Enabling offline payments in an online world

A practical guide to offline payment design

Researched and written by

LIPIS ADVISORS

Sponsored by

crunchfish
AUGMENTING PAYMENTS

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 are 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

AUGMENTING PAYMENTS

Crunchfish have the bold ambition to take a global leadership position within payment technology

Table of Contents

Enabling offline payments in an online world

A practical guide to offline payment design

INTRODUCTION

There have been numerous examples of how payments digitalization has transformed society in recent years, whether it be the surge in mobile money usage in sub-Saharan Africa[1], the stunning success of real-time payments in markets such as Brazil, India, and Thailand[2], or the increased adoption of contactless payment methods following the COVID-19 pandemic.[3] According to the World Bank, roughly two-thirds of the population now make and receive digital payments, with the share of adults in developing economies increasing from 35 percent in 2014 to 57 percent in 2021.[4] This shift has not only led to reduced cash usage and the availability of more convenient payment options but also to much needed improvements in financial inclusion and digital access for underserved populations.

As payments have increasingly gone digital, the dependency on internet connectivity for making payments has also risen. However, there still exist many areas of the world without consistent internet access, and even in markets with reliable connectivity, service outages still happen, often due to temporary congestion either in the uplink or at banking servers. As such, there has been increased interest on the part of central banks and payment system operators to enable digital payments in an offline setting. Indeed, offline use is likely to become a core feature of future retail central bank digital currencies (CBDCs), which seeks to emulate similar levels of availability and resiliency as cash. Many of the world's major central banks (e.g., Bank of England, European Central Bank, People's Bank of China) and those with live CBDCs (e.g., Bahamas, Nigeria) are already investigating how to enable offline CBDCs.[5] Moreover, offline capability has the potential to become a key aspect of real-time payment (RTP) systems as well, particularly in markets where cash usage is declining or has declined to the point where it is not a viable back-up in the event of a network outage. For example, RTP systems such as UPI in India (UPI "Lite"), Pix in Brazil and Swish in Sweden are or have investigated different ways of enabling offline transactions for when their systems are temporarily unavailable.[6 7 8]

1 https://www.communicationstoday.co.in/smartphone-adoption-doubled-between-2015-2020-in-sub-saharan-africa/
2 https://www.theasianbanker.com/updates-and-articles/real-time-retail-payment-systems-in-thailand-and-india-experience-rapid-growth
3 https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments
4 Ibid.
5 https://www.bis.org/publ/othp33.pdf, p. 10-11
6 https://www.bhimupi.org.in/content/upi-lite
7 https://www.europeanpaymentscouncil.eu/news-insights/insight/pix-rapid-development-instant-payments-brazil
8 https://www.crunchfish.com/crunchfish-and-swish-continue-to-plan-for-digital-cash/

But despite all the recent attention on the topic of offline payments, there still lacks a clear understanding in the market around the practical design choices and trade-offs for offline real-time payments and CBDCs. This white paper, the first in a series, aims to describe the imperative for and practical definitions of offline payments and provide an overview of the various design considerations for payment system operators. It will conclude by detailing ongoing innovation in this space, including real-world examples of offline payment implementation globally.

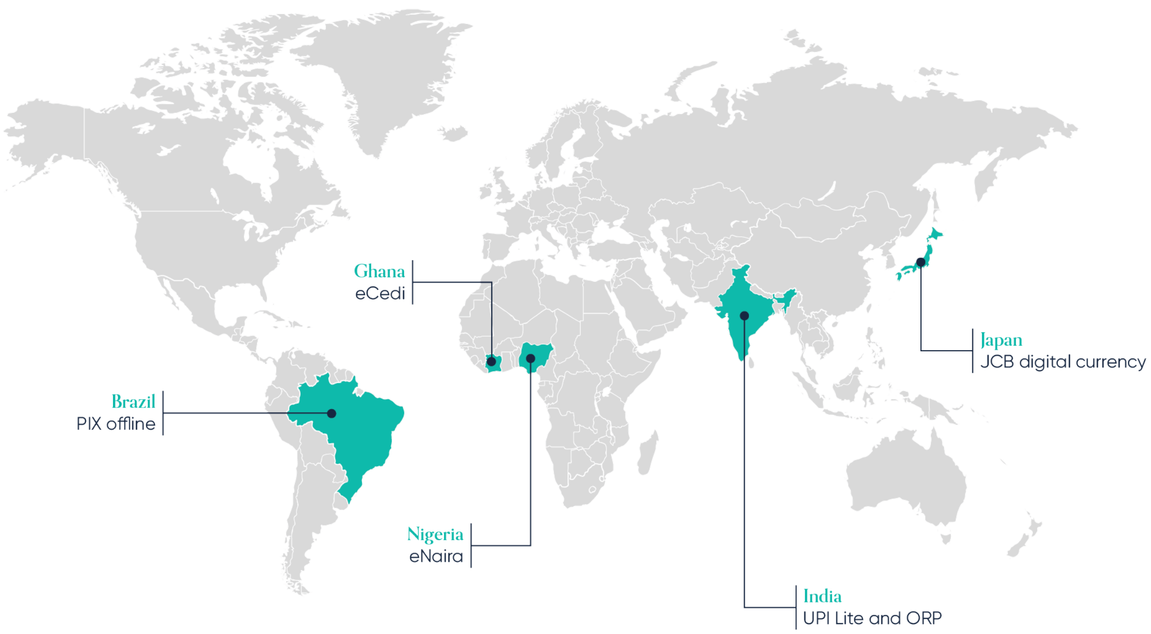

Figure 1 Selected real-time payment systems and CBDCs exploring offline capabilities Source: Author's elaboration

THE IMPERATIVE FOR OFFLINE PAYMENTS

There are many reasons for why payment system operators should be thinking about how to allow offline payments for real-time payment systems and future retail CBDCs. These include greater financial inclusion, improved payment system resilience, and higher levels of user convenience, trust, and privacy. These three aspects are explained in more detail below.

MEETING FINANCIAL INCLUSION GOALS

Limited or unreliable internet connectivity can be a major hurdle in the adoption of digital payments, with around 50% of people in low- and middle-income countries still lacking reliable internet access.[9] Many such populations have been effectively excluded from internet-based digital payments and banking. Offline payments have the potential to significantly accelerate the provision of digital financial services access for these populations. Along these lines, the role of offline payments in furthering financial inclusion in a CBDC context has also been widely discussed. For example, the BIS has previously noted that CBDCs must have features such as offline payment capabilities to address financial inclusion challenges in their implementation.[10]

IMPROVED PAYMENT SYSTEM RESILIENCE

Apart from providing digital financial access to people with limited network connectivity, offline payment capabilities can provide additional resiliency and availability for payment systems, particularly in the event of temporary or

[9] https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=XO-XT-XD&name_desc=false
[10] https://www.bis.org/fsi/publ/insights41.pdf

prolonged (e.g., natural disaster, cyberattacks) network outages. Similarly, offline payments can also be used to reduce the impact of the system shutdown due to power outage and cyberattack. There have been multiple recent examples of critical payment infrastructure becoming non-available due to operational failure. For example, in 2020, the Eurosystem's large-value payment system, TARGET2, suffered an operational failure for eight hours during which even the backup systems and contingency modules were unable to function.[11] More recently, in 2022 UPI servers were down causing mass complaints by users about failed payments on social media.[12] In the CBDC space, the East Caribbean Central Bank's DCash CBDC went offline for more than a month in early 2022, further underscoring the need for offline capabilities in this context.[13] In certain countries, such as Sweden, where successful alias based real-time system Swish has practically replaced cash and most day-to-day transactions are carried out digitally, cash as a contingency payment option is no longer viable.[14] Any disruption of the network services even for a small duration of time can cause mass disruptions in people's ability to make and receive payments.

INCREASED USER CONVENIENCE, PRIVACY, AND TRUST

In a world where offline digital payments are enabled, users do not need to worry about whether they have internet access or not to make or receive a payment. This capability would greatly enhance the digital payment experience from a convenience perspective. However, it also ensures greater user trust in the system, as a transaction will be processed even if the user is temporarily offline, or if a bank's network is momentarily congested or down. From this angle, the benefits of offline payments are not only limited to increased system resilience but also extend to increased usability and convenience for consumers, businesses, and merchants. Enhanced privacy for users could also be a benefit of some offline payment implementations where transactions are not revealed in real-time but after they have occurred.

DEVELOPING A PRACTICAL DEFINITION OF "OFFLINE"

Various use cases for offline payments are being tested worldwide by central banks, payment system operators, financial institutions, and tech providers. However, there is still a lack of understanding among such players regarding what models for offline payments exist as well as potential use cases.

DISSECTING THE MEANING OF "OFFLINE"

Offline payments have previously been understood as a transaction that is recorded offline and processed at a later point of time. However, defining what makes a payment offline is not as straightforward as it might seem. Some industry experts would define it as a transaction that occurs between users without an internet connection. Payments made using non-internet servers, such as telecom servers, would fall under the definition of "offline." Others counter that a transaction can only be considered offline if it occurs "without a connection to any external power source, non-internet server, or general ledger."[15] Under this definition, offline transactions typically occur using hardware-based instruments that typically exist on either stored-value cards or smart phones. The devices communicate with each other, either manually or by using near-field communication (NFC), without the need for reconciliation with the online ledger for settlement.

While experts might disagree about definitions, this is not highly relevant. Practically speaking, the characteristics of offline payment systems will vary depending on the operator's specific aims and requirements. Certain payment system operators may find that online connectivity after every transaction is adequate, while others may prefer

[11] https://www.finextra.com/newsarticle/36825/target2-experiences-total-system-failure-sepa-payments-delayed
[12] https://www.livemint.com/news/india/upi-server-down-complaints-flood-social-media-about-failed-payments-11650816808870.html
[13] https://www.bloomberg.com/news/articles/2022-02-21/eastern-caribbean-dcash-outage-is-test-for-central-bank-digital-currencies
[14] https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-report-2022/trends-on-the-payment-market/-in-sweden-we-prefer-to-pay-digitally/the-digitalisation-of-the-payments-market-is-a-global-trend/
[15] https://www.progressoft.com/blogs/between-a-rock-and-a-hard-place-offline-use-in-cbdcs

functionality that allows for consecutive offline payments after a limited number of transactions or value threshold. Similarly, in some models of offline payments, both the payer and payee can be in 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.

Who is offline?	• User (payer and/or payee) • Intermediary (banks, PSP) • System (infrastructure, directory, other ancillary systems such as digital identity systems etc.)
Type of connectivity	• Internet server • Non-internet server (e.g., telecom) • None
Frequency of connectivity	• Continuous • After each transaction • After a limited number of transactions/hitting a certain value threshold • None

Figure 2 Offline characteristics will vary by system type and by goals of payment system operator

Source: Author's elaboration

In determining the appropriate model for offline payments, central banks and payment system operators should consider their overarching goals as well as the use cases that they are trying to target. For example, in a CBDC context, enabling consecutive offline payments, in which the payer and payee exchange a transaction offline, and the payee can immediately spend the received funds in another offline transaction, may be the most desirable approach for CBDC given its resemblance to the properties of cash. This next section digs deeper into use cases for offline payments.

USES CASES FOR OFFLINE PAYMENTS

An offline transaction must be recorded in local ledgers on user devices and settlement is not final and irrevocable until subsequently reconciled with the online ledger. Hence, design choices for offline functionality are informed by the degree of asynchrony with the general ledger.[16] We describe the three main categories of use cases for offline payments below, which we define according to their relationship to the general ledger.

[16] https://www.progressoft.com/blogs/between-a-rock-and-a-hard-place-offline-use-in-cbdcs

Use case	Who is offline?	Type of non-internet connectivity	Connectivity frequency
Temporary outage	System, issuer or end-user	Telecom	Frequent
Out-of-range (no internet)	End-user	Telecom	Intermittent
Off-grid (full offline)	End-user	No connectivity	Limited or none

Figure 3 Analysis of offline use cases

Source: Author's elaboration

Temporary outages

In this case, a payment system can be made more resilient for temporary network outage or power interruptions, caused by a natural phenomenon or because of cyber-attack on the system. Payment data for limited transaction amounts and volume may be temporarily stored on devices for completion of the transaction when connectivity is re-established. One approach for such use cases is the wallet-based approach, whereby there is an upper limit on the individual transaction value as well as on the wallet balance, within this limit offline transactions are allowed. The wallet balance is allowed to be reloaded using on-line payment methods. The settlement shall take place when the temporary outage is resolved.

Out-of-range use (no internet connectivity)

The offline payments design for high-volume/-value transactions for longer spans of time with continuous unavailability of the network, requires more robust and efficient offline payment processing. The ability to authenticate the payment and reset the authentication through network-based authentication and reconciliation becomes necessary for long duration use. Telecom network can be used for re-authentication considering the widespread availability of telecom network even in remote areas.[17]

Off-grid use (full offline mode)

Off-grid use cases for offline payments arise from the need to have offline payments capacities for extended period of network non-availability. This would require tamper-proof storage and application to reduce the end user risk of settlement. These use cases would need to allow for a high number of transactions to occur offline over an extended period. Enabling these use cases involve much more complex onboarding and implementation in many instances, the need for common standards for interoperability of relevant hardware and software, and reconciliation when connection with the general ledger is re-established.[18]

ENABLING OFFLINE PAYMENTS

KEY DESIGN PRIORITIES FOR OFFLINE PAYMENTS

Regardless of the specific use cases for offline that are being targeted, or the specific offline model implemented, interoperability, scalability, and security should be key design areas for offline payment system design. Understanding why these areas is important for offline payment system design and implementation is described in further detail below.

[17] https://www.progressoft.com/blogs/between-a-rock-and-a-hard-place-offline-use-in-cbdcs
[18] Ibid.

Fostering ecosystem interoperability

Interoperability can be defined as the "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units."[19] Ecosystem interoperability for offline payments is an important aspect that will drive future usage and adoption. Lack of offline payment interoperability can arise when different payment systems or networks use different technologies, data standards, or protocols, hampering communication and the exchange of information. This can result in errors when processing offline transactions, and can also restrict the options available to users for making and receiving payments. Many of these issues can be addressed by leveraging existing protocols and standards to the extent possible, and the creation of new schemes where necessary. In addition, the way in which offline payments using tokenized digital cash are recorded and managed may also impact interoperability.[20] For example, they may be integrated into existing payment systems by using APIs to connect the two systems and enable the transfer of tokens between them. A practical design principle for offline payment systems regarding interoperability is that all system nodes as well as the payment receiver should be able to validate the integrity of the offline transaction using a common CA root certificate together with the payer's payment signature and the payer's certificate chain.[21]

Integration with ancillary systems is another important aspect of offline payment interoperability, such as digital ID systems. Failure to do so can create adoption challenges and limitations for users, merchants, and other participants in the payment ecosystem, and can hinder the growth and development of offline payment infrastructure. Developing offline payment systems that can work with existing systems should also be a key priority for payment system operators.

Mitigating security risks

Much like online payment systems, offline payment systems could become highly susceptible to issues such as fraud, digital counterfeiting, and increased cyber risks without proper security measures in place.[22] The specific security challenges of transacting offline include ensuring that the payer does not send the same transaction twice, that there are actually enough tokens held by the payer to fund the transaction, and that the payer is the holder of a legitimate wallet.[23] These risks can manifest and be mitigated by security measures at various levels of the payment system architecture (e.g., bearer application, offline transaction, back-end system rail), and a failure of the payment system operator to adequately address them could lead to criminal exploitation and significantly undermine user trust and adoption. Understanding and protecting against these threats should therefore be a key priority for payment system operators.[24]

Ensuring scalability

Scalability refers to a system's ability to handle an increased workload or number of users without a decrease in its performance. For offline payment systems, the most relevant design issues for ensuring scalability are the ability to onboard and add users, ease of roll-out and implementation, and costs to ecosystem participants. Considerations such as whether the execution environment for offline payments is hardware or software-based, and whether the capability can be implemented using any smart phones, or also feature phones, are relevant to this discussion.

OUTLINING DIFFERENT DESIGN OPTIONS FOR OFFLINE PAYMENTS

In designing the architecture for offline payments, it is important to note that the main design choices are agnostic to the underlying payment rail. The main design choices are instead related to the type of security protocol of the offline transaction (native layer-1 vs. non-native layer-2) as well as the trusted environment of the

---

[19] International Standards Organization (ISO/IEC 2382-01).

[20] https://www.bis.org/publ/othp42_system_design.pdf

[21] There are already patents granted regarding interoperable offline payment systems, see e.g., https://www.crunchfish.com/crunchfish-receives-clean-iprp-for-key-digital-cash-patent-application/

[22] https://usa.visa.com/dam/VCOM/global/sites/visa-economic-empowerment-institute/documents/veei-secure-offline-cbdc.pdf

[23] https://www.idemia.com/secure-offline-cbdc-wallet

[24] The next whitepaper in this series will explore issues surrounding practical offline payment security in more detail.

payer's bearer application (hardware-based vs. software-based). This distinction is illustrated in the figure below. The purpose of this next section is to lay out the different design choices for offline payment system design and highlight some of the trade-offs between them.

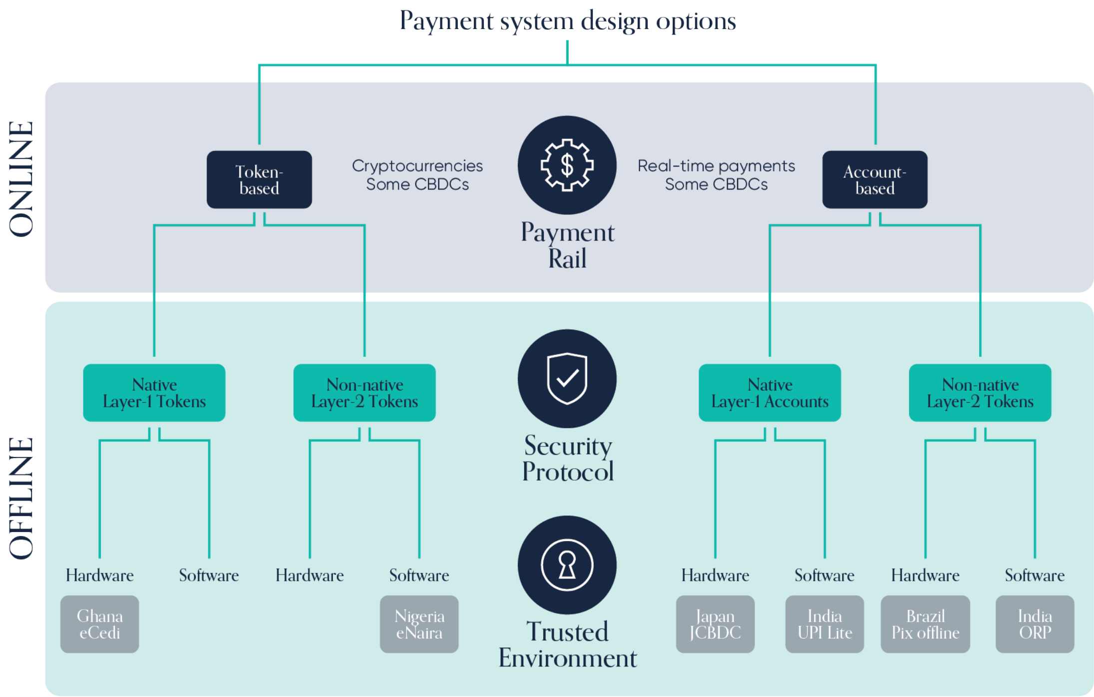

Figure 4 Payment system design options: An offline perspective

Source: Author's elaboration

Online payment rail

Offline capabilities can be enabled for token-based payment rails (e.g., all cryptocurrencies and some CBDCs) as well as account-based rails (e.g., all real-time payment system and some CBDCs). Central banks have a distinct choice when implementing digital cash. They may either base it on digital money by choosing an account-based payment rail implementation as the Reserve Bank of India (RBI)[25] and enable digital money to work offline just as cash, or alternatively base it on physical cash by representing the physical banknote digitally and implement a token-based payment rail between the central bank and banks as intermediaries.[26]

Offline Security Protocol: Native Layer-1 vs. Non-native Layer-2 tokens

A security protocol for offline payments serves the purpose of addressing the various security risks by ensuring the integrity and authenticity of the offline transaction. There are generally two design options for such a protocol. First, a native layer-1 solution, where the offline payment solution uses the same native security protocols as the underlying payment service. Alternatively, offline payments can be implemented using a non-native layer-2 security protocol, where tokens are signed out by debiting a locally held offline balance. A non-native layer-2 solution can be integrated with any type of payment rail and general ledger as the offline security protocol can be interoperable with any underlying payment system.[27]

Layer-1 and layer-2 solution are common practice used by cryptocurrencies to augment the crypto payment system with higher throughput.[28] Similarly, offline payment systems implemented as either

[25] https://conventuslaw.com/report/india-rbis-concept-note-on-digital-currency/
[26] https://www.crunchfish.com/why-must-banks-change-their-infrastructure-as-cash-becomes-digitized/
[27] The distinction between layer-1 and layer-2 infrastructure from the perspective of a blockchain network can be thought of as analogous to this distinction in the context of a security protocol for offline payments.
[28] https://academy.binance.com/en/articles/blockchain-layer-1-vs-layer-2-scaling-solutions

layer-1 and layer-2 solutions augment the underlying payment service with resilience and other desired features by enabling it to function offline as well.

Offline Trusted Environment: Hardware- vs. software-based

The second major design choice for offline payments relates to the nature of the Trusted Environment where the offline application can execute in a separate, secure environment in which the security protocol is being carried out. Such environments can be either hardware- or software-based.

Hardware-based protocols involve the use of physical devices to facilitate transactions without an internet connection, allowing them to perform payment processing tasks and store data locally or using non-internet servers. Software-based protocols, on the other hand, involve the use of software applications on a smartphone. In terms of scalability, hardware-based offline payment systems can typically handle a large volume of transactions without requiring an internet connection or external infrastructure. However, the production and distribution of physical devices, also known as Secure Elements (SE), can make this approach relatively more expensive to implement and maintain. Software-based trusted environments, on the other hand, do not require the distribution of physical components and may be updated more easily over the air. Whether a smart phone is required, or whether a feature phone or card can be supported is another consideration for scalability. Software-based offline payment could be more easily compromised by malware or other forms of tampering, whereas hardware-based solutions may be more resilient against such threats. However, further experimentation and research into security issues in a real-world context is required for further clarity on this point.

RELEVANT EXAMPLES OF OFFLINE PAYMENT EXPERIMENTATION AND IMPLEMENTATION

Offline payments are being explored by payment system operators in multiple countries, both to enhance the functionality of traditional payment rails as well in the ongoing design of and experimentation with CBDCs. Various pilot projects have been launched by regulators in collaboration with tech providers to explore the offline capabilities of their payment systems, driven by a need for increased financial inclusion and other considerations.

Country	System	Type of payment rail	Security protocol	Trusted environment
Ghana	eCedi	Token-based	Native Layer-1 tokens	Hardware-based
Nigeria	eNaira	Token-based	Non-native Layer-2 tokens	Software-based
Japan	JCB digital currency	Account-based	Non-native Layer-2 tokens	Hardware-based
India	UPI Lite	Account-based	Native Layer-1 accounts	Software-based
Brazil	Pix offline	Account-based	Non-native Layer-2 tokens	Hardware-based
India	ORP	Account-based	Non-native Layer-2 tokens	Software-based

Figure 5 Comparative analysis of selected real-time and CBDC offline solutions

Source: Author's elaboration

[29] https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline

eCedi (Ghana)

With the aim of increasing digitalization, fostering financial inclusion, and improving the efficiency, security, resilience, and consumer adoption amongst all demographic groups of digital payments, the Bank of Ghana (BoG) is working on the digital Cedi, or "eCedi". Presented as a token-based alternative to physical cash free of charge to consumers, it aims to facilitate payments without a bank account, contract, or smartphone.[30]

Since many rural areas in Ghana lack internet access - internet penetration rate was around 50% at the start of 2022[31] - it is imperative that the eCedi work offline to ensure countrywide access.[32] The solution adopted by BoG for offline transactions has been G+D Filia, a layer-1 native token-based hardware solution using smartcards as the primary bearer device. These smartcards will be loaded either by a bank or payment service provider, or by receiving funds from another peer. Smartphone wallets will be used for online transactions, and they will serve as intermediary applications for consecutive offline transactions between smartcards.[33]

eNaira (Nigeria)

In 2021, Nigeria became the first African country to launch a live CBDC – the eNaira, aimed at expanding access to banking, improving financial inclusion, enabling cheaper and faster remittances, and growing the digital Nigerian economy. To increase the existing use cases and increase financial inclusion, the Central Bank of Nigeria (CBN) is in the process of studying offline payments capabilities for e-Naira. For this purpose, CBN has engaged a Swedish technology vendor, Crunchfish, for a Proof-of-Concept (PoC) of their Digital Cash capabilities for Android and iOS, and its integration into the eNaira wallet and back-end. This solution is a layer-2 offline payments solution, working with non-native tokens for proximity payments, in a software-based trusted environment on the eNaira wallet.

JCB Offline Digital Currency Pilot (Japan)

The Bank of Japan carried out a PoC from April 2021 to March 2022 with the aim of evaluating whether basic CBDC transactions such as issuance, payout, transfer, acceptance, and redemption can be properly processed. Nevertheless, the offline capabilities were not completely studied. In this space, Japan's international card payment network (JCB), along with IDEMIA and the fintech company Soft Space, have been working in a layer-1 offline payment solution with native tokens for retail payments in proximity, using smartcards as the bearer device – as part of their JCB Digital Currency pilot project.[34]

Trying to show that CBDC can be integrated with existing payment card systems and infrastructure, CBDC payments using payment cards will be routed through the conventional account-based card network and eventually to JCB's blockchain-based CBDC network. It is expected to conduct a pilot test with Tokyo merchants during the first quarter of 2023.

UPI Lite (India)

Since July 2022, the United Payments Interface (UPI), India's stunningly successful real-time payments platform, has processed more than 6 billion transactions per month, around half of which are for values of less than INR 200 (USD 2.4).[35] Processing of this massive volume leads

[30] https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf
[31] https://datareportal.com/reports/digital-2022-ghana
[32] https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf
[33] https://www.gi-de.com/en/payment/central-bank-digital-currencies/cbdc-implementation/filia
[34] https://www.ledgerinsights.com/jcb-cbdc-idemia-soft-space-jcbdc/
[35] https://www.npci.org.in/what-we-do/upi/product-statistics

to huge stress on the core banking infrastructure of the banks, which has led to reports of system glitches and a higher rate of rejection for initiated transactions.

In response to these issues, the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI) launched an "on-device wallet" pilot program with limited banks named UPI Lite with the purpose of offering small-value offline payments to address system overload. UPI Lite was launched in September 2022 and offers offline payment initiation capabilities up to a limit INR 200 per transaction, using one click single factor authentication. It is a layer-1 solution, where the wallet has a holding limit of INR 2000 (USD 24). By using this pre-loaded balance, UPI Lite allows the remitting bank to be offline at the moment-of-payment, which significantly decreases its transaction load. The payer must be online to load and use the wallet. In the next phase of UPI Lite, NPCI plans on allowing also the beneficiary bank to be offline. NPCI is also exploring a future UPI Lite version where the payer and/or payee may also be offline.[36]

Pix Offline (Brazil)

Pix, Brazil's instant payment scheme, has experienced astronomical growth since its launch in the summer of 2019. According to the Central Bank of Brazil over 80% of the Brazilians with a bank account already use Pix. To increase the reach of Pix even further, enhancing financial inclusion and driving adoption, the Central Bank of Brazil is exploring offline capabilities of Pix. Pix offline is a hardware-based layer-2 solution that is expected to work through a pre-paid Pix proximity card, allowing users to carry out payments via Pix without internet access.[37]

Offline Retail Payments (India)

As part of its innovation strategy, RBI introduced Regulatory Sandboxes in 2020 to foster responsible innovation in financial services, promote efficiency and bring benefit to end users. One of the Regulatory Sandbox, focused on offline payments, started a pilot with HDFC Bank to explore Offline Retail Payments (ORP).[38]

The ORP project is piloting a layer-2 offline payment solution for proximity payments with non-native tokens, issued from a software-based trusted environment in payment apps on smartphones. Onboarded merchants for offline payments may accept payments on any device running the Swedish vendor Crunchfish's Digital Cash verifier application. The pilot was extended in scope by the RBI to include P2P payments and scheduled to run to April 2023, followed by a one-month evaluation by RBI. The project will provide input for RBI's guidance and regulatory support in providing offline payments to the payment ecosystem of India.[39]

[36] https://www.npci.org.in/what-we-do/upi-lite/product-overview
[37] https://www.pagbrasil.com/pix/pix-offline-understand-more-about-brazils-instant-payment-upcoming-feature/
[38] https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=54314#:~:text=The%20product%20'Offline%20Retail%20Payments,to%20have%20a%20network%20connection.
[39] https://www.crunchfish.com/crunchfish-ready-to-start-digital-cash-pilot-with-indian-banks/

CONCLUSION

Offline payments are quickly becoming an essential aspect of the modern payments landscape, acting not only as a tool to improve financial inclusion and payment system resilience but also as a mean of ensuring the highest levels of user trust and convenience. Making the right decision choices for offline payments is key to ensuring the usability, security, and overall effectiveness of these systems. Developing interoperable, secure, and scalable offline payment solutions is of utmost importance, and payment system operators must effectively weigh the potential trade-offs between the different offline approaches and market solutions. Ultimately, their design decisions will be a function of local market conditions, use cases targeted, as well as the goals and aims of their payment system.

Like cash and online payment systems, offline payment systems can be vulnerable to issues such as fraud, digital counterfeiting, and increased cyber risks without proper security measures in place. Protecting against risks such as double-spending and transaction replay should therefore be a top priority for payment system operators. In the next white paper of this series, we will expand on the nature of the security risks faced for offline payment systems, and detail and analyze the available mitigation techniques and outline how offline payment security may be implemented in practice.