reservation that allocates a bounded offline spending limit to the wallet while ensuring the same value cannot be spent simultaneously online.

Each architecture affects liquidity anchoring, exposure behaviour and governance continuity differently.

Interoperability Requires Two Conditions

For transactions executed in one layer to settle into another payment system, two structural conditions must be satisfied: authorised intent to pay and assured sufficiency of funds.

• **Immediate and deferred** architectures satisfy one of these conditions structurally while the other remains conditional or coupled to device- or scheme-specific logic.
• **Governed offline** is the only architecture in which both conditions can be satisfied simultaneously through standardised, verifiable payment instructions.

Governed Offline Architecture and Settlement Model

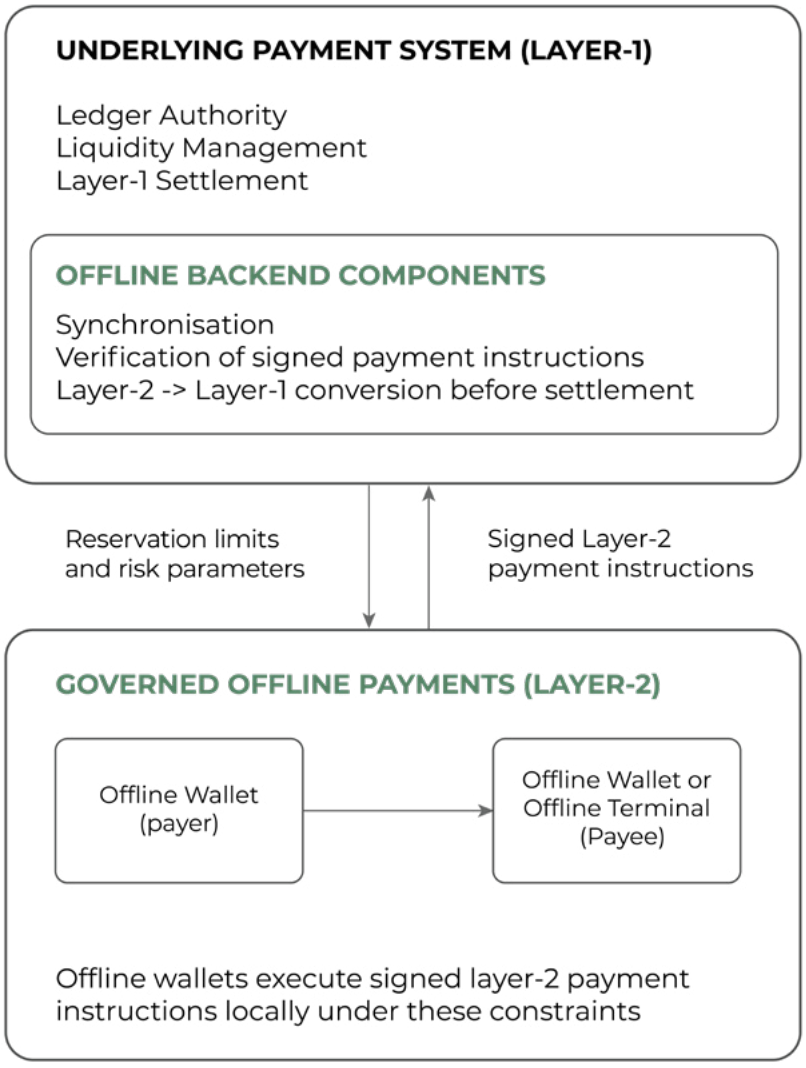


Figure 1: *Governed offline separates local execution from settlement authority. Offline capacity is derived from centrally governed limits, ensuring that liquidity remains anchored within the payment system while enabling transactions during connectivity interruptions.*

Protecting Payment Instructions Is Different From Protecting Money

Offline architectures also differ in the asset protected within the device environment.

Immediate offline protects stored monetary value and therefore typically rely on hardware secure elements.

Deferred and governed offline protect payment instructions rather than device-held money. As a result, security may be implemented either through hardware secure elements or through certified isolated runtime environments in software.

This distinction allows greater deployment flexibility while preserving system integrity.

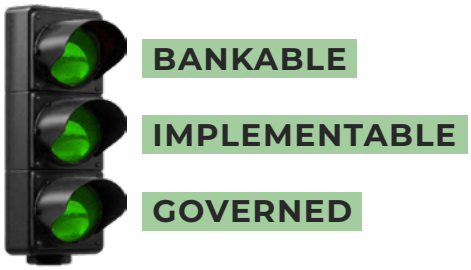
Institutional Compatibility Determines Scalability

Offline architectures must ultimately be evaluated not only for technical feasibility but also for institutional compatibility. The BIG Analytical Framework evaluates whether an architecture aligns with the structural requirements of payment systems operating at national scale.

Bankable	Liquidity remains anchored within regulated institutions, exposure remains bounded, and funding efficiency is preserved.
Implementable	Architectures scale operationally through interoperability, vendor neutrality and deployable execution environments.
Governed	Monetary integrity, privacy alignment and operational governance remain intact even when real-time validation is unavailable.

Architecture Determines Institutional Outcome

When these structural conditions are satisfied simultaneously, offline capability no longer functions merely as a contingency mechanism. It becomes a resilience layer integrated into the architecture of digital money.



Governance Boundaries and Offline Architectures

Architecture determines whether resilience reinforces or reshapes digital money governance. To understand this, we must examine the institutional boundaries that offline design affects. These boundaries define how authority, exposure, and liquidity behave when normal system conditions are disrupted.

When real-time validation or underlying system availability is interrupted, the fundamental question is whether the governance structure of digital money remains intact. Offline capability must therefore be evaluated as architecture, not as a feature.

Governance Boundaries

Three institutional boundaries are affected:

Ledger Authority	Where authoritative ledger state and settlement finality reside during offline operation.
Payment Obligations and Exposure	Whether exposure accumulates or remains bounded during disruption.
Liquidity Anchoring	Whether liquidity remains within regulated institutions or relocates outward.

Architecture determines how these boundaries behave under stress.

Three Principal Offline Architectures

Three principal offline architectures are observed in practice: **Immediate, Deferred, and Governed.**

Immediate offline seeks to replicate physical cash digitally. Value is stored or transferred at device level through hardware-dependent or token-dependent logic. Finality is asserted locally.

Deferred offline seeks to replicate cheque-style authorisation. Transactions are accepted offline and verified later. Exposure exists temporarily within issuer or scheme defined limits.

Governed offline seeks to enable digital money to function offline without altering its monetary character. Ledger authority remains central. Liquidity remains anchored within regulated institutions. Exposure is predefined and bounded.

Immediate replicates cash. Deferred replicates cheques.
Governed Offline preserves digital money.

Interoperability Between Payment Layers

For one payment layer to post settlement into another, two structural conditions must be satisfied: authorised intent to pay and assured sufficiency of funds.

If either condition fails, interoperability becomes conditional rather than structural. Immediate and deferred models each satisfy one interoperability condition structurally, while the second becomes conditional or coupled to device- or scheme-specific logic. Governed offline is the only architecture in which both conditions are satisfied simultaneously through standardised, verifiable instructions.

Interoperability requires two conditions.
Governed offline satisfies both locally on device.

A third architectural consequence follows from these two conditions: vendor neutrality. If a payment system must embed wallet-specific logic to trust intent or sufficiency, the system becomes coupled to a particular offline module. If intent and sufficiency are verifiable through standardised instructions, multiple wallet providers can interoperate on equal terms under the same acceptance framework.

Immediate offline guarantees sufficiency through value transfer. However, authorised intent becomes inseparable from hardware or token logic. This tight coupling constrains vendor neutrality because acceptance depends on device-specific or token-specific logic rather than standardised payment instructions.

Deferred offline captures authorised intent. Sufficiency of funds is verified only after connectivity is restored. Vendor neutrality can exist within card-scheme ecosystems where standards such as EMVCo enable multiple vendors to implement compatible acceptance. However, neutrality remains scheme-bounded rather than structurally cross-system.

Governed offline satisfies both structural conditions simultaneously. Authorised intent is cryptographically verifiable through signed payment instructions. Sufficiency of funds is secured in advance through centrally governed reservations. At the time of reservation, the payment system allocates an offline spending limit to the wallet and places a corresponding hold on funds or credit in the backend. Both conditions are enforced locally within an isolated runtime environment governed by strict business logic, while central ledger authority remains intact.

Because intent and sufficiency are guaranteed at the point of execution, offline wallets interoperate with payment systems in the same structural way as online wallets. The system verifies standardised instructions. It does not embed vendor specific wallet logic. Vendor neutrality therefore becomes structural. This enables ecosystem rollout without binding the underlying payment system to a single vendor's offline implementation. The payment system validates a standardised instruction set rather than a proprietary wallet implementation.

Multiple wallet providers can interoperate within a common offline acceptance framework. Cross-service and cross-system interoperability remain possible because central authority is preserved. Vendor neutrality becomes structural because payment systems verify standardised instructions rather than wallet-specific execution logic.

Vendor neutrality is an architectural outcome.
Multiple offline wallet providers can interoperate. No vendor lock-in.

Regulatory and Governability Implications

Immediate offline introduces device-level monetary representation. This creates a parallel monetary form distinct from centrally governed digital balances.

Deferred offline introduces temporary unmanaged credit exposure.

Governed offline does not introduce a new monetary form. Offline capacity represents centrally reserved balances. Exposure is predefined and bounded. Authority remains central. Because risk is governed and bounded by design, supervisory continuity is preserved. Structurally bounded exposure supports clearer supervisory thresholds than models that relocate liquidity or accumulate unmanaged exposure.

Offline should preserve digital money, not redefine it.

Privacy and Supervisory Reality

Offline capability is often assumed to improve privacy by default. In practice, privacy depends on where reconciliation and supervisory controls reside, and how AML/CFT obligations are met.

Immediate offline can, in theory, approximate physical cash anonymity. In practice, few system operators are willing to accept full anonymity at scale, because they must balance privacy with AML/CFT compliance, fraud control, and recovery processes. This commonly leads to centrally governed reconciliation functions and monitoring mechanisms. For citizens, this can reduce perceived privacy, especially in CBDC contexts where the state is also the system operator. The privacy promise becomes asymmetric and uncertain under real-world governance.

Deferred offline, as implemented in card-scheme environments, typically provide privacy at the merchant interface through tokenisation and related mechanisms. However, settlement requires detokenisation or equivalent resolution so the customer's account can be debited at the remitting bank. Privacy is therefore partial and context-bounded. It protects the customer from broad merchant visibility, but not from the institutions required for settlement.

Governed offline can preserve privacy consistently across the ecosystem by design. For any payment rail, settlement can be structured so the remitting bank pays by proxy for the customer. The remitting bank retains full visibility for compliance and customer protection, while other ecosystem participants see only what is necessary for acceptance and settlement. This same approach can be applied to online payments as well, enabling symmetry of privacy regardless of connectivity or system availability.

Full anonymity can also be implemented for governed offline as a special case by debiting and crediting offline balances without attribution, typically only for small amounts. However, if anonymity exists only for small values, it introduces asymmetry with online payments and may not justify the added governance risk. For institutional deployments, privacy is most robust when it is consistent, controllable, and aligned with supervisory obligations. Structurally bounded exposure supports clearer supervisory thresholds than models that relocate liquidity or accumulate unmanaged exposure.

Privacy is not an offline feature.
Privacy is a settlement and governance design choice.

Offline Architecture	Immediate Offline Model	Deferred Offline Model	Governed Offline Model
Ledger Authority	🔴 Ledger authority and systemic exposure at device-level	🟢 Ledger authority remains central	🟢 Ledger authority remains central
Payment Obligations & Exposure	🟢 Bounded by device-value	🟡 Exposure accumulates during disruption	🟢 Exposure bounded by design
Liquidity Anchoring	🔴 Liquidity relocates to devices	🟢 Remains in regulated accounts	🟢 Reserved within regulated accounts

Table 1: *Immediate and deferred architectures alter at least one governance boundary. Governed offline preserves governance continuity while bounding exposure and maintaining liquidity anchoring.*

Governed Offline Architecture

Governed offline separates local execution from settlement authority, as illustrated in Figure 1. Governed offline payments are structured as a Layer-2 capability operating above the underlying payment system. Execution may occur locally, but ledger authority and final settlement remain anchored within Layer-1.

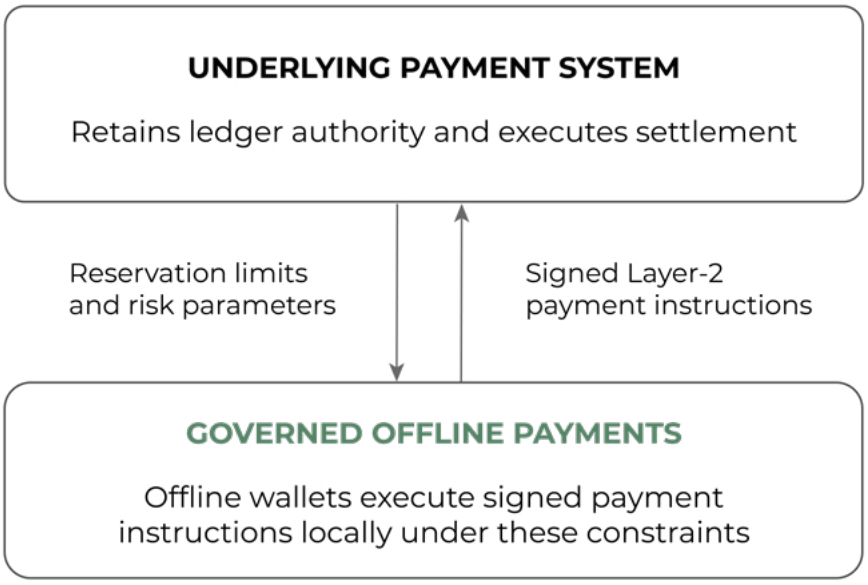


Figure 2: *Governed offline operate at Layer-2[2], while ledger authority and settlement remain within the underlying payment system (Layer-1).*

Regulatory Recognition

In December 2023, Crunchfish in partnership with HDFC Bank and IDFC First Bank completed the Reserve Bank of India's Regulatory Sandbox test phase for offline retail payments and exited the sandbox. Governed offline is approved by RBI for adoption by regulated entities, subject to applicable regulatory requirements.

This demonstrates that the governed offline model, built on a centrally governed reservation mechanism has been evaluated within a central bank supervisory framework and can operate within existing governance structures while preserving central ledger authority and defined exposure limits.

Governed offline may be considered by regulated entities in India.

2. The governed offline architecture described in this paper is payment-rail agnostic and may operate above either account-based systems, token-based systems or hybrid payment infrastructures.

Governed offline also enables privacy continuity. Because offline instructions can settle without exposing customer-level payment details across the ecosystem, privacy can be designed to match the payment system's chosen policy model. A bank-proxy settlement pattern can preserve customer privacy at ecosystem level while retaining full visibility within the remitting bank for compliance and customer protection. This supports a consistent privacy posture online and offline, rather than treating offline as a special case.

Layer Separation and Governance Continuity

Governed offline separates execution from settlement without separating authority.

- **Layer-1** retains authoritative ledger state and settlement finality.
- **Layer-2** provides controlled offline functionality within predefined limits.

Offline execution may occur locally.
Authority remains central.

Reserve, Pay, and Settle Lifecycle

Reserve	Offline capacity is reserved centrally while the wallet is online. The payment system allocates a bounded offline spending limit to the wallet and places a corresponding reservation on funds or credit in the backend so the same value cannot be spent simultaneously online.
Pay	Payment instructions are generated locally within reservation-derived limits.
Settle	Instructions are verified and converted into native Layer-1 settlement messages.

Settlement does not alter total reservations in the system.

Operational Incidental Risks

As with any offline architecture, incidental operational risks exist and are managed through policy thresholds and certification standards defined by the underlying payment system. Offline execution depends on the integrity of the device execution environment. Malicious actors may attempt replay attacks, stored-state manipulation, or duplication of payment instructions. Such attacks could create temporary exposure until settlement verification occurs.

These risks are mitigated through certified isolated runtimes, cryptographic signing, transaction deduplication, certificate revocation, and wallet lock mechanisms. Importantly, these attacks do not compromise monetary integrity. Settlement verification prevents unauthorised value creation, and compromised wallets can be revoked when connectivity is restored.

As with other instruction-based offline architectures, the primary risk concerns execution-environment integrity rather than loss of stored monetary value. Additional considerations include dispute handling, consumer protection, reconciliation cadence, monitoring, and supervisory oversight.

Execution Environment and Security Architecture

Offline architectures differ in the nature of the asset protected within the device environment.

Immediate offline stores or transfers monetary value locally. Protecting device-resident value therefore requires strong tamper resistance, typically implemented through hardware secure elements or specialised payment hardware.

Deferred and governed offline generates cryptographically verifiable payment instructions that are settled later by the underlying payment system. Devices therefore protect payment instructions rather than monetary value.

Because the protected asset is a payment instruction rather than stored money, different security architectures become possible. Both hardware secure elements and certified software-based isolated runtimes can protect the execution environment. Governed offline can therefore operate within hardware-secure elements or within certified virtual secure elements. This allows system operators to balance security assurance, deployment flexibility, and operational governance while preserving the monetary form of the underlying payment system.

When payment instructions are protected instead of money, security can be governed by architecture rather than hardware alone.

System-Level Reservation Logic

At system-level, settlement of offline transactions does not change the total amount of reserved funds. The aggregate reservation pool changes only when users deliberately reserve additional offline capacity or release reservation after reconciliation. Settlement only redistributes reserved value between parties. It does not alter the reserved amount in total.

Reserved liquidity remains anchored within regulated institutions. Deposits are not fragmented into device-level monetary forms. Unmanaged credit exposure does not expand temporarily. Because aggregate reservations change only through deliberate reserve or release operations, liquidity remains structurally predictable.

Conceptually, this reservation functions similarly to a payment-card pre-authorisation, except that the reservation is held for the payer's own offline capacity rather than for a third-party merchant. In architectural terms, the reservation functions similarly to a conditional settlement instruction, comparable to a self-beneficiary smart contract that executes once the payment system verifies a signed payment instruction.

Governed offline differs from legacy models because sufficiency of funds is secured before the transaction occurs, not verified afterward or transferred to the device.

The BIG Analytical Framework: Institutional Evaluation

The BIG Analytical Framework provides a structured method for assessing whether an offline architecture remains compatible with the institutional structure of modern payment systems.

Bankable - liquidity anchoring, bounded exposure, funding efficiency
Implementable - scalable deployment, interoperability, vendor neutrality
Governed - monetary integrity, privacy alignment, operational governance

Bankable: Liquidity, Exposure and Funding Efficiency

Immediate offline relocates liquidity to devices.

Deferred offline introduces temporary unmanaged exposure.

Governed offline preserves institutional anchoring. Reserved balances remain within regulated institutions. Exposure is predefined and bounded. Because aggregate reservations change only through deliberate reserve or release operations, liquidity remains structurally predictable. As shown in Figure 1, liquidity remains anchored within the payment system because offline capacity derives from existing balances or credit allocations.

Implementable: Scalable, Interoperable and Vendor Neutrality

Immediate offline is hardware-dependent and token-dependent. Interoperability is constrained and vendor lock-in risk emerges at the system interface.

Deferred offline is scheme dependent. Vendor neutrality can exist within scheme standards such as EMVCo, but implementation remains bounded by scheme rules rather than structurally cross-system.

Governed offline verifies standardised payment instructions without embedding wallet-specific logic. Vendor neutrality becomes structural, enabling multiple wallet providers to interoperate within the same offline acceptance framework.

Because governed offline operates above the underlying payment system, it can be implemented across multiple payment system models. The same architectural principles apply whether the underlying infrastructure is a central bank-operated system, a bank-led instant payment network, or a telecom-operated mobile-money ecosystem.

Governed: Risk, Privacy and Authority Continuity

Immediate offline can imply strong privacy in theory, but at institutional scale they typically require central reconciliation and supervisory controls that weaken perceived privacy, especially in CBDC contexts.

Deferred offline often protect privacy at acceptance through tokenisation, but settlement requires resolution and debiting at the remitting bank. Privacy is therefore partial and bounded by scheme processes.

Governed offline enables privacy continuity as a design option. Bank-proxy settlement can preserve ecosystem privacy while maintaining compliance visibility within the remitting bank. Authority remains central and exposure remains bounded by design. Because exposure, execution environments and settlement authority remain governed centrally, supervisory control of the ecosystem remains intact even during disruption.

The BIG Analytical Framework Impact of Offline Architectures

The BIG Analytical Framework does not prescribe policy. It provides a structured institutional lens for evaluating whether offline capability can operate at scale as digital money.

Offline Architecture	Immediate Offline Model	Deferred Offline Model	Governed Offline Model
Bankable Liquidity, Exposure & Funding Efficiency	🔴 Liquidity relocates to devices	🟡 Neutral funding, credit exposure builds	🟢 Reserved liquidity, predefined exposure
Implementable Scalability, Interoperability & Vendor Neutrality	🔴 Hardware and token dependent; vendor lock-in risk	🟡 Scheme dependent; vendor-neutral within scheme standards	🟢 Structurally interoperable; vendor-neutral acceptance
Governed Risk, Privacy & Authority Continuity	🔴 Theoretical anonymity, but scale typically requires central reconciliation and controls, privacy becomes uncertain, governance risk high	🟡 Tokenised privacy at acceptance, but detokenisation needed for settlement, privacy partial and scheme bounded	🟢 Bank proxy settlement enables ecosystem privacy, compliance visibility retained within remitting bank, authority central and exposure bounded

Table 2: *Institutional alignment across liquidity, implementability (scalable, interoperable, vendor neutral), and governance determines whether offline payment resilience can scale sustainably.*

Resilience scales only when it is
Bankable, Implementable, Governed as Digital Money.

Governed Offline Enables Resilience Without Structural Trade-Off

Offline payments do not require redesigning the governance of digital money. They require choosing an architecture that preserves it. This whitepaper has examined offline architecture through institutional incentives, deployment conditions, and governance boundaries. The conclusion is straightforward: Resilience is achieved not by altering the institutional monetary order under stress, but by preserving it.

Legacy offline models introduce structural trade-offs. Liquidity relocates. Exposure accumulates. Governance boundaries shift.

- **For banks,** this affects funding discipline.
- **For payment providers,** it constrains scalability.
- **For central banks,** it alters supervisory continuity.
- **For system operators,** it determines whether liquidity discipline, scalability, and governance continuity can be aligned simultaneously.

These are structural effects. They shape balance sheets, interoperability, systemic coherence, and regulatory confidence.

Governed offline proceeds from a different premise. Liquidity remains anchored. Exposure is bounded. Ledger authority remains central.

Resilience does not require redistributing authority under stress. It requires continuity. When institutional incentives align and governance continuity is preserved, offline capability ceases to function as a contingency mechanism. It becomes an integrated resilience layer within the architecture of digital money. When offline capability preserves liquidity anchoring, bounded exposure and central settlement authority, resilience becomes an architectural property of digital money rather than an operational contingency.

Governed offline preserves the governance of digital money.

Comparative Architectural Analysis of Offline Models

Offline capability is often discussed functionally. Architecturally, however, different models redistribute authority, exposure, and liquidity in materially different ways. This appendix compares the three principal offline architectures: Immediate, Deferred, and Governed. It uses the BIG Analytical Framework, which provides an structured lens to assess how Bankable, Implementable, and Governed an offline architecture is. The objective is not to assess technical sophistication; rather, it is to examine the institutional consequences.

Structural Comparison of Offline Payment Architectures Across Institutional BIG Dimensions

Offline Architecture	Immediate Offline Model	Deferred Offline Model	Governed Offline Model
Liquidity Anchoring	Relocates to devices	Within regulated institutions	Within regulated institutions
Exposure	Device-level systemic risk	Unmanaged credit exposure	Predefined and bounded
Interoperability	Hardware- and token-dependent	Scheme-dependent	Structurally interoperable
Vendor Neutrality	High risk of vendor lock-in	Scheme-bounded vendor-neutral	Structurally vendor-neutral
Monetary Integrity	Parallel monetary form	Credit exposure distortion	Preserved as digital money
Privacy	Governance tension at scale	Partial; scheme-bounded	Configurable; institutionally aligned

Table 3: *Comparative assessment of Immediate, Deferred and Governed offline architectures across the BIG Analytical Framework dimensions: Bankable, Implementable and Governed.*

Immediate Offline Architecture

Immediate offline seeks to replicate physical cash digitally. Value is stored or transferred at device level using hardware-dependent or token-dependent logic. Settlement is asserted locally at the moment of transfer.

Bankable

Immediate offline relocates liquidity to devices during offline operation.

Although balances originate from regulated institutions, monetary representation resides at device level until reconciliation. Deposit symmetry is therefore partially externalised. Liquidity anchoring weakens structurally because value temporarily exists outside institutional balance sheets.

Implementable

Immediate offline inherently satisfies the sufficiency condition because value is transferred directly.

However, authorised intent becomes inseparable from hardware or token logic. Interoperability therefore becomes hardware and token-dependent. Payment systems must recognise or embed device-specific logic. Vendor neutrality is constrained. Cross-system interoperability becomes limited by hardware architecture.

Governed

Immediate offline introduces a parallel monetary form at device-level.

Monetary integrity becomes partially coupled to user hardware. Systemic risk therefore extends to the device-level. Governance continuity is diluted because authority is temporarily asserted locally. Privacy can appear strong in immediate models by analogy to cash. However, at institutional scale the operational need for dispute handling, fraud controls, and AML/CFT alignment often introduces central reconciliation and monitoring functions. In CBDC contexts, where the state may be the system operator, perceived privacy can become a central concern. For these reasons, privacy is complicated in immediate offline architectures at scale.

Immediate offline relocates liquidity and asserts finality locally.

Deferred Offline Architecture

Deferred offline seeks to replicate cheque-style authorisation. Transactions are accepted offline and validated later once connectivity is restored.

Bankable

Deferred offline does not relocate liquidity to devices. However, sufficiency of funds is not secured in advance.

Temporary unmanaged exposure accumulates until reconciliation. Funding predictability becomes conditional. Liquidity remains institutionally anchored, but exposure fluctuates during disruption. This reservation mechanism ensures that sufficiency of funds is secured in advance rather than verified after the transaction or transferred to devices.

Implementable

Deferred offline satisfies the authorised intent condition. Vendor neutrality can be achieved within established scheme standards such as EMVCo. However, interoperability remains scheme-bounded and dependent on scheme-defined exposure tolerance.

Sufficiency of funds is verified post-connectivity. Interoperability therefore depends on scheme-defined exposure tolerance rather than structural assurance. Models such as “pay by identity” inherit this deferred exposure logic. Implementation scales within scheme boundaries rather than structurally across systems.

Governed

Deferred offline introduces a parallel monetary form in the form of temporary unmanaged credit exposure.

Although ledger authority remains central, exposure expands during disruption. Supervisory oversight must accommodate fluctuating exposure levels. Governance continuity becomes conditional on reconciliation boundaries rather than structurally across systems. Deferred models typically protect customer privacy at acceptance using tokenisation and related scheme mechanisms. However, settlement requires the token to be resolved so the remitting bank can debit the customer’s account. Privacy is therefore bounded. It can reduce merchant-level exposure, but it does not remove institutional visibility required for settlement.

Deferred offline preserves authority but accumulates temporary exposure.

Governed Offline Architecture

Governed offline is structured as a reservation-based Layer-2 capability operating above the underlying payment system. Offline capacity is derived from centrally reserved balances. Execution may occur locally. Authority and final settlement remain within Layer-1.

Bankable

Offline capacity is reserved from existing balances. Reserved liquidity remains anchored within regulated institutions.

Aggregate reservations change only through deliberate reserve or release operations. Settlement redistributes value but does not expand or contract the reservation pool. Liquidity therefore remains structurally predictable. Funding efficiency is preserved.

Implementable

Governed offline satisfies both interoperability conditions:

1. Authorised intent is cryptographically verifiable.
2. Sufficiency of funds is secured in advance through reservations.

Both are enforced locally within a secure runtime environment governed by strict business logic, while central authority remains intact. Vendor neutrality becomes structural at the system interface because acceptance validates standardised instructions rather than proprietary wallet logic. Cross-service and cross-system interoperability remain possible. Governed offline is the only architecture that satisfies both conditions simultaneously.

Governed

Governed offline does not introduce a new monetary form. It is governed as digital money.

Offline capacity represents centrally reserved digital balances. Exposure is predefined and bounded. Authority remains central throughout the lifecycle. Supervisory continuity is preserved. Governed offline enables privacy as a configurable design choice. A remitting bank can settle by proxy for its customer, protecting customer-level payment details from broad ecosystem exposure while retaining full visibility inside the remitting bank for AML/CFT and customer protection. The same privacy approach can be used online and offline, reducing asymmetry and strengthening institutional trust.

Governed offline preserves governance of digital money.

Institutional Engagement and Regulatory Context

Governed offline architecture has been examined within regulated and institutional environments. The examples below reflect publicly communicated regulatory processes, sandbox completion, and structured evaluation contexts in which the reservation-based model has been assessed.These references do not constitute endorsements. They reflect regulatory examination and institutional evaluation.

Reserve Bank of India - Regulatory Sandbox (2023) [3, 4]

In December 2023, Crunchfish in partnership with HDFC Bank and IDFC First Bank completed the Reserve Bank of India's Regulatory Sandbox test phase for offline retail payments and exited the sandbox. Following completion, the product may be considered for adoption by regulated entities, subject to applicable regulatory requirements.

This demonstrates that the centrally governed reservation mechanism has been evaluated within a central bank supervisory framework and can operate within existing governance structures while preserving central ledger authority and defined exposure limits. India represents a large-scale payments environment where resilience requirements are material. Completion of the sandbox test phase confirms practical feasibility within a central bank context.

European Central Bank - Digital Euro Innovation Platform (2025) [5]

Governed offline architecture has been examined within the context of the Eurosystem digital euro innovation platform. The Eurosystem context represents a highly rule-based supervisory environment, reinforcing the importance of institutional coherence.

3. https://www.crunchfish.com/wp-content/uploads/2023/12/RBI-RS-Press-Release-Completion-of-Test-Phase.pdf
4. https://www.crunchfish.com/reserve-bank-of-india-approves-crunchfish-digital-cash-for-offline-retail-payments/
5. https://www.crunchfish.com/crunchfish-pioneers-offline-payments-with-online-settlement-in-ecb-innovation-platform/

Bank of England - Digital Pound Lab (2026) [6]

Governed offline architecture has been evaluated within the Bank of England's Digital Pound Lab. The lab provides structured evaluation of technical and governance implications associated with CBDC design. Assessment has centred on preserving central authority, bounding exposure, and avoiding fragmentation of digital monetary form.

Institutional Evaluation by the BIG Analytical Framework

Across jurisdictions, institutional evaluation increasingly centres on three structural questions:

Bankable	Does liquidity remain anchored within regulated institutions, with funding- and implementation cost- efficiency?
Implementable	Does architecture scale without hardware, scheme, or vendor lock-in, and is it interoperable cross-services, -systems, and -borders?
Governed	Does central ledger authority remain intact with bounded exposure and preserve privacy?

Governed offline is designed to answer all these structural questions affirmatively.

6. https://www.crunchfish.com/crunchfish-selected-to-participate-in-the-digital-pound-lab/

Peer Reviews

Jeremy Light

- **Former Managing Director (Payments) at Accenture**
- **Board Member, PAPSS**
- **Fintech co-founder**

"Payment system operators need to treat offline payments strategically - with digital payment volumes expanding rapidly, offline payments can no longer be treated as optional or as a tactical backstop. It is impractical and unrealistic to assume 100% connectivity and 100% uptime of payment systems, yet consumers and businesses expect and need 100% availability to make and receive payments digitally, on demand, at any time.

Offline payment capability is indispensable for any payment system wanting to remain relevant and grow in the digital economy. Now is the time for payment system operators to address it. How offline payments are implemented is an important consideration for payment system strategies. Implemented properly, users will adopt them and costs and liquidity will be managed efficiently; whereas the wrong architecture, with a poor user experience risks an expensive flop.

This paper is an essential aid to guide strategic thinking on the practicalities and architectures for integrating offline payments into online payment systems to create always-available payment propositions. Payment system operators should take heed."

Gopalaraman Padmanabhan

- **Former Executive Director, Reserve Bank of India**
- **Former Chairman, Bank of India**
- **Board Member, Axis Bank**

"As payments become increasingly digital, one challenge that faces authorities particularly in large countries is how retail payments can remain operational during connectivity interruptions or lack of connectivity. Every government is keen to drive inclusive digital payments facilitation as digitisation ensures robustness, controls leakages and enables monitoring.

While many fintechs have scrambled to offer solutions for offline payments as a contingency feature, Crunchfish brings fresh thinking by treating offline payments as an architectural design choice. They offer the BIG Analytical Framework as a solution to the problem of keeping digital payments operational during network interruptions or lack of coverage.

Their engagements with the Reserve Bank of India, European Central Bank and Bank of England have helped to design a robust offline payment architecture that retains system integrity without distorting funding structures, fragmenting interoperability or altering governance of digital money. The three elements of the BIG Analytical Framework reinforce each other to maintain institutional coherence.

To authorities, any innovation must preserve institutional continuity and be mindful of systemic consequences. The BIG Analytical Framework attempts to build this focus into the model.

I shall be watching with interest the adoption and success of this model across various countries. I wish Joachim and his team all success."

Ram Rastogi

- **Former Head of Product, NPCI (UPI, IMPS, AePS)**
- **Chairman, Governance Council at Fintech Association for Consumer Empowerment**
- **Digital Payments Strategist & Career Banker**

"Crunchfish AB's executive whitepaper presents a principled examination of offline payments as a structural property of digital money rather than a contingency feature. Avoiding promotional framing, the paper advances a central thesis: architecture determines institutional outcomes. Offline capability, therefore, must be evaluated not as a technical add-on, but as a design choice with systemic implications for liquidity management, exposure containment, and governance integrity.

The paper contrasts two legacy offline paradigms. The immediate model delivers transaction finality during connectivity outages but introduces exposure risks when value is effectively held at the device level. The deferred model, by contrast, mitigates such exposure through centralized control, yet relies on post-event reconciliation, creating settlement uncertainty and operational complexity at scale. Each model resolves one risk vector while amplifying another; neither independently satisfies the requirements of institutional-grade digital money.

The proposed governed hybrid model structurally integrates elements of both legacy models. Offline transactions are treated as digitally bounded claims that remain institutionally anchored, with exposure predefined and reconciliation structurally embedded rather than improvised. In this formulation, resilience is not procedural but architectural. Digital money continues to function coherently even when the payment system is temporarily unavailable.

The whitepaper's primary contribution lies in reframing offline payments as a governance and monetary design question rather than a connectivity problem. This perspective is especially salient as retail payment infrastructures increasingly resemble public utilities and as central bank digital currency (CBDC) discussions foreground offline capability as a policy requirement. By focusing on structural consequences rather than technical novelty, the paper challenges designers and policymakers to evaluate offline models against institutional integrity criteria."

Jens Seidl

- **Chair & CEO, Currency Research**

"Offline digital payment solutions have been widely discussed in the last few years, typically in the context of retail Central Bank Digital Currencies. What makes this Whitepaper different, timely and relevant is that, despite the title "Enabling Offline Payments at Scale as Digital Money" the paper is not delving into technical specifications but is taking a strategic, high-level view of how to design any digital payment solution, not just for CBDCs but for any digital payment solution. So, while this paper does not provide a "turnkey" solution, it informs an important discussion about an underlying framework enabling offline payments versus an overlay on existing systems."

Lars Sjögren

- **Former COO, Danske Bank and CEO, P27**
- **Board member at banks, payments infrastructures and fintechs across Europe and APAC**
- **Senior Advisor, McKinsey**

"As payments infrastructure evolves, the question is no longer just who can move money faster. More and more, the real test is whether payments can become both smarter and more resilient at the same time.

That is what makes Crunchfish's whitepaper relevant. It does not look at offline payments as a side feature or just a technical add-on. Instead, it treats offline capability as a broader architecture and governance issue: how digital money can continue to work under stress without weakening institutional coherence, liquidity anchoring or supervisory continuity.

That is a useful contribution. In 2026, payments leaders are dealing with a lot at once: new rails, new regulation, AI, stablecoins, geopolitical fragmentation and growing expectations around resilience. The strength of this paper is that it cuts through some of that noise and focuses on something more basic. If payments are becoming more programmable, more data-rich and more decision-oriented, they also need to be able to keep working when systems are under pressure.

The BIG Analytical Framework is helpful because it brings some focus to the discussion. Bankable, Implementable and Governed is a practical way to test whether an offline model can work not just in theory, but in real institutions and at scale. In that sense, this whitepaper is a valuable contribution to an increasingly important debate. I wish Joachim and the team the best of luck."


crunchfish
RETHINKING PAYMENTS