Enabling offline payments in an online world

Privacy considerations

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.

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

Privacy considerations

INTRODUCTION

Increased payments digitalization has undoubtedly had numerous benefits for millions of people across the world. The adoption of faster and more convenient digital payment services (e.g., mobile wallets, real-time payments) has unlocked new economic opportunities and served as an engine for financial innovation in many societies. At the same time, it has led to the gradual displacement of cash, the most anonymous form of payment that exists today.

Cash is not only preferred by criminals; individuals may have a legitimate need for greater anonymity around the types of transactions they make given their personal situation or because they lack the typical documentation required to use other types of digital payment methods.[1] This raises numerous questions regarding how to best safeguard user privacy in a world that is increasingly digitalized. The demand for alternative digital payment instruments with cash-like privacy features is one of the most compelling reasons for the development of central bank digital currencies (CBDCs). In a public consultation that the ECB carried out in April 2021, a plurality of respondents considered "transaction confidentiality" to be the most important parameter in the design of the digital euro.[2]

Enhancing the privacy features of existing payment methods such as real-time payments also has numerous advantages. For example, it can help prevent the unauthorized use of consumer data in the event of a cyber-attack or data breach and can help mitigate the commercial exploitation of data without user consent. This is important as many studies have shown that privacy concerns can have a significant impact on users' willingness to use or adopt digital payment methods or services.[3]

In our last two white papers, we discussed the benefits of enabling offline capabilities from the perspective of enhanced payment system resilience, increased financial inclusion and improved user convenience and trust. In this paper, we explore another potential benefit of offline payment functionality: enhanced user privacy. We first investigate offline payments as a privacy-enhancing tool as well as the specific offline privacy models that can be explored. Second, we consider the privacy benefits of different offline payment system design choices as well as the various KYC considerations that must be weighed. We conclude with an analysis of the same six case studies we profiled in the previous two papers, with a focus on the privacy aspects of each project.

[1] https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/

[2] https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

[3] https://ieeexplore.ieee.org/abstract/document/6339927

ASSESSING TODAY'S METHODS FOR SAFEGUARDING USER PRIVACY

Over recent years, both the private and public sectors have responded to increased digitalization with new tools and strategies for safeguarding user privacy. Encryption and tokenization have become important tools for protecting user data; they serve the function of securing data that is transmitted during payment processing, thereby making it less vulnerable to criminal or commercial exploitation in the event of a cyber-attack or data breach. Tokenization has become very popular in the cards space, where tokens (a unique string of numbers or characters) are used to substitute the cardholder's Primary Account Number (PAN).[4] Services such as Apple Pay, Samsung Pay and Google Pay, etc., use tokenization for online and (contactless) in-store transactions. The fact that the PAN is not transmitted during the transaction reduces the risk that criminals, merchants and/or other third parties will be able to successfully exploit sensitive data if it is hacked or stolen. Using encryption during payment processing offers the same types of benefits, though the data transformation that occurs is reversible using a corresponding encryption key.[5]

Alongside the adoption of these technologies, the development of data privacy legislation aimed at strengthening legal protections for individuals has emerged across the globe. According to UNCTAD, 137 out of 194 countries tracked have legislation in place aimed at protecting user data.[6] Examples include the General Data Protection Regulation (GDPR) in the EU, Lei Geral de Proteçao de Dados (LGPD) in Brazil, and Thailand's Personal Data Protection Act (PDPA), to name a few. These types of legislative initiatives are another important tool in mitigating against criminal and commercial exploitation of user data and ultimately ensuring trust and adoption of digital payments.

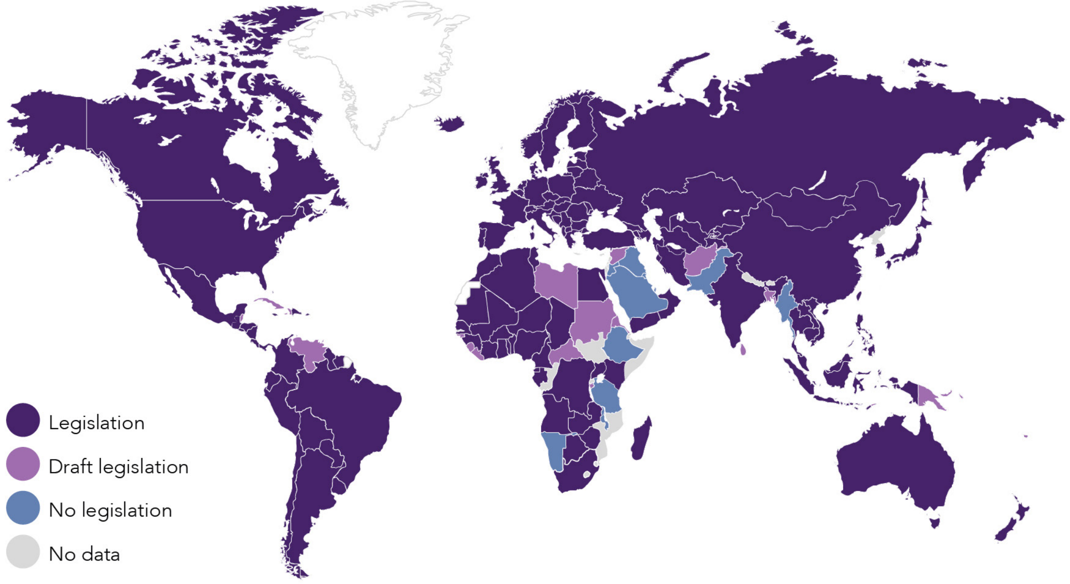

Figure 1 Data protection and privacy legislation worldwide

Source: UNCTAD

While the use of tokenization and encryption combined with better legal protections for consumers can help increase the security of user data in the hands of merchants, their benefits are limited to certain types of payments and use cases. For CBDCs, it is important to have anonymity in relation to the payment providers (e.g., system operator, intermediaries such as banks and payment service providers) as well. This underscores the need for new tools and solutions for enhancing the privacy options of existing payment instruments through innovations such as offline payments.

[4] https://www.pwc.in/industries/financial-services/fintech/dp/tokenization.html
[5] https://csrc.nist.gov/glossary/term/encryption
[6] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

OFFLINE FUNCTIONALITY AS A PRIVACY-ENHANCING TOOL

In our first white paper on offline payment system design choices, we described how offline payment implementations can vary according to different parameters such as who is offline, what type of connectivity is required (e.g., internet, non-internet, none), and the required frequency of that connectivity with the online ledger. Similarly, there are various options available to system operators, central banks, and regulators regarding the privacy features of offline payment systems. They may differ according to who has access to the information, whether the identity of the wallet holder is known, and what kind of data is reconciled with the online ledger. For example, do providers (system operator, payment service provider, etc.) and/or participants (merchants, beneficiary, and other third parties privy to a transaction) have access to the information? Is the identity of the wallet holder anonymous or is KYC required? What type of data is shared with the online ledger, i.e., transaction data vs. balance adjustments? These considerations are summarized in the visual below.

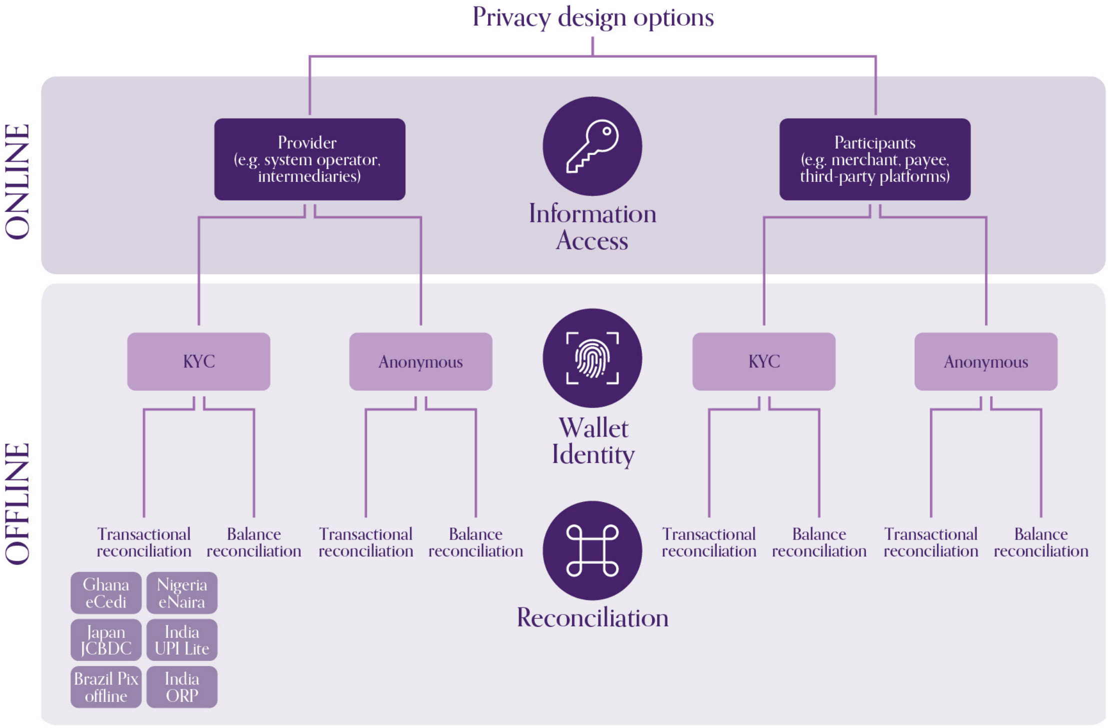

Figure 2 Privacy considerations for offline payment system design

Source: Author's elaboration

With transactional reconciliation, offline transaction data is fully shared with the system operator once connectivity with the online ledger occurs. Even though the transaction data is shared fully with the system operator, the time delay between when the offline transaction occurs and when it is shared with the system operator offers some additional privacy for the transaction. In contrast, balance reconciliation is where offline transaction data is kept off the shared online ledger, though adjustments to balances would be reflected once reconciliation with the online ledger occurs. This therefore offers greater privacy with respect to the transaction data but still a degree of transparency for the system operator. Figure 3 shows how the privacy features of different offline payment implementations can offer different levels of privacy depending on the choice of wallet design and the nature of reconciliation with the online ledger.

It should also be noted that there is also the possibility of no reconciliation with the online ledger for each of the previous cases. In a fully offline model, neither offline transaction data nor adjustments to balances are reconciled with the online ledger or a third-party. This would allow for completely anonymous payments, with cash-like user privacy. However, fully anonymous offline payments would pose numerous challenges from a compliance perspective, as even CBDCs would still need to comply with existing KYC/AML regulations. This could potentially be mitigated through the introduction of third-party service providers that could offer funding and defunding services for offline CBDC wallets. Such a model could enable greater anonymity for the user and their transactions.

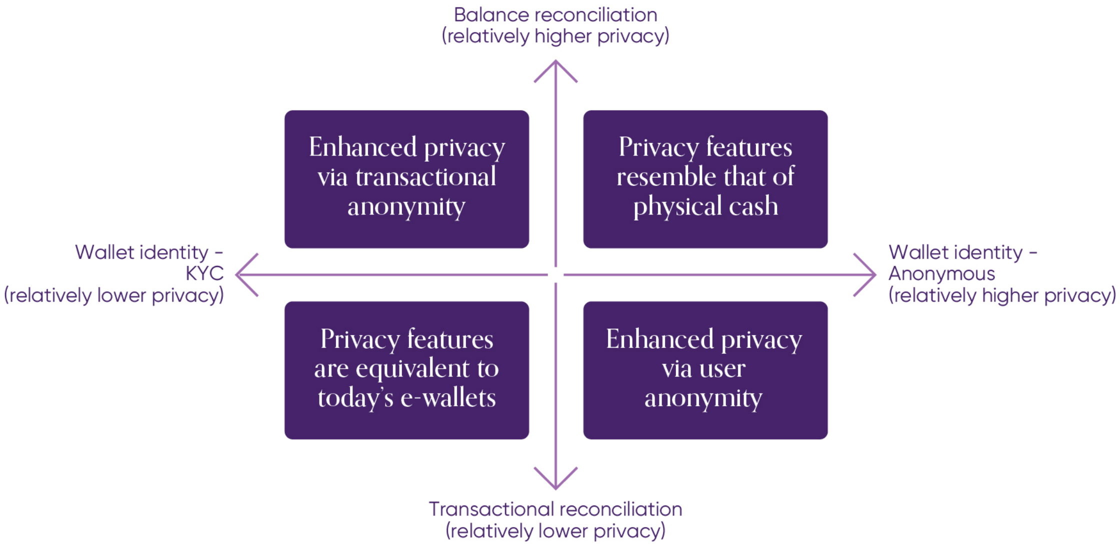
Balance reconciliation
(relatively higher privacy)
Enhanced privacy via transactional anonymity
Privacy features resemble that of physical cash
Wallet identity - KYC
(relatively lower privacy)
Wallet identity - Anonymous
(relatively higher privacy)
Privacy features are equivalent to today's e-wallets
Enhanced privacy via user anonymity
Transactional reconciliation
(relatively lower privacy)

Figure 3 Privacy features of different offline implementations

Source: Author's elaboration

DESIGN CONSIDERATIONS FOR ENHANCING THE PRIVACY OF OFFLINE PAYMENT SYSTEMS

Our analysis in the previous section illustrates the unique and novel aspects of using offline functionality to enable privacy. Specifically, it can enable a model through which the system operator or payment service provider has a more limited ability to observe users' transactional data. This can be done by restricting the type of data that is shared with the online ledger at the time of reconciliation to include only balance adjustments rather than transaction-level data.

However, from the perspective of the system operator, achieving greater levels of privacy for offline payments inevitably results in trade-offs, such as greater operational complexity and higher costs resulting from the increased amount of data that must be secured.[7] This underscores the need for smart design choices that maximize efficiency and scalability. There are a range of design choices that can support the various privacy implementations available for offline payments. In our previous two white papers, we detailed the three most relevant aspects of offline payment system design: the online payment rail (account-based or token based), security protocol (native layer-1 or non-native layer-2), and trusted environment (hardware- or software-based). In this section, we consider how the choice of security protocol can impact the privacy features of offline payments.

The purpose of the offline security protocol is to preserve the integrity of the payer as well as the offline payment data to prevent double-spending and protect sensitive data.[8] A native

[7] https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/#:~:text=Privacy%20in%20a%20CBDC%20goes,requires%20consultation%20with%20external%20parties.

[8] https://www.crunchfish.com/wp-content/uploads/2023/03/Lipis_WP2_Crunchfish_Enabling-offline-payments_FINAL_.pdf

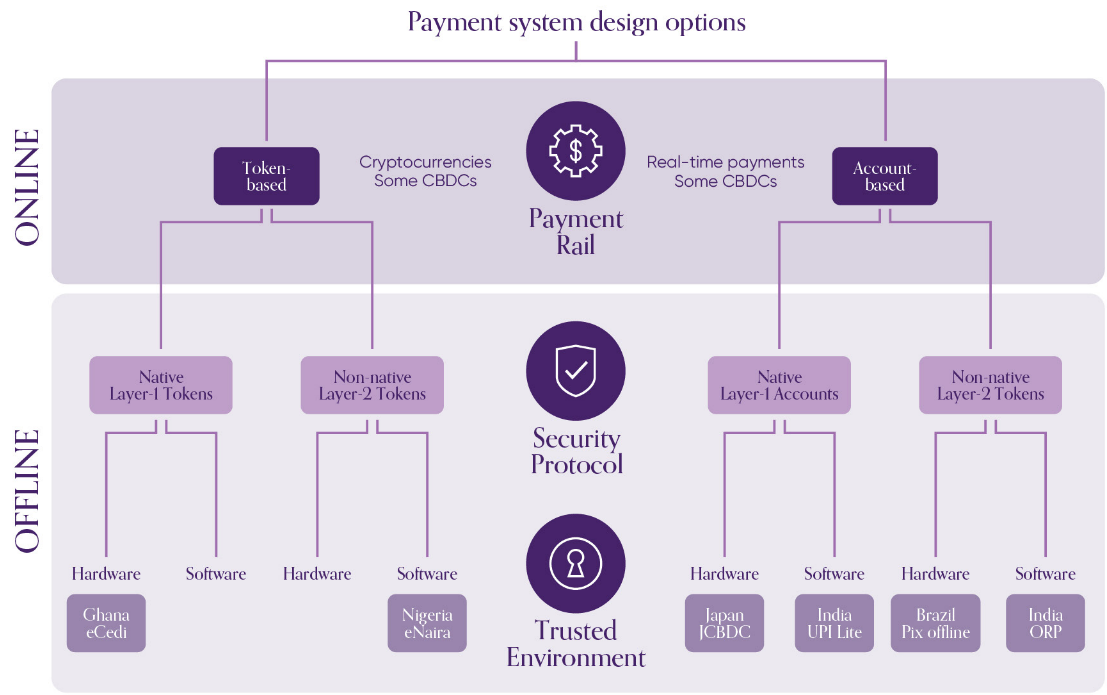

Figure 4 Payment system design options: An offline perspective

Source: Author's elaboration

layer-1 security protocol for offline payment systems is defined as one that uses the same security protocol as the underlying online payment rail; in contrast, a native layer-2 security protocol uses as a separate scheme from the online rail. The choice of security protocol is a highly relevant design choice that will impact the privacy features of the offline payment system. In building an offline payment system designed to complement an account-based online rail, for example, a layer-1 offline protocol may limit privacy from the system operator as offline transactions would be subjected to the same degree of transparency as the online transactions. In contrast, offline payments based on a non-native layer-2 protocol would potentially allow for greater privacy for users given that the security protocol is separate from the online payment scheme. In this instance, the level of privacy would be comparable to withdrawing money from an ATM; the sender signs out funds through the debiting of a locally held offline balance. Only adjustments to balances are reflected on the online ledger.

BALANCING ENHANCED PRIVACY WITH THE NEED FOR REGULATORY TRANSPARENCY AND KYC

While it is certain that offline functionality can offer some enhanced privacy benefits depending on the type of implementation, it must also be balanced against other needs, such as the need to mitigate against fraud risks.[9] Typically, stricter frameworks for KYC can be associated with lower privacy levels while higher levels of privacy can be associated with less strict KYC requirements. In nearly all markets, this trade-off is determined by the need to comply with existing regulations covering KYC as well as other areas such as Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF), which usually involve collecting and verifying information about the identity of the parties involved in a transaction. While privacy features can help protect the confidentiality of this information, it does not negate the need to comply with the existing legal

[9] Refer to the second white paper in the series "*Enabling offline payments in an online world: a practical guide to offline payment security*" for a deep dive into the security risks and mitigation techniques for offline payments.

framework, particularly for real-time payment systems. In the debate around the appropriate degree of privacy for CBDCs, regulators and payment system operators around the world have been inclined toward tiered KYC models with restrictions to prevent criminal exploitation and misuse, which is also likely to apply for offline use. For instance, an offline wallet may be subject to caps on the value of holdings or limits can be imposed on the number of consecutive offline transactions that can occur without connecting to the online ledger. Different limits for different levels of KYC compliance could also allow for some privacy flexibility, with fully KYC-compliant wallets providing the least restrictions on holdings and services.

In the case of the design of the eCedi in Ghana, the KYC regime is risk-based and provides for tiered KYC requirements for offline wallets, mostly with the aim of being accessible to the financially excluded.[10] According to the Bank of Ghana, eCedi wallets may be subject to different requirements for identification checks depending on value thresholds and daily/aggregate transaction limits, and maximum account balances will be available. While the user may have some anonymity in performing consecutive offline transactions, the fact that the onboarding for an offline wallet involves a KYC process limits the privacy benefits for the payer in this example.

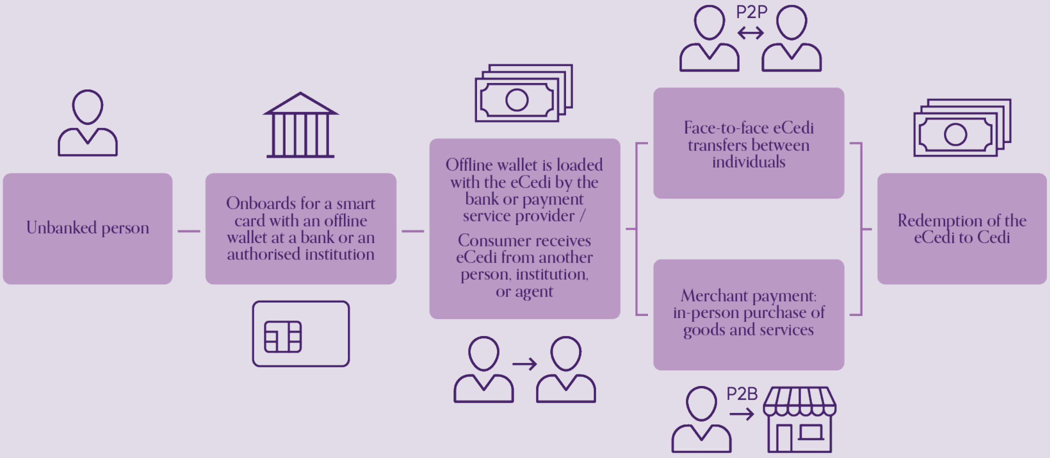
P2P
Unbanked person
Onboards for a smart card with an offline wallet at a bank or an authorised institution
Offline wallet is loaded with the eCedi by the bank or payment service provider /
Consumer receives eCedi from another person, institution, or agent
Face-to-face eCedi transfers between individuals
Merchant payment: in-person purchase of goods and services
P2B
Redemption of the eCedi to Cedi

Figure 5 Consumer journey: offline wallet on a smart card

Source: Bank of Ghana

Exploring new forms of privacy for CBDCs may also require reassessing the existing legal frameworks. In the case of a digital euro, the European Data Protection Board (EDPB) recommended developing a specific legal framework for the digital euro that would address data protection and AML/CFT aspects, having deemed that the current legal framework on electronic payments does not seem to be appropriate for a tool like the digital euro, which is likely to have different characteristics from other means of electronic payments.[11] Additionally, balance reconciliation for offline payments may offer an attractive middle ground within existing regulatory frameworks as well by providing some confidentiality around transactional data while still providing a degree of transparency to the system operator and other involved parties. How these aspects evolve will likely be a function of the regulatory and legal context of the market as well as cultural preferences and user expectations around privacy.

[10] https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf
[11] https://edpb.europa.eu/system/files/2022-10/edpb_statement_20221010_digital_euro_en.pdf

GREATER MARKET EXPERIMENTATION IS NEEDED TO BETTER UNDERSTAND THE TRADE-OFFS

In our previous two papers, we profiled six examples of market experimentation with offline payments in five markets (Brazil, Ghana, India, Japan, and Nigeria). Reflecting on our prior analysis, the area of privacy has not been the primary motivator for markets to explore offline functionality. Rather, improving financial inclusion and/or payment system resilience have been cited as the primary reasons for doing so in all these cases.

Indeed, limited public information is available regarding the specific privacy features offered in these implementations; it is presumed that they are all designed according to the concept of transactional reconciliation. All in all, this suggests that further experimentation around the potential privacy benefits of offline payments is needed. Specifically, a greater understanding of the benefits and risks of balance reconciliation is required to enhance knowledge and expertise in this area.

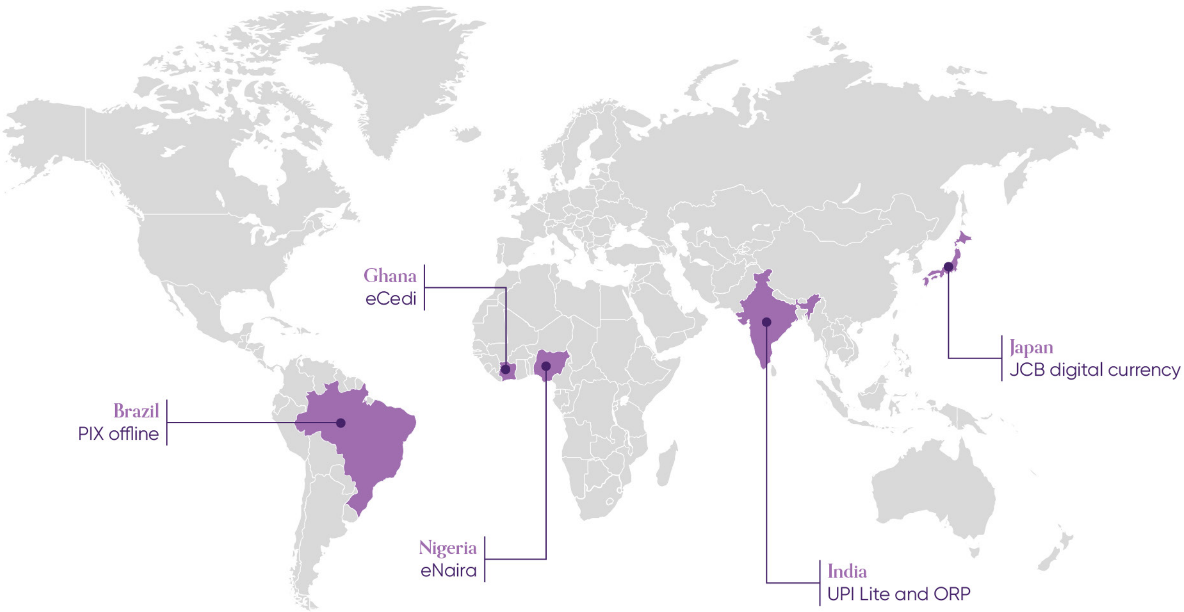

Figure 6 Selected payment systems and CBDCs exploring offline capabilities

Source: Author's elaboration

CONCLUSION

In this paper, we outlined several practical considerations for payment system operators as they navigate how offline functionality can be implemented to enhance privacy for digital payment systems. One key takeaway is that it is important that payment system operators consider how other facets of the system design (e.g., security, interoperability) interact with privacy and how these different aspects should be prioritized.

All in all, our analysis suggests that privacy is an area that has not been explored deeply by the market yet. Given the complexity of these topics and what is at stake, it is a topic that requires much greater attention and consideration.

Greater digitalization, cash displacement, and the introduction of CBDCs raise many thought-provoking questions. What role should payment market infrastructures play in safeguarding privacy? Is privacy a human right or a luxury good? Above all, it is important for payment system operators not to simply take the current privacy framework as a given and to evaluate how they can play a role as thought leaders in this area. Even though security, resilience, and trust are the core issues for payment systems, privacy is a key component of each of these. Thus, it is imperative that privacy be given more consideration now, and not before it is too late. In our next paper, we will explore another topic that deserves greater consideration in the context of offline payments: interoperability. ■