Enabling offline payments in an online world

A practical guide to offline payment security

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.

CONNECT AND PAY. ALWAYS.

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

Table of Contents

Enabling offline payments in an online world

A practical guide to offline payment security

INTRODUCTION

As digital payment usage in many markets has spiked dramatically over the last several years, the urgency around improving the resilience of today's digital payment infrastructure has never been greater. Digital payment services must be able to not only withstand temporary disruptions but also achieve the same level of operational robustness and security consistent with other types of public infrastructure. However, today's online payment schemes lack the necessary resilience in the face of temporary system failures, such as downtime in back-end infrastructure (e.g., bank servers, payment switches) or poor internet connectivity for users.

In this regard, payment system operators around the globe are increasingly becoming aware of the advantages of offline use of digital payments to enhance the functionalities of both real-time payment systems and central bank digital currencies (CBDCs). Major markets such as Brazil, India, Japan, and Nigeria, have already begun to experiment with offering offline payment capabilities to improve payment system resilience, increase financial inclusion and enhance the experience of users with greater convenience, privacy, and trust. As interest in this area continues to grow in the medium term, additional markets are likely to delve into this area as well.

Much like online payment systems, offline payment systems face risks from cyberattacks, data breaches, digital counterfeiting, or other forms of criminal exploitation. If not properly mitigated, these risks can result in reputational damage for the system operator and hamper user trust and adoption. As system operators increasingly explore offline payment capabilities, it is crucial that they understand the unique security challenges of enabling offline payments. They must put in place appropriate mitigation techniques to address risks that are likely to emerge at each level of the offline payment system architecture. Moreover, they must do so by effectively balancing the trade-offs between providing a secure means of payment and user convenience.

In our last white paper, we provided practical insights to payment system operators as they begin to navigate the various design choices for offline payment system design.[1,2] In this paper, we will provide a practical guide to navigating the unique challenges of offline payment security.

---

[1] https://mb.cision.com/Public/14959/3700171/9a9a65213fd7363f.pdf

[2] The key insights of the paper were discussed in a webinar that can be viewed here:
https://www.youtube.com/watch?v=e98bETROYfc

THE BASICS OF OFFLINE PAYMENT SECURITY

Whether online or offline, all payment systems are vulnerable to criminal exploitation. Even the most modern payment systems face risks of cyberattacks, data breaches, and digital counterfeiting, which can undermine trust in system operators and hamper usage of the underlying payment instrument.[3, 4] Designing and maintaining a secure payment system is therefore a key priority for any digital payment system. This is especially true when designing or enhancing a payment system that can successfully perform consecutive, secure offline payments.[5] This section details the unique security issues that must be considered when designing an offline payment system.

System-wide vs. transaction-based validation

Unlike a physical bank note, digital money is almost infinitely duplicable or falsifiable and is only meaningful when a trusted authority validates its authenticity and ownership.[6] The trusted authority maintains a copy of the general ledger and updates it in real-time. It is responsible for validating each transaction, including checking whether the funds have already been spent, whether there are adequate account balances, whether the user is receiving the funds is authorized to do so, etc.[7]

For offline transactions, the validation and authentication at the time of payment must occur without the benefit of a real-time connection to the general ledger, or depending on the type of offline implementation model, without any connection to a general ledger. We refer to this concept as transaction-based validation. A useful analogy is a merchant accepting a bank note in exchange for the sale of goods or services. The authenticity of the bank note must be assessed by the individual merchant as the transaction is taking place and without the help of any type of centralized counterfeiting or fraud detection.

Greater double spending risks

Transaction-based validation inherently creates a particular challenge for offline payments in mitigating the risk of double spending. Double spending is where a user either spends the same money or token two or more times, makes several transactions with the same funds, or successfully tampers with the payment network to accept a duplicate transaction.[8] Online payments typically prevent double-spending through system-wide validation and authentication of each transaction. The lack of real-time connectivity with a trusted authority in an offline setting therefore makes these types of payments more vulnerable to the double-spending problem.

Time validity as a security tool

As mentioned above, online payment systems process transactions in real-time, with the network constantly updating the general ledger. The ledger is either maintained by a trusted third party or verified by a consensus mechanism that ensures that all nodes on the network have an identical copy of the ledger. As a result, transactions are processed almost instantly, and the time validity of a payment is not a significant concern.

For offline payment systems, limiting the time validity of payment tokens or offline wallets is a highly relevant security tool that prevents unauthorized transactions or double-spending attempts. It offers a specific time frame in which the payment must be completed, after which the tokens become invalid or the offline wallet inoperable; it also requires a mechanism to trust the time reference in an offline mode. In contrast, offline payments that have no time limit and that can be accepted or processed at any time may be more susceptible to fraud, as there exists a longer window for malicious actors to attempt digital counterfeiting, double-spending or unauthorized transactions. Practically speaking, it is important to strike the right balance between the convenience of having no time expiration on funds versus the security benefits of limiting time validity.

---

[3] https://link.springer.com/chapter/10.1007/978-3-319-73150-6_68

[4] https://hal.science/hal-00537097/

[5] As discussed in our last white paper, consecutive, secure offline payments are those in which the payer and payee exchange a transaction offline, and the payee can immediately spend the received funds in another offline transaction.

[6] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

[7] In the case of traditional payment systems, the trusted authority is a central counterparty or infrastructure, and in the case of cryptocurrencies and some CBDCs, it is a distributed network.

[8] In the case of physical cash, double spending is avoided given that after paying with a banknote, the payer no longer has the funds in their physical possession. https://www.bankofcanada.ca/2021/12/staff-working-paper-2021-67/

DESIGNING A SECURE OFFLINE PAYMENT SYSTEM

Implementing a security protocol is a requirement for an online or offline payment system to ensure the integrity and authenticity of any transactions processed on the platform. Online systems typically use either account-based security protocols (e.g., real-time systems and some CBDCs) or token-based protocols (e.g., cryptocurrencies and some CBDCs). Account-based protocols rely on unique account identifiers that are associated with a single entity or account within the system. Token-based protocols protect the va-

lidity of the data using a unique encrypted identifier generated in a secure manner that must be validated when a transaction is executed.

SECURITY PROTOCOL DESIGN OPTIONS

Designing a secure offline system involves implementing a security protocol that will preserve the integrity of the payer as well as the payment data to prevent double- spending, protect sensitive data, and provide resilience in the face of any temporary disruptions. As discussed in our first white paper, there are two main design options for offline security protocols: native layer-1 or non-native layer-2.
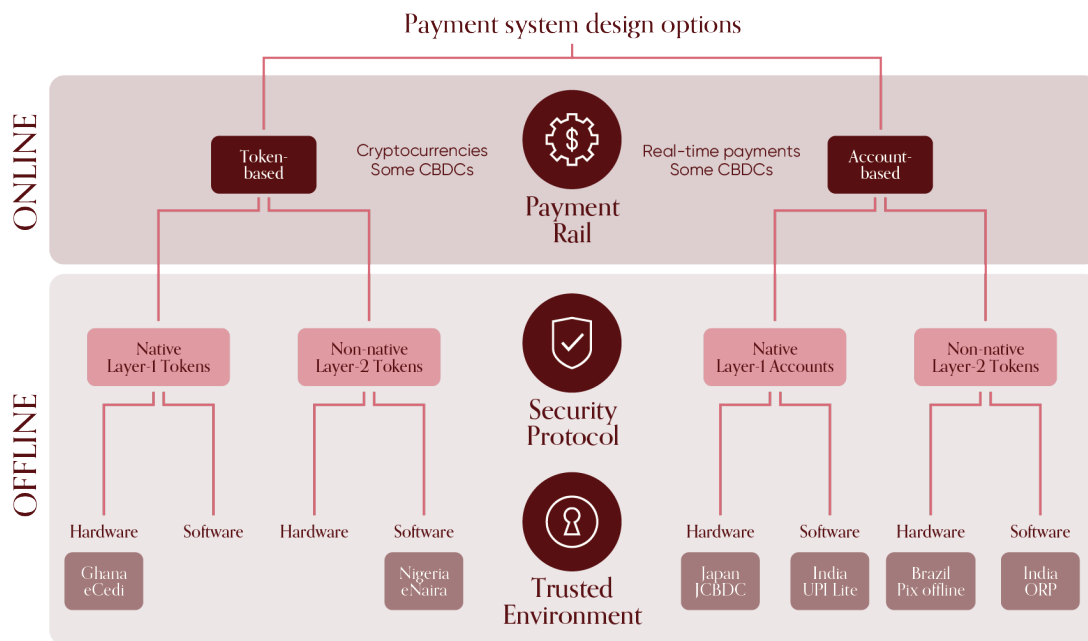

Figure 1 Payment system design options: An offline perspective

Source: Author's elaboration

In addition to this distinction, we have also identified two other relevant design choices. First, the security protocol can be either based on a proprietary or open scheme. Second, it can use either encryption or signatures in the application layer. We describe each of these in detail below .
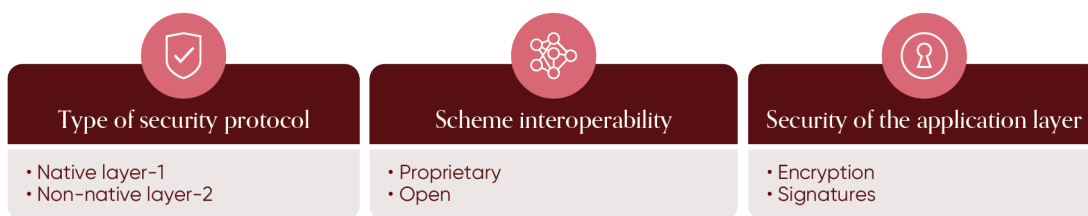
Figure 2 Payment system design options: An offline perspective

Source: Author's elaboration

**Type of security protocol:
native layer-1 vs. non-native layer-2**
For layer-1 solutions, the security protocol utilized by the offline payment system is the same protocol used by the underlying online payment rail. This may limit the privacy of offline transactions as they would be subjected to the same level of "surveillance" as online transactions. With

non-native layer-2 solutions, the security protocol is separate from the online payment scheme, potentially allowing for greater privacy for users. Tokens are "signed out" by debiting a locally held offline balance. Non-native layer-2 solutions can typically be integrated with any type of payment rail and general ledger as the offline security protocol and can be made interoperable with any underlying payment system.[9]

Scheme interoperability: proprietary vs. open

Offline payment systems may either be proprietary or open (interoperable). Proprietary protocols are often developed for a specific payment service - and not designed to be interoperable with other services. Proprietary encryption is typically used by companies to secure their own systems and products. Although they can offer enhanced security, they may not be compatible with other systems, and can be more difficult and expensive to implement. Interoperable protocols tend to be more scalable and rely typically on standard Public Key Infrastructure (PKI).[10] PKI is widely used by online as well as offline payment schemes. Cryptographic public keys are linked to digital certificates to authenticate the identity of devices or payers. The certificates are signed by a trusted third party, known as a certificate authority (CA), and serve to verify the service and provide trusted identification of the payer and the recipient.

Security at the application layer: encryption vs. signatures

Offline security protocols that rely on encryption typically involve an initial handshaking[11] procedure in which the payer and recipient agree on what key to use for the encryption. This key could either be a one-time key or the payer may encrypt the offline payment message using the recipient's public key in a PKI-based setup. The recipient is then the only party able to decrypt the offline transaction using either the matching private key or the agreed upon one-time key.

An alternative approach to encryption that is being explored is to instead use signatures at the application level. This approach is also based on PKI and uses the same Security Association (SA)[12], using private keys and certificates with associated public keys, as used with encryption. However, the way the private keys and certificates are used is different. Using signatures, the payer uses their private key to sign the offline transaction message that includes the payer's digital certificate with its public key. The offline payment message is still encrypted as it provides a standard upon which the offline payment message can travel through each protocol layer.

Encryption	Signatures
Encryption is used to encode sensitive information in the message	A signature is used to verify the authenticity of the message
The recipient uses his/her private key to decrypt the encrypted data in the message	The payer uses his/her private key to sign the message
The payer uses the recipient's public key to encrypt data in the message	The public key is used by the recipient to verify the signature with the payer
Only the receiver can use his/her private key to decrypt the data. If the data is decrypted, it is considered to be verified.	Signature is considered verified only if the message remains unaltered and untampered in between payer and recipient of the signature
A digital signature certificate verifies and authenticates the identity of the recipient to generate the encryption keys	A digital signature certificate stores the signature of the payer after verification of identity
Recipients need to possess an encryption certificate from an authorized certifying authority to successfully encode a message	Payers need to have a signature certificate from an authorized certifying authority to legally sign a transaction
May use proprietary or PKI-based encryption with certificates	May use signatures with public key pairs or PKI with certificates

Table 1 Comparison of encryption vs. signatures for use in offline payments[13] Source: Author's elaboration

---

[9] A future white paper will explore the various aspects of privacy in offline payment systems.
[10] https://csrc.nist.gov/glossary/term/public_key_infrastructure
[11] https://csrc.nist.gov/glossary/term/handshake
[12] https://csrc.nist.gov/glossary/term/security_association
[13] https://emudhradigital.com/kc/what-is-the-difference-between-signature-and-encryption.jsp

Utilizing this approach to exchange offline payment messages may offer some advantages over encryption. First, there is no handshaking required with the recipient at the moment-of-payment, which enables offline payment initiation remotely via SMS or locally via a QR code. Second, the offline transaction can be verified at any node in the system, which enables a much simpler SA in the form of access to the CA-root certificate. Last, the recipient could have a payment application without a trusted application or even be not yet onboarded with the payment service.

OFFLINE TRUSTED ENVIRONMENT DESIGN OPTIONS

The offline trusted environment refers to the separate offline application environment in which the security protocol is executed. Having an offline trusted environment is needed for maintaining cryptographic keys and legitimate balances, ensuring authorized use and the integrity of the offline payment application. An offline trusted environment ensures that the balances stored in the application are accurate and reflect the legitimate transactions that were carried out. Moreover, the offline trusted environment helps to prevent errors or inaccuracies in the balance information. It can be designed to limit access to the payment application and its associated data to only authorized users, which prevents unauthorized access, use, or tampering of payment data. Last, it ensures the integrity of the offline payment application. The usage of an offline trusted environment ensures that the payment application and its associated data are protected from unauthorized modifications or tampering. This also helps maintain the integrity of the payment system and ensures that payment transactions are processed accurately and securely.

Hardware-based vs. software-based

Hardware-based applications use hardware security modules to secure payment transactions and protect sensitive information. They involve the use of physical devices to allow transactions to be processed without an internet connection. The use of these physical devices – that can perform payment processing tasks and storage data locally - aims to protect against unauthorized access, tampering, and theft of payment information. The costs of producing and distributing the physical devices make a hardware-based solution more expensive to implement and maintain in comparison to software-based solutions, though hardware-based solutions may also provide a higher level of security and protection.[14]

Software-based environments, on the other hand, provide virtual secure environments integrated onto a digital device. Unlike hardware-based solutions, they do not need to distribute physical components and updates can be made more easily which make such solutions more scalable. However, software-based offline payment systems can be more susceptible to compromise by malware or other types of tampering. The reliance on software may more easily enable malicious actors to access or alter the payment information stored on the device. To mitigate these risks, software-based protocols may include additional security measures. Despite the potential for compromise, software-based protocols can offer a convenient and cost-effective solution for offline payment.[15]

Offline payment schemes are likely to use both hardware- and software-based trusted environments. Whereas the software-based trusted environments are most applicable for trusted applications on smartphones, there is also a need for cards, wearable and feature phones for financial and digital inclusion reasons, which would be deployed using hardware-based trusted environments. It should be possible to interact offline between trusted applications on smartphones and trusted applets on cards, wearables and feature phones, even in offline mode.[16]

MITIGATING AGAINST OFFLINE SECURITY THREATS

Having gained a better understanding of the design elements of a secure offline payment system, we next discuss the specific security risks and mitigation at each level of the system architecture:

---

[14] https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline
[15] Ibid.
[16] https://www.crunchfish.com/crunchfish-digital-cash-non-mobile-devices-webinar/

- offline trusted environment within the bearer application
- offline security protocol for payments
- online payment application and rail.

As noted previously, one of the key risks in an offline payment scheme is double spending. There are many types of attacks that might lead to double-spending, e.g., man-in-the-middle attacks, transaction replay, cloning, jailbreaking, and tampering with the bearer application. Here we provide a discussion of some mitigation techniques that can be used to protect against such security risks.

PRESERVING THE INTEGRITY OF THE BEARER APPLICATION

Some of the major security threats that can occur at the level of bearer application (e.g., smartphone, feature phone, wearable device, card, etc.) include tampering[17] with the trusted application or its data. There is also the risk of cloning if the device is jailbroken or rooted, which enables a reset of the offline balance to prior levels. Although it is always possible to discover fraudulent cloning when the payer goes online, it is important to mitigate against rollbacks if the payer stays offline by imposing additional

risk limits on transactional amounts. Cloning between devices is commonly mitigated via device fingerprinting, which ties the offline trusted application to the device on which it is running. Unauthorized access may be mitigated using Additional Factor Authorization (AFA) based on passphrases or biometrics to access the offline trusted application, for example. The trusted environment also protects against overdrafts and ensures that imposed risk limits by the issuer and the regulator are followed.

Traditionally, Secure Elements (SEs) have existed in the form of a hardware chip or token that are designed to run a limited set of applications, and/or store confidential data and cryptographic keys. However, recent innovation in the space has led to the development of software-based SEs, or virtual SEs.[18] Virtual SEs purportedly offer a similar level of protection from unauthorized access as hardware chips or tokens but have the benefit of greater ease of distribution and lower implementation costs. Therefore, their use may allow for easier scalability when compared to hardware-based SEs. However, they must be deployed on a smartphone, limiting their relevance in markets with low smartphone penetration for the time being.
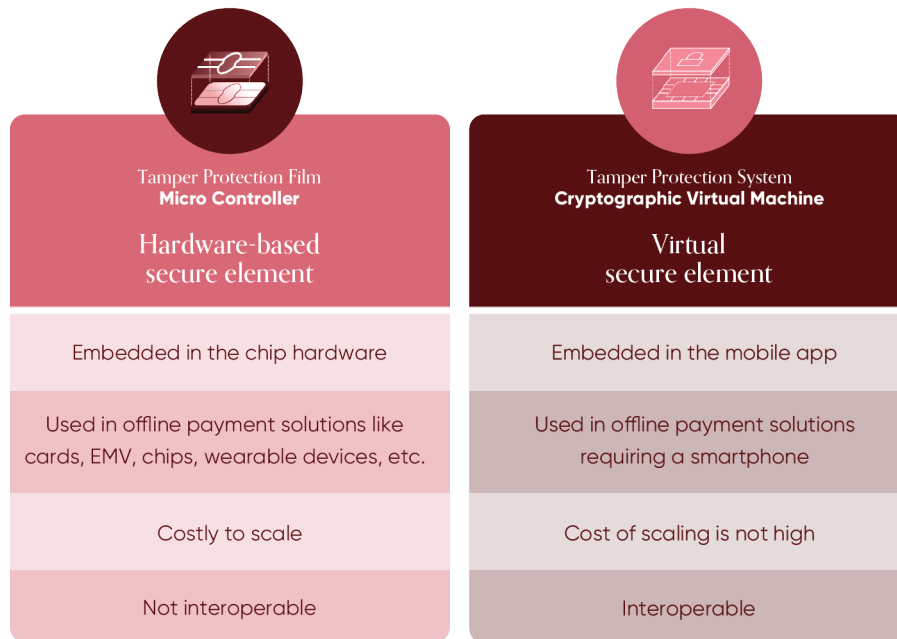

Tamper Protection Film **Micro Controller**	Tamper Protection System **Cryptographic Virtual Machine**
Hardware-based secure element	Virtual secure element
Embedded in the chip hardware	Embedded in the mobile app
Used in offline payment solutions like cards, EMV, chips, wearable devices, etc.	Used in offline payment solutions requiring a smartphone
Costly to scale	Cost of scaling is not high
Not interoperable	Interoperable

Figure 3 A comparison of hardware secure elements vs. virtual secure elements   Source: Author's elaboration

---

[17] https://csrc.nist.gov/glossary/term/tampering
[18] https://www.v-key.com/wp-content/uploads/2019/09/1.-V-Key-Factsheet-V-OS-Virtual-Secure-Element.pdf

ENABLING THE INTEGRITY OF OFFLINE PAYMENT MESSAGING

At the level of the offline payment messaging scheme, the risk of transaction replay and man-in the-middle attacks, both manifestations of double-spending, must be mitigated. A transaction replay attack uses malicious apps to delay or intercept data transmission that occurs over a network. This information can then be processed and re-sent numerous times to effectively duplicate transactions. Even though it is relatively simple for hackers to carry out replay attacks, offline payment messaging schemes offer preventive measures for these attacks using timestamps and challenge requests and by positioning bookmarks in the new local ledger.[19] Targeting the connection between the two parties is an alternative to directly attacking the integrity of the offline payment, with a man-in-the-middle assault the most typical method of doing this. In such attacks, the payer application and the payee application believe that they are communicating directly with the intended end point, but the attacker is intercepting and/or modifying the communication in the middle.[20] All cryptographic systems that are secure against man-in-the-middle attacks use two means: authentication and tamper detection. While an SE approach can provide tamper detection, authentication of the transactions can be ensured using public key infrastructure (PKI).[21]

While PKI is widely used on the internet today, it relies upon cryptography that is believed to be secure given the computational power available today and in the medium term. However, popular cryptographic schemes based on these hard problems, including RSA and Elliptic Curve Cryptography, will eventually be broken by a quantum computer.[22] This will rapidly accelerate the irrelevance of today's security systems and will have a dramatic impact on all sectors of the economy. To address this, there are plans to update the security algorithms with longer keys and signatures so that quantum computers cannot break them. However, for offline payments this is not viable due to limited bandwidth and storage capacity offline. To ensure integrity of offline payments when quantum computers are available therefore requires using a quantum-secure cryptographic key as a shared secret.[23]

ENSURING THE INTEGRITY OF ONLINE PAYMENT SYSTEMS

Even if protection against double-spending must be provided at the transactional level in an offline payment scheme, there should nevertheless be a seamless integration with the online general ledger where double-spending can also be discovered at the time of reconciliation between the offline and online ledgers. Offline payment solutions should therefore have adequate back-end protections, such as certificate revocation, to ensure that the risks arising at the time of reconciliation are effectively addressed. It is also possible to deploy measures like those used in securing online payment systems, like behavioral biometrics and certificate expiration, etc. Last, the risk of loss and fraudulent use of offline payments can be reduced by imposing risk limits on offline wallets. These limits can be linked to KYC levels, higher limits for full KYC compliance and lower limits for partial KYC compliant customers. Such limits could be imposed by the issuer or driven by regulatory mandate.

RELEVANT EXAMPLES OF OFFLINE PAYMENT EXPERIMENTATION AND IMPLEMENTATION

As we discussed in the last white paper, offline payments are being explored by payment system operators in multiple countries to enhance the functionality of traditional payment rails on the one hand and as a key aspect of the ongoing design of and experimentation with CBDCs on the other hand. Various pilot projects have been launched by regulators in collaboration with technology providers to explore the offline capabilities of their payment systems. This section details the offline security design choices of the same six offline payment experiments and pilots that were first introduced in the last white paper.

---

[19] https://learn.bybit.com/blockchain/what-is-a-replay-attack/

[20] https://www.insidesecure.com/content/download/1133/13650/file/Securing%20Mobile-Payments.pdf

[21] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/pub-lic-key-infrastrukturen.html

[22] https://math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf
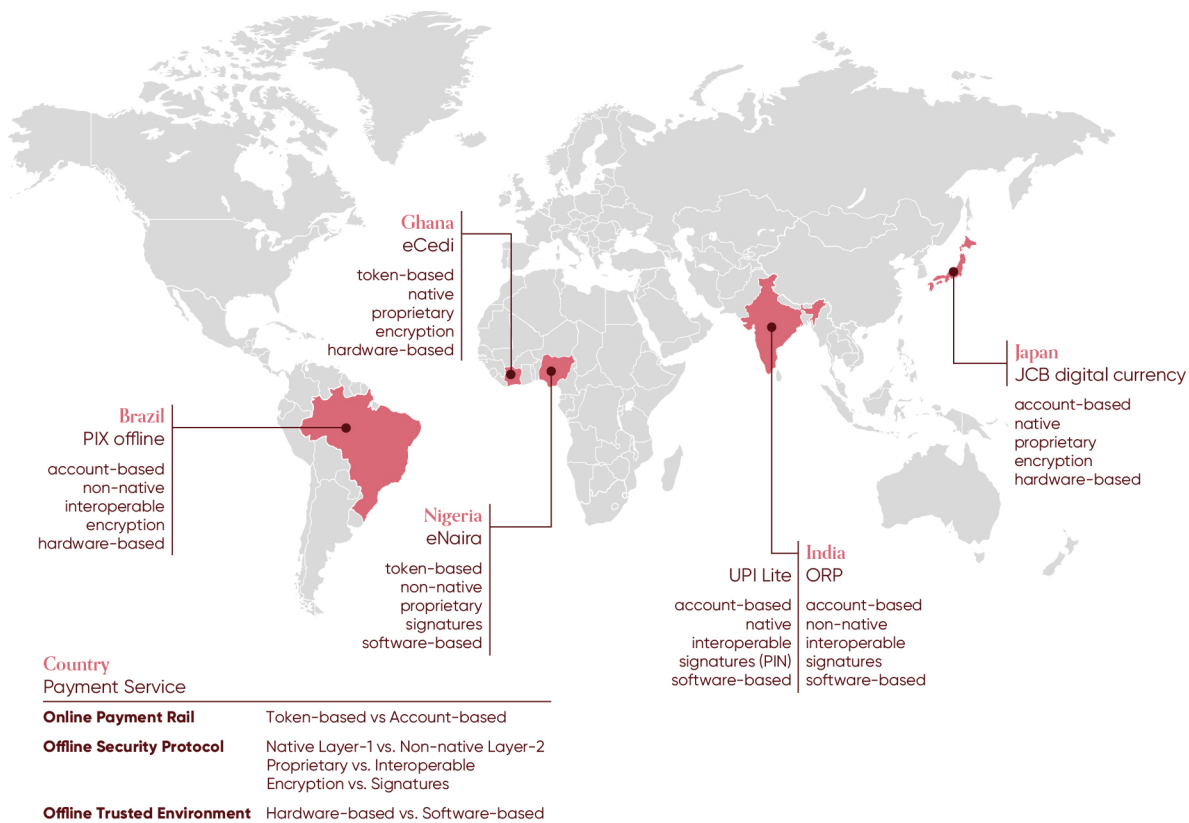
[23] https://www.crunchfish.com/crunchfish-makes-digital-cash-quantum-safe/

Figure 4 Comparison of real-world offline payment implementations

Source: Author's elaboration

eCedi (Ghana)

With the aim of increasing digitalization, fostering financial inclusion, and improving the efficiency, security, resilience, and widespread consumer adoption 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.[24]

Since many rural areas in Ghana lack internet access - internet penetration rate was around 50% at the start of 2022[25]- it is imperative that the eCedi work offline to ensure countrywide access.[26] 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.[27] The solution is proprietary for eCEDI with encryption in the application layer.

eNaira (Nigeria)

In 2021, Nigeria became the first African country to launch a live CBDC with 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

---

[24] https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf

[25] https://datareportal.com/reports/digital-2022-ghana

[26] https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf

[27] https://www.gi-de.com/en/payment/central-bank-digital-currencies/cbdc-implementation/filia

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. Merchants accepting these payments can do so on any device. The solution is proprietary and uses signatures in the application layer.

JCB Offline Digital Currency Pilot (Japan)

The Bank of Japan (BOJ) 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.

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.[28] The solution is proprietary and uses encryption in the application layer.

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).[29] Processing this massive volume has led 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.[30] The solution is interoperable for all UPI payment services where the payer signs off a transaction with a Pin in the UPI common library.

Pix Offline (Brazil)

Pix, Brazil's instant payment scheme, has seen 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.[31] The solution is interoperable for all Pix payment services with encryption in the application layer.

---

[28] https://www.ledgerinsights.com/jcb-cbdc-idemia-soft-space-jcbdc/
[29] https://www.npci.org.in/what-we-do/upi/product-statistics
[30] https://www.npci.org.in/what-we-do/upi-lite/product-overview

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 and IDFC First Bank to explore Offline Retail Payments (ORP).[32]

The ORP project, implementing the Swedish tech provider Crunchfish's Digital Cash solution, 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 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.[33] The solution is interoperable for the participating banks using signatures in the application layer.

CONCLUSION

In this paper, we outlined some of the key practical considerations related to enabling secure offline payment systems. With double spending the key security risk for offline payments, traditional mitigation techniques used in online systems are not enough. Payment system operators must therefore understand the far-reaching implications of the paradigm shift away from transaction-based validation and put in place mitigation techniques to combat the unique security challenges as posed in the offline payments context. Doing so is key to fostering adoption and trust.

While theoretically the security threats and their mitigation techniques can be identified and solved individually, security mitigation methods are also interlinked with other features like privacy, interoperability, scalability, and sustainability linked to the implementation of the offline solution, topics which will be explored in future papers. All these factors must be weighed together in deciding what type of approach or techniques to apply. ■

---

[31] https://www.pagbrasil.com/pix/pix-offline-understand-more-about-brazils-instant-payment-upcoming-feature/
[32] https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx
[33] https://www.crunchfish.com/crunchfish-ready-to-start-digital-cash-pilot-with-indian-banks/

Crunchfish editorial on offline payment design choices[1]

OFFLINE PAYMENT DESIGN OPTIONS

There are five distinct design choices for offline payments. In the first whitepaper Lipis Advisors outlined three of them and in this second whitepaper they have outlined two additional in relation to the offline security protocol.

As a deep tech company Crunchfish have a contrarian perspective on each design choice. This section outlines Crunchfish's perspectives on best practices when it comes to offline payment design and security.

Online payment rail: Token-based vs. **Account-based**
Digital Cash is made up by two words. Digital and Cash. The mistake many central banks and payment service providers do is to think that Digital Cash is about digitizing the banknote. It is not. This is very difficult and leads to all sorts of problem for offline payments. It is much better for multiple reasons to start with the digital money we already have today in accounts and provide payments with cash-like properties.[2]

Offline security protocol 1: Native vs. **Non-native**
Payment systems, especially CBDCs must provide the same level of personal integrity as paying with cash. It is still possible to balance integrity with AML and tax evasion by imposing transaction limits on offline wallets not subject to full KYC. A security protocol separate from the underlying online payment rail is therefore much preferred. This provides privacy-by-design, in contrast to an unacceptable surveillance-by-design.

Offline security protocol 2: Proprietary vs. **Interoperable**
To avoid having payment services in incompatible silos it is important to ensure interoperability. To accomplish this the e-wallets must guarantee the payer´s intent to pay and that the debit is cleared before sending the payment to the recipient on the backbone rail. This same mechanism is used by Crunchfish Digital Cash to be able to pay to any domestic handle. The required mechanism for full offline payments is that multiple payments services verify offline payments with the same CA-root. It is possible to use a global root certificate authority and achieve interoperability world-wide for offline payments using any payment service.[3]

Offline security protocol 3: Encryption vs. **Signatures**
Front-end offline payments applications have a Security Association (SA) with a private key and a certificate with the associated public key. Most offline systems rely on application-level encryption where the payer gets and uses the receivers public key. This has several severe drawbacks. With standard PKI-based signatures it is possible to avoid handshaking completely at the moment-of-payment, verify any issued offline payment at any node in the system and be able to pay to recipients that do not have applications executing in trusted environments. Encryption is delivered at each protocol level anyway.[4]

---

[1] This editorial reflects Crunchfish's proprietary views.
[2] https://www.crunchfish.com/crunchfish-goes-global-within-cbdc-having-solved-offline-and-private-payments/
[3] https://www.crunchfish.com/crunchfish-receives-clean-iprp-for-key-digital-cash-patent-application/
[4] https://www.crunchfish.com/crunchfish-patents-inclusive-payments-with-privacy-and-interoperability-using-digital-cash/

Offline Trusted Environment: Hardware-based vs. **Software-based**

Smartphones are the dominant bearer for payments today. In the future it is likely that smart glasses will play the same role. As it is not possible that all should be forced to use devices with the same hardware when it comes to smartphones or smart glasses, its trusted environment must be software-based. For financial and digital inclusion there is a need to deploy Digital Cash applications on cards, wearables, and feature phones as well. These hardware-based trusted environments are peripheral bearers that need to be able to exchange digital cash with the smartphone as the main bearer, even in full offline-mode.[5]

A PARADIGM SHIFT IN PAYMENTS

In addition to ensure the integrity of the payer, the offline payment application as well as the offline transaction an offline payment scheme can deliver survivability in the face of any temporary failures. Today's payments services are not robust as they fail if any link or node fails. Digital payments must be robust given their critical role in modern societies and will never ever become robust until they are redesigned from an offline perspective. An offline protocol enables a payment to go through instantly if the pipes are open, but more importantly it provides payments with the resilience to survive in the face of temporary failures on any link or node.[6]

Crunchfish propose using PKI-based signatures implemented by an application and communication network agnostic augmentation to the application layer in the communication protocol stack that Crunchfish refer to as the Trusted Application Protocol (TAP). Whereas online payment schemes lack survivability in the face of failures, TAP is designed to cope despite of temporary failures on any link or node at the moment-of-payment. This is achieved by logically breaking up payments into three distinct steps; reserve, pay and settle and adding a TAP header to the application data at the application-level in the protocol hierarchy.[7]
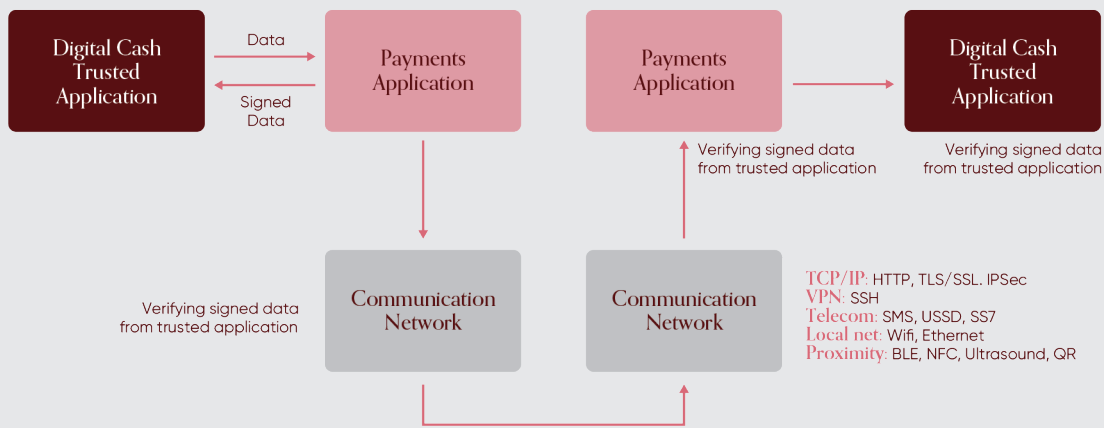

Figure 5 Offline payment systems using signatures from a Digital Cash Trusted Application   Source: Crunchfish

---

[5] https://www.crunchfish.com/crunchfish-digital-cash-non-mobile-devices-webinar/

[6] https://www.crunchfish.com/crunchfish-ceo-argues-for-a-necessary-paradigm-shift-in-payments-at-aktiedagen-in-gothenburg/

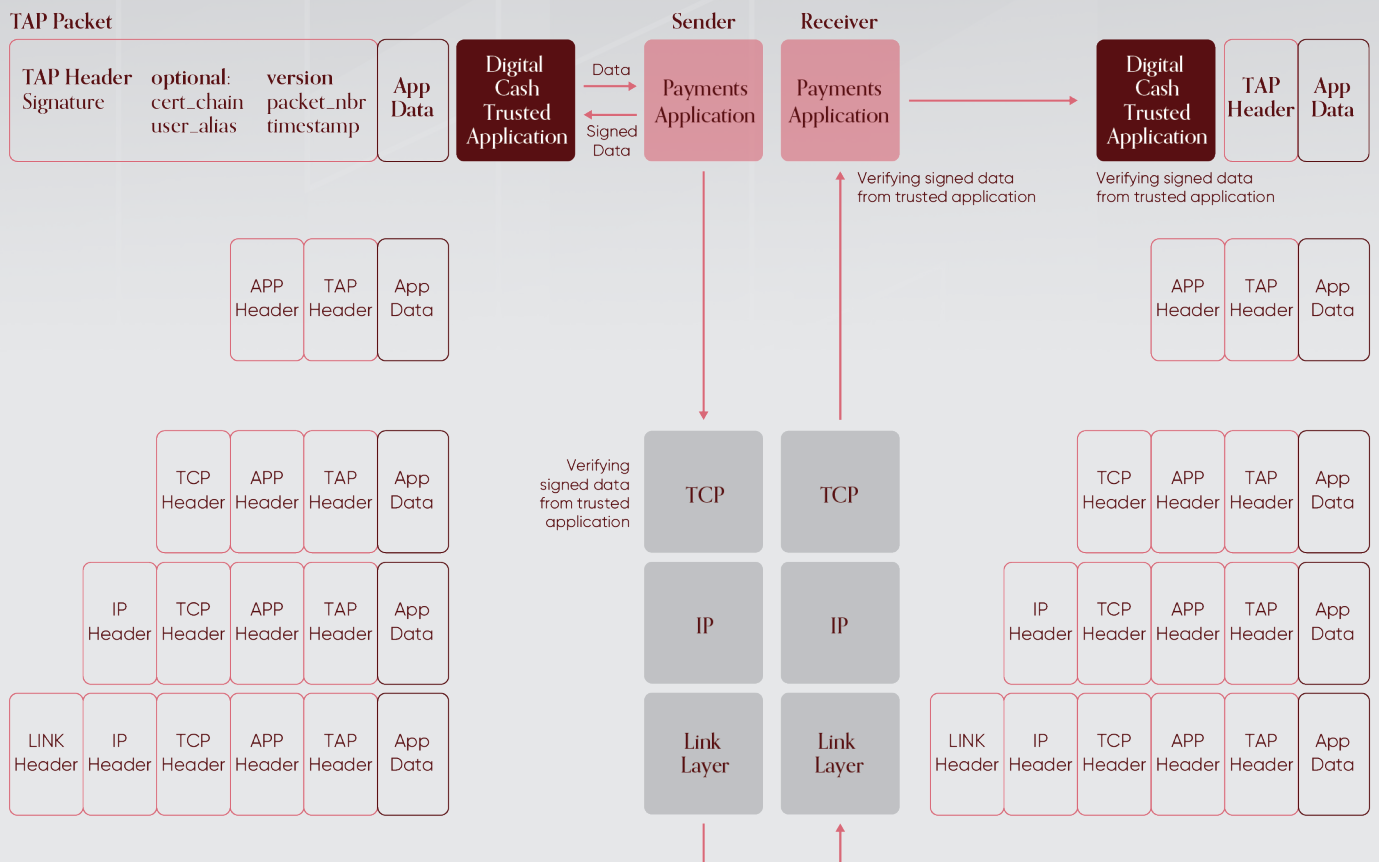[7] https://www.crunchfish.com/crunchfish-digital-cash-2-0-a-paradigm-shift-in-payments/

Figure 6 The Trusted Application Protocol used with the internet TCP/IP protocol stack

Crunchfish propose that all payment applications should augment their service with the TAP. Although today's payment services are reliant on the robust internet protocol, a payer has no use of the payment service without internet access. For the same reasons the packet-switched internet completely replaced legacy voice circuit-switched networks in the 90s, the packet-oriented TAP will replace today's circuit-oriented online payment schemes and become the baseline of payments in the future. In addition, TAP facilitates instant settlement as well if the payment rail is open, which makes TAP ideal as the underlying protocol for payment services. A paradigm shift in payments is necessary as the current online payment schemes cannot offer the robustness required by society due to their circuit-oriented design.

The TAP header contains at least the signature of the application data using the private key of the payer. The extended application data payload may then be sent and verified at any node in the system, regardless of it is sent remotely using TCP/IP, VPN, or telecom to a host server or locally to a payment application over WiFi, LAN or in proximity.[8]

---

[8] https://www.crunchfish.com/crunchfish-enable-digital-applications-to-become-robust-trusted-and-secure/