Enabling offline payments in an online world

Interoperability

Researched and written by

LIPIS ADVISORS

Sponsored by

crunchfish

CONNECT AND PAY. ALWAYS.

About Lipis Advisors

Lipis Advisors is a leading strategy consultancy specializing in the payment sector. Lipis Advisors staff are experts on payment systems, services, and strategy, as well as the underlying technologies that support payment infrastructures. Lipis Advisors advises on all forms of payments, including ACH payments, real-time payments, card payments, cheques, mobile payments, online payments, and RTGS/wire payments.

To learn more about Lipis Advisors, please visit **www.lipisadvisors.com**

About Crunchfish

Crunchfish is a deep tech company developing a Digital Cash platform for Banks, Payment Services and CBDC implementations and Gesture Interaction technology for AR/VR and automotive industry. Crunchfish are listed on Nasdaq First North Growth Market since 2016, with headquarters in Malmö, Sweden and with a subsidiary in India.

To learn more about Crunchfish, please visit **www.crunchfish.com**

Authors

Bonni Brodsky is a managing consultant at Lipis Advisors.

Anurag Dubey is a consultant at Lipis Advisors.

David Tercero Lucas is a consultant at Lipis Advisors.

We greatly appreciate the contributions from Crunchfish CEO Joachim Samuelsson, CTO Paul Cronholm and CPO Magnus Lageson.


crunchfish
CONNECT AND PAY.
ALWAYS.
Crunchfish have the bold ambition
to take a global leadership position
within payments technology.

Table of Contents

Introduction 5

Interoperability considerations for online systems 6

- Closed- vs. open-loop systems 6
- Interoperability across closed- and open-loop systems 7

Design choices to facilitate offline interoperability 8

- Design choices for the offline security protocol 8
- Hardware- vs. software-based trusted environments 10
- Other use cases for offline interoperability 11

Innovative ways of enabling interoperability in India 11

- What has been achieved in India already? 11
- What is next for interoperability in India? 12

Conclusion 13

Enabling offline payments in an online world

Interoperability

INTRODUCTION

Interoperability is a key design feature of the most successful payment systems today. It expands the reach of electronic payments to a wider user base by reducing the risks of market fragmentation. It drives competition and innovation by freeing up resources previously dedicated to managing the complexities of connecting to multiple payment systems. Furthermore, it promotes a more inclusive ecosystem with fewer barriers to entry.

Real-time payment systems such as Pix in Brazil, Swish in Sweden, and UPI in India have seen widespread adoption and success due to their innovative approaches to enabling interoperability. For example, Swish allows users to connect their bank accounts with the Swish platform enabling seamless transfers between different banks and financial institutions. With UPI and Pix, users can instantly and seamlessly send payments across the ecosystem, regardless of which bank and/or third-party provider they choose. In these markets, there have been concerted regulator- and/or industry-led efforts to make this possible, through strategies such as the standardization of messaging, APIs, and QR codes, etc. along with common scheme rules governing aspects such as service levels and dispute management.

In the above examples, both the sender and receiver must be online for the transaction to be successful. In this paper, we consider the key design questions that must be weighed to maximize interoperability in an offline context. First, we analyze the different ways of considering the interoperability of online systems. Second, we introduce new frameworks for understanding interoperability between online and offline systems. Third, we consider how offline systems can be best designed to maximize interoperability from the outset. Finally, we describe recent and future innovations related to payment interoperability in India, a global innovator in this area.

INTEROPERABILITY CONSIDERATIONS FOR ONLINE SYSTEMS

In this section, we describe the conventional ways of thinking about payment system interoperability for online systems. Specifically, we cover the mechanics of closed vs. open-loop systems and how interoperability across these types of systems is typically achieved.

CLOSED- VS. OPEN-LOOP SYSTEMS

Closed-loop payment systems are designed to facilitate transactions within a specific network or ecosystem. These systems often involve a dedicated payment instrument, such as a prepaid card or mobile app, which is issued by the network or a participating merchant. The payment instrument typically has a stored value that can be used for purchases within the network. Some examples of closed-loop systems include pre-paid instruments or proprietary wallets. Closed-loop systems lack interoperability and can only process payments within their network primarily due to the closed nature of their proprietary settlement structure.

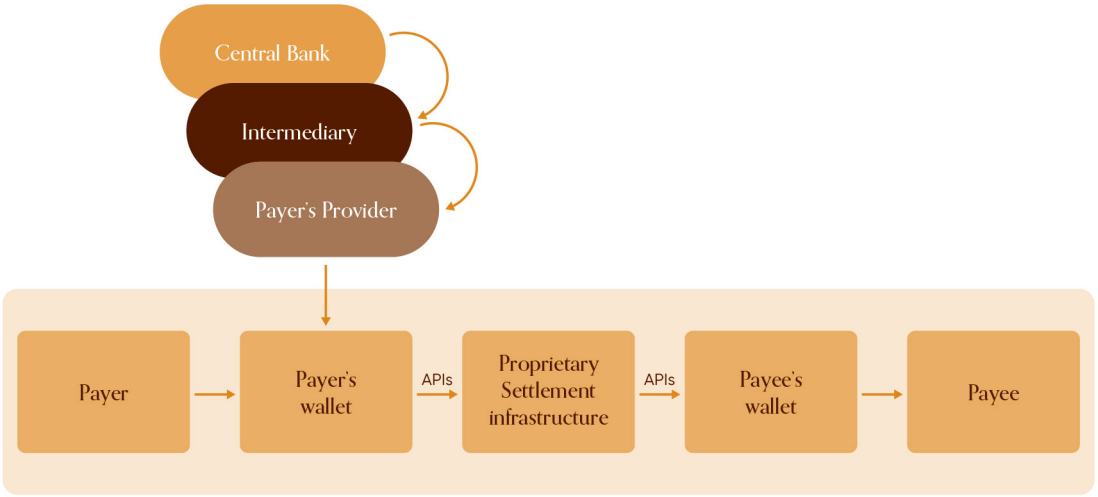

Figure 1 Closed-loop systems

Source: Author's elaboration

In contrast, open-loop systems enable competing networks, services, or platforms to interact with one another at the same level of the value chain. This type of "horizontal" interoperability has enabled wide scale adoption of real-time payment systems and services.[1] The convenience and reach of such systems ensure that the payer does not have to maintain multiple payment wallets and can pay irrespective of the payees preferred store of value (wallet). Using open-loop systems, users can make transactions across multiple platforms without the need for separate accounts or redundant registration processes. This seamless connectivity streamlines the payment experience, allowing customers to make purchases effortlessly and businesses to receive payments promptly.

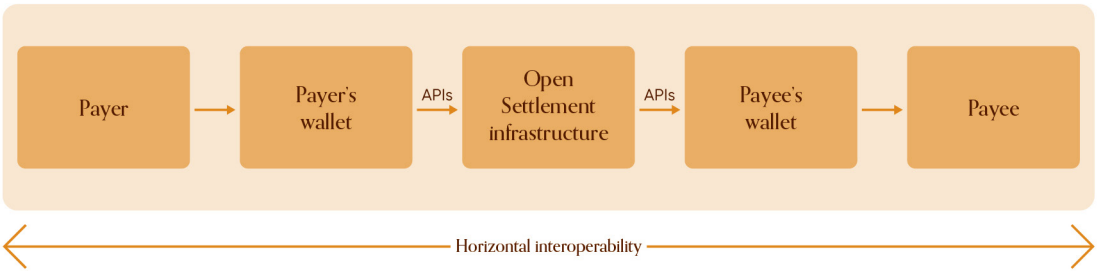

Figure 2 Horizontal interoperability through open-loop systems

Source: Author's elaboration

[1] https://www.jipitec.eu/issues/jipitec-8-1-2017/4531

INTEROPERABILITY ACROSS CLOSED- AND OPEN-LOOP SYSTEMS

Achieving interoperability across different types of systems requires seamless communication and exchange of information at different levels of the value chain. This type of "vertical" interoperability can occur between a closed-loop system such as a pre-paid instrument and an open-loop system as well as between multiple open-loop systems.[2] It has the benefit of further enhancing competition, innovation to offer new services riding on the near ubiquitous acceptance of their payments. For example, Pre-paid Payment Instruments (PPI) on UPI allows for interoperability between an online third-party account-based wallets with UPI.[3, 4] In this case, the user loads value on one PPI wallet, which can be used for transactions across the UPI acceptance network in India, which enables full KYC PPIs issued in the form of wallets to interoperate across PPIs through UPI. Standardization of messaging standards and APIs along with common rules have typically been the factors that have driven this type of "vertical" interoperability.

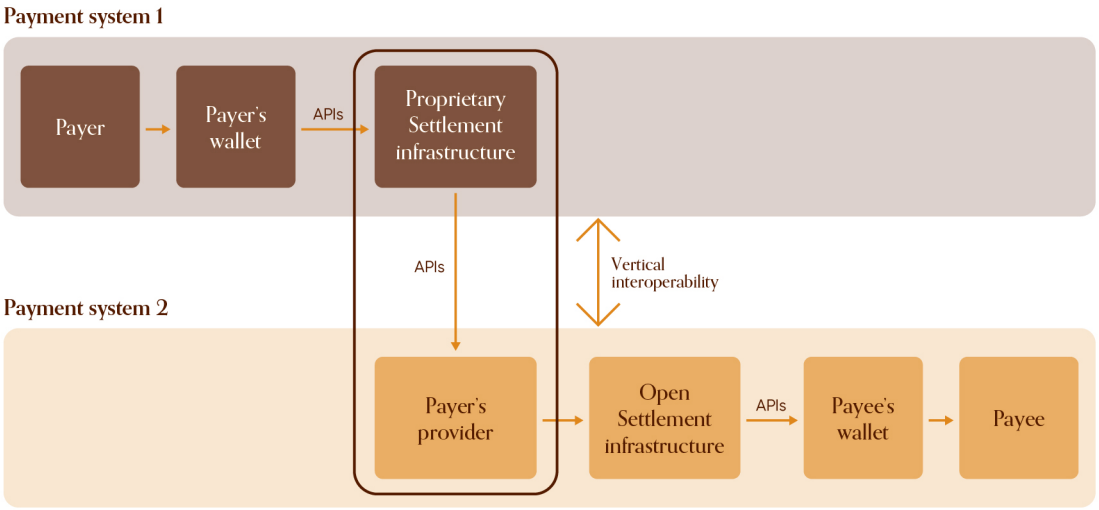

Figure 3 Vertical interoperability across closed- and open-loop systems

Source: Author's elaboration

Interoperability across different open-loop systems can be considered from both a domestic and cross-border context. From the cross-border perspective, there are generally two different models for enabling interoperability. The first is to create bilateral linkages between different systems. Singapore has been a global innovator in this regard, having facilitated bilateral connections between its real-time service PayNow and other similar services in markets such as Malaysia, Thailand, India, and others.[5, 6, 7] A second approach is to develop a single, common technical infrastructure that operates across borders. For example, multi-CBDC arrangements that connect jurisdictional CBDCs in a single, common technical infrastructure offer significant potential to improve the current system by enabling cross-border payments to be immediate, cheap, and universally accessible with secure settlement.[8] Both approaches require agreement upon common technical and messaging standards, as well as a harmonization of different countries' regulatory and legal frameworks.

[2] Ibid.

[3] Prepaid Payment Instruments (PPIs), refer to certain payment instruments that facilitate purchase of goods and services against the value stored in them. The value stored in such instruments represents the money paid for it by its holder either by physical or digital means. There can be different variants of prepaid instruments ranging from smart cards, magnetic strip cards, mobile wallets or even a simple paper voucher.

[4] https://www.caluniv.ac.in/dj/BS-Journal/vol-38/Prepaid-Payment.pdf

[5] https://www.bancaditalia.it/media/agenda/convegni-2021/Cross-border_Lau.pdf?language_id=1

[6] empsa.org

[7] https://www.europeanpaymentscouncil.eu/what-we-do/other-sepa-payments/sepa-goes-mobile/ad-hoc-multi-stake-holder-group-mobile-initiated

[8] https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

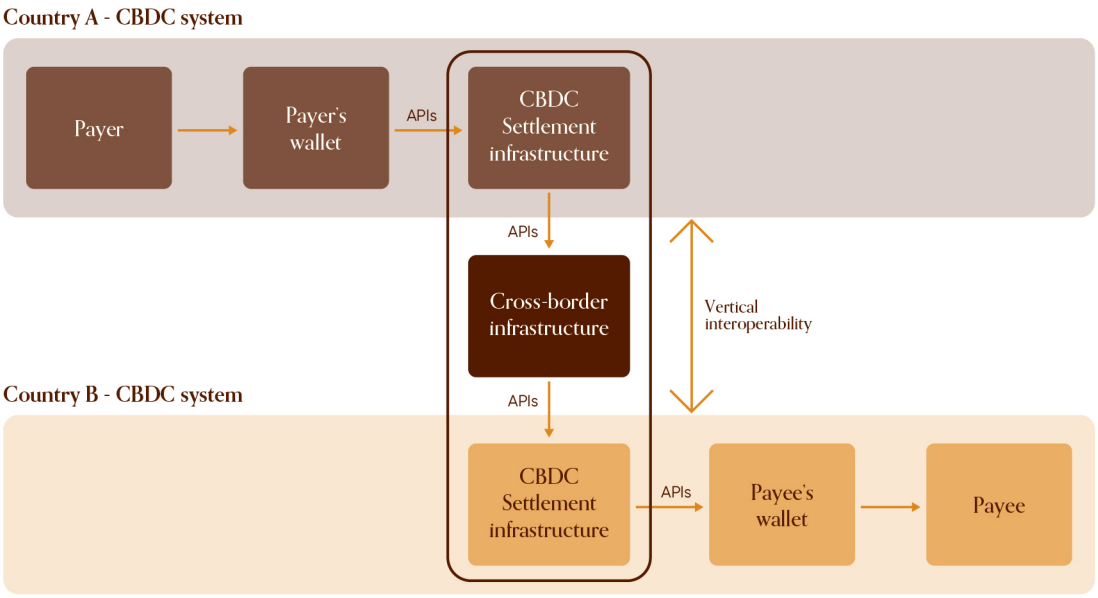

Figure 4 Cross-border interoperability between open-loop systems based on a common infrastructure

Source: Author's elaboration

DESIGN CHOICES TO FACILITATE OFFLINE INTEROPERABILITY

In our previous white papers, we discussed the different models under which offline payment systems can be designed.[9, 10, 11] In some models of offline payments, both the payer and payee can be offline, and in other models, only one can be offline for the transaction to be successful. In other models where an intermediary is required to settle the transaction, the offline element need not only be on the side of the payer/payee, but also on the side of the remitting bank, infrastructure, or other third-parties. Payment system operators should choose implementation approaches that best suit targeted use cases and the local market context in which they operate.

Increased payment system resilience, access, and financial inclusion may be achieved through a mix of online and offline parties and systems that enable users to successfully make a payment regardless of whether they are connected to the internet. In these instances, online-offline payment system interoperability is required to enable effective communication between online payment schemes and offline payment schemes and to facilitate the secure exchange of information. This can be a complex task, but the right design choices can help facilitate this type of interoperability with greater ease. In this next section, we lay out how the choice of offline security protocol (native layer-1 vs. non-native layer-2 along with encryption vs. signatures) and the choice of offline trusted environment (hardware vs. software-based) can impact interoperability.

DESIGN CHOICES FOR THE OFFLINE SECURITY PROTOCOL

As discussed in our previous white papers, layer-1 offline payment systems use the same native security protocol as the online scheme, while layer-2 solutions use a non-native protocol. Whereas both design options can provide online-offline interoperability for a specific payment rail, offline interoperability between different payment rails could be a challenge for layer-1 schemes as separate online payment systems often have separate security protocols. To become interoperable, the payment schemes, need to share common roots, agree on setting rules, and establish

[9] https://www.crunchfish.com/wp-content/uploads/2023/01/Lipisadvisors_WP1_offlinepayments.pdf
[10] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP2_Crunchfish_Enabling-offline-payments_v5.pdf
[11] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP3_Crunchfish_Enabling-offline-payments_FINAL.pdf

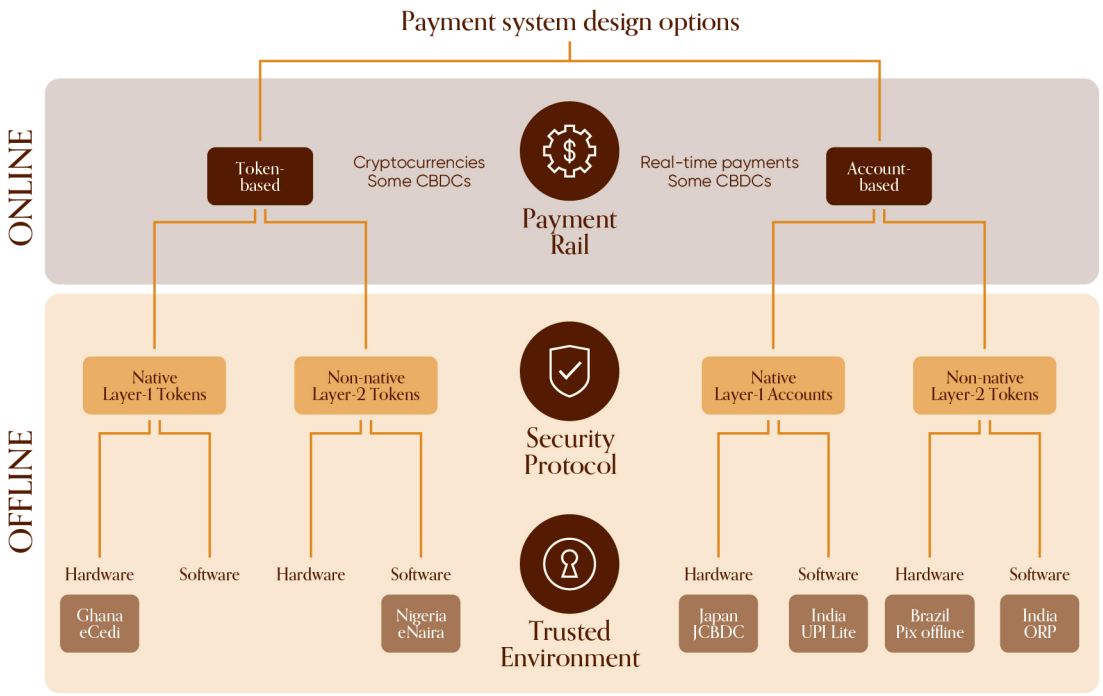

Figure 5 Payment system design options

Source: Author's elaboration

trust in between them to accept each other's layer-1 offering. A non-native, layer-2 solution, on the other hand, may be used as an offline bridge making several online payment rails interoperable offline. This may also be applied in a cross-border context with interoperable offline wallets originating from different countries having different currencies handling foreign exchange offline.[12]

In the second white paper we also introduced two additional design options for offline payments: scheme interoperability being proprietary or open and the security of the application layer being based on encryption or signatures. These design choices can also directly impact offline interoperability.

Figure 6 Offline security protocol design options

Source: Author's elaboration

To trust offline payments from payer's wallets, the offline payment platform must either be a proprietary system where values are trusted as they are transferred between closed-loop payment applications executing in tamper-resistant elements (TRE) or alternatively be open and typically rely on Public Key Infrastructure (PKI). Whereas signatures are designed to be interoperable, application layer encryption tends to limit interoperability. This is also evident

[12] https://www.crunchfish.com/crunchfish-receives-clean-iprp-for-key-digital-cash-patent-application/

in many offline payment systems where an offline payment can only be verified by the payee, whereas in signature-based systems, anyone with access to the CA root certificate can verify the transaction.

This implies that by using PKI and sender signatures, only the sender wallet needs to be secured by a TRE. By verifying the sender signature using the CA root certificate receivers or any node may trust the sender and accept the value transfer. Looking at the different approaches in the market, on the one hand, trust can be established for offline payments with central banks acting as certificate authority (CA) by signing certificates with wallets' public keys.[13] Alternatively, offline payments can act as a bridge between vertically interoperable payment schemes when the sender wallets are authenticated by the same CA. This has the potential to enable interoperability between CBDC wallets and existing payment services or to support cross-border payments with other CBDCs, even in offline mode.[14]

HARDWARE- VS. SOFTWARE-BASED TRUSTED ENVIRONMENTS

It is imperative that the payer's offline wallet is executing the payment in a trusted and tamper resistant environment to protect cryptographic keys and sensitive data such as offline balances or transaction data. To provide online-offline interoperability the trusted environment could either be implemented in hardware or software.[15] In this context, it is important for software-based solutions and hardware-based solutions to communicate seamlessly with each other; this maximizes inclusion for users and scalability for system operators by expanding the ubiquity and reach of the system.

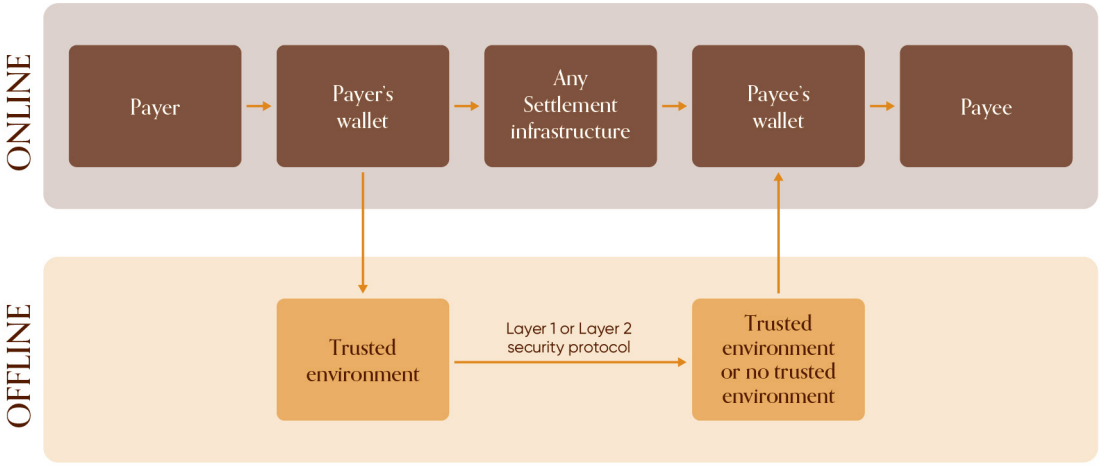

Figure 7 Interoperable offline proximity payments

Source: Author's elaboration

Moreover, to fulfill the financial inclusion goals related to offline payments, it is imperative to enable interoperability between different offline wallet form factors such as cards, smart phones, and feature phones, issued by either the same or different wallet providers. Offline form factor interoperability enables end-users to make offline payments without having to consider differences between form factors or providers. This allows for a more inclusive design and maximizes user choice. An example of form factor interoperability could include a debit can be done in offline mode in a software-based trusted environment and a credit in a hardware-based trusted environment on another form factor and vice versa.[16]

Another important consideration for interoperable offline payment systems is the dynamic nature of such systems and the need to regularly upgrade them. For example, the payer´s offline

[13] https://arxiv.org/pdf/2012.08003.pdf
[14] https://www.crunchfish.com/crunchfish-receive-clean-iprp-for-another-key-digital-cash-patent-application/
[15] https://www.bis.org/publ/othp64.pdf
[16] https://www.crunchfish.com/crunchfish-digital-cash-non-mobile-devices-webinar/

wallet can be configured to consider whether the payee can accept a payment. This relies on the fact that the payee's payment system can trust the payment from an interoperable payment system and with a version that the payee's system is able to verify. This requires that the payer's offline wallet is easily upgradable. This is likely more feasible in a software-based trusted environment, rather than in hardware.

OTHER USE CASES FOR OFFLINE INTEROPERABILITY

Offline payments are not limited to just proximity payments but can also refer to payments in which the payer connects using a SMS or USSD over the telecom network in cases where there is no internet connection available. In the latter case, the payer does not have to worry about whether they can connect to the internet. This use case is very interoperable with online payment rails as no changes are required to credit the payees. This use case requires a tamper resistant environment on a mobile phone, which could be software-based on a smartphone and hardware-based on a feature phone.[17] The offline balance may be used both for offline push payments as well as offline proximity payments.

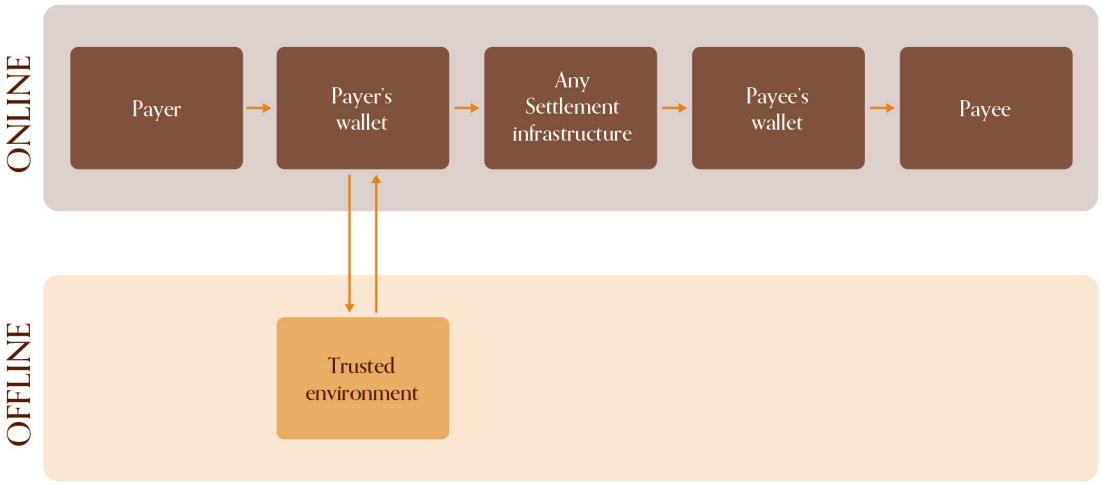

Figure 8 Interoperable online-offline push payments

Source: Author's elaboration

INNOVATIVE WAYS OF ENABLING INTEROPERABILITY IN INDIA

India leads the world when it comes to designing interoperable payment systems. Its payment industry has demonstrated that with smart design choices and strong collaboration, interoperable payments at scale are not only achievable but can also drive growth in digital payments and improve financial inclusion.

WHAT HAS BEEN ACHIEVED IN INDIA ALREADY?

UPI: horizontal online interoperability

Unified payments interface (UPI), operated by NPCI in India, is an alias based low-value open loop instant payment system. UPI is a great example of horizontal interoperability in online-online mode, allowing seamless fund transfer across banks when both the payer and payee are online and connected to the network. UPI operates as an overlayer layer using the IMPS rails. This overlayer layer allows for payment

[17] https://www.crunchfish.com/crunchfish-digital-cash-2-1-trusted-payments-over-telecom-10/

initiation through not only banking apps but also third-party apps, facilitating a seamless user experience where individuals can send money to each other across banks and across TPAPs by using a single, two-click authentication process.

UPI 123 and UPI Lite: Horizontal offline-online interoperability

Owing to the ease of use, widescale adoption, and interoperability provided by UPI, it has now become one of the preferred modes of payments in India. However, both the payer and payee need to be online for the payment to be processed, which has hindered growth in areas that do not have stable internet connectivity or where a majority of users users do not own smartphones. To solve for connectivity issues in making UPI payments, NPCI came out with two solutions: UPI123 Pay and UPI Lite. UPI123 Pay is a solution based on the UPI technology made available feature phones. UPI23 Pay is an interoperable service that relies on telecom connectivity instead of internet connectivity, allowing the user to make UPI payment even in an offline mode by connecting to the telecom network. UPI123 allows for payment initiation via IVR number, through missed call, through functionality implemented by OEM and through sound-based technology for proximity payments. UPI123 PAY uses Dual-Tone Multi-Frequency (DTMF) signaling technology with two-factor authentication for peer-to-peer transactions.[18, 19]

Another solution to foster online-offline horizontal interoperability in the UPI ecosystem is UPI Lite. UPI Lite is a solution that allows users to conduct transactions using an 'on-device' wallet instead of directly from a linked bank account. To use UPI Lite, users need to add money to the UPI Lite wallet in an online mode. However, to make a successful payment the remitting bank need not be online. Other than the remitting bank being offline, the rest of the payment process remains the same as the current UPI system. If the payer has online connectivity it increases the chances for a hassle-free payment experience.

PPI on UPI: vertical online interoperability

Apart from the horizontal interoperability in the payments ecosystem in India, NPCI recently allowed Pre-Paid Instruments (PPIs) to be part of the interoperable UPI ecosystem, thus paving the way for enhanced vertical interoperability amongst various closed loop systems with UPI. However, the RBI included significant changes to the KYC requirements for existing and new PPIs issued to the customers. It also provided for having a tiered approach to interoperability with only full KYC PPIs being interoperable with UPI; the small PPIs with limited KYC are not interoperable considering the high risk associated with lack of full KYC.[20] Vertical interoperability enables closed-loop wallet users to seamlessly transfer funds from one closed-loop wallet to another (of a different issuer) and from their closed-loop wallets to bank accounts through the platform. This is expected to increase the acceptance of non-bank PPI players.

WHAT IS NEXT FOR INTEROPERABILITY IN INDIA?

As the Indian payments market continues to evolve, a natural question is how India is and should further enhance the interoperability of its digital payment ecosystem. Below, we provide a summary of ongoing experimentation in new areas as well as suggested areas for future experimentation:

- *Enhancing UPI and UPI Lite through offline-offline interoperability.* NPCI has announced that it is planning to enhance offline interoperability for both UPI Lite and UPI in a second phase of its development. It plans to enable users to successfully make a payment with both the beneficiary and remitting bank being offline. This would further enhance the convenience and resilience of these systems.[21] Future exploration in this area could also focus on enabling payments when the entire value chain is offline.

- *Enabling online-offline interoperability for PPI on UPI.* With the success of PPI on UPI, a next

[18] https://www.wintwealth.com/blog/what-is-upi-123pay-how-to-use-it-and-how-is-it-different-from-the-current-upi-interface/#:~:text=UPI123%20Pay%20is%20an%20instant,payments%20without%20using%20the%20internet.

[19] https://trak.in/tags/business/2021/07/22/voice-based-payments-using-upi-without-using-internet-npcis-latest-innovation-for-feature-phones/

[20] https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156

[21] https://www.businesstoday.in/personal-finance/banking/story/rbi-introduces-upi-lite-for-faster-real-time-low-value-transactions-check-more-details-here-348070-2022-09-23

step is to explore enabling online-offline interoperability across these systems. This would enable users to make payments via offline PPI wallets on UPI, enhancing user convenience and access.

- *Solving interoperability challenges for a future eRupee.* As eRupee development advances, it will be important for the future CBDC to be interoperable with existing online and offline payment systems. Organizations such as the BIS and others have pointed to the importance of CBDC interoperability with existing payment systems in determining future adoption. This implies that both horizontal and vertical interoperability will need to be enabled.

Another important area for the eRupee will be enabling online-offline interoperability, given the RBI's view that offline use will be an important feature for the eRupee.[22] In this context, facilitating vertical interoperability between the eRupee and UPI will be important, and potential approaches for enabling online-offline vertical interoperability between payment systems are already being piloted in the RBI's regulatory sandbox.[23] Enabling offline push payments for the eRupee is already currently being explored by IDFC First Bank.[24, 25]

CONCLUSION

In this paper, we provided an analysis of the key considerations around payment system interoperability, with a focus on the offline space. We introduced the concept of online-offline interoperability and the benefits, and how choices related to the offline security protocol and trusted environment matter for ease of implementation, inclusivity, and reach. Moreover, we weighed how the choice of native layer-1 vs. non-native layer 2 offline security protocols, the use of encryption vs. signatures, as well as hardware vs. software-based trusted environments can impact the ease of interoperability between online and offline payment systems.

Ultimately, a payer in any market should be able to make payments without having to worry about connectivity, what provider they or the payee are using, or what device they choose to use. Much like for online payment systems, offline system interoperability is highly connected to its scalability and sustainability, which we will explore further in our next paper. In considering the various solutions and options in the market, it is important for payment system operators to think practically about what is needed from a technical, functional, and operational perspective. Not all markets have the same problems or needs, but they should equally make practical and efficient design choices that can best further their goals. ■

[22] https://www.cnbctv18.com/finance/cbdc-digital-rupee-looking-at-offline-functionality-of-central-bank-currency-rbi-executive-director-16090091.htm

[23] This approach was successfully piloted by HDFC and IDFC banks in the RBI's regulatory sandbox as part of the Offline Retail Payments project.

[24] https://www.idfcfirstbank.com/cbdc

[25] https://www.livemint.com/news/india/idfc-first-bank-join-hands-with-crunchfish-to-be-a-part-of-rbi-s-pilot-project-to-enable-offline-payments-11679910289261.html