THE BIS POLARIS *OFFLINE PAYMENT WITH CBDC* REPORT

SHEDDING LIGHT ON A CRITICAL PAYMENT FUNCTIONALITY

A key debate for retail central bank digital currencies (CBDCs) revolves around whether they can meaningfully offer a compelling alternative to existing digital payment solutions, especially wallet-based ones promoted by GAFAs and other service providers in conjunction with card schemes. Indeed, these currently combine a good user experience with a high level of security through the use of tokenisation, therefore questioning the need for a CBDC alternative. However, whilst wallet-based X-pay solutions have been primarily designed to handle point-of-sale payments, they are less well suited for situations where payees have no card payment terminals, especially P2P and, to a lesser extent, P2Pro and P2MicroB interactions, therefore opening an opportunity that is targeted by the European Payment Initiative in its A2A wallet-based payment solution.

But the central question remains: is there a compelling need for retail CBDCs when good or very good payment solutions are available or under development, especially in Europe where card payments are dominant and digital payment solutions ubiquitous?

We do not claim to have the definitive answer to this important question and note that the retail CBDC debate involves several additional dimensions also coming into the equation, including for example the need to offer citizens an access to risk-free central bank money fit for the digital age, to facilitate financial inclusion and, last but probably not least, to offer payment means to non-residents and facilitate cross-border trade.

We do believe, however, that an important part of the answer lays in whether retail CBDCs handle offline interactions, i.e. whether CBDCs can be exchanged without internet connectivity, through the paring of smartphones via proximity data transfer solutions such as NFC, Bluetooth Low Energy, QR codes or other data transfer protocols. Indeed, offline connectivity greatly improves the flexibility of CBDC solutions and position CBDCs as quasi-bearer instruments and true 'digital cash' alternatives, whereas online-only CBDCs are in our view best seen as 'digital payment' alternatives.

It should therefore come as no surprise that offline connectivity is actively considered by several central banks, including of course European ones. In its fourth digital euro progress report published last July, the ECB confirmed that the online and offline functionalities will be available "*simultaneously in the first release, with offline transactions settled directly between users' devices using "secure hardware"*". On the other hand, the Bank of England appears to take a more measured approach by viewing offline connectivity as an "additional CBDC functionality" and simply stating that "*the CBDC system might enable offline payments*" (February 2023 Digital Pound Technology Working Paper)

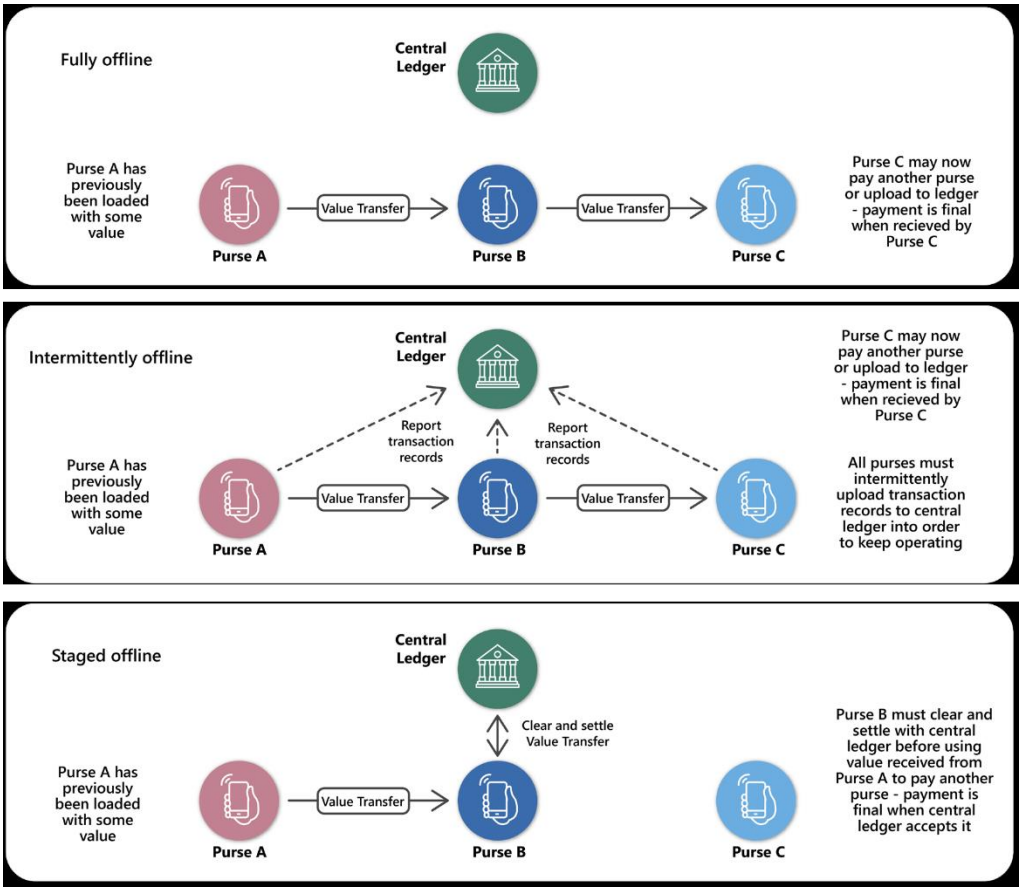
But offline connectivity, whilst certainly attractive from an end-user perspective, is a complex subject fraught with technical difficulties in view of its technology-discriminating status – it supports certain technologies and standards but is more difficult to reconcile with others, including for example blockchain and other distributed ledger technologies. This makes the '*Offline payments with CBDC*' Polaris Project undertaken by the BIS Innovation Hub Nordic Centre all the more relevant, leading the recent publication of the Handbook for offline payments with CBDC, a must-read for anyone interested in this key payment functionality. Although aiming at central banks for the implementation of CBDC projects, it is clearly relevant for other digital payment contexts, such as those offered by payment wallets, including the forthcoming European Digital Identity wallets aiming to offer a digital finance functionality as well as support offline connectivity.

The BIS Polaris report first confirms that offline connectivity is viewed by half of central banks as vital, with the other half considering it advantageous, a not so surprising result in view of its many benefits. Indeed, offline connectivity offers resilience – users are not dependent on internet availability or digital payment systems to settle payments and can still transact in situations of network disruptions – but can also bring enhanced privacy and cash resemblance as well as act as a key tool for financial inclusion and universal access to cash-like solutions. For these reasons, we believe the potential of offline connectivity is greatest for P2P and P2MicroB transactions, which incidentally are today underserviced due, inter alia, to the lack of a truly pan-European solution.

Whilst clearly advantageous to CBDC users and relevant to central banks, offline transactions no doubt remain a challenge for CBDCs, as illustrated by the Bank of England Digital Pound technology working paper highlighting that they "*pose a range of technological, operational, policy and legal challenges, including liability for any failed or fraudulent transactions while offline*" as well as the need for "*Verifiable authenticity controls for offline transactions [which] are essential to reduce the risk of counterfeit CBDC, double spending and other forms of fraud*."

Clarifying 3 mains forms of offline transactions

The BIS Polaris report offers an important clarification of the various offline functionalities by distinguishing when settlement occurs offline and value is immediately transferred to the payee ('full offline' and 'intermittent offline') and when value is only transmitted when the payee connects online to the ledger system ('staged offline'). In Full offline mode, there is potentially no limit to the sequence of offline transactions, raising the possibility that they may never be reconciled with the central CBDC ledger. The following graph illustrates the categories:



BIS *Offline payment with CBDC* Polaris Report – May 2023

The Staged offline version is probably simpler to implement as settlement only occurs online but prevents the payee from immediately reusing the funds offline and appears similar to a digital cheque written by the payer, directly cashed with the central bank once the payee is online. It is not immediately clear whether that option will prove attractive enough to be implemented as it brings no obvious benefits when compared to a standard instant payment account to account transfer. On the other hand, it may still prove a viable proposition for partial offline situations when payers are offline but payees are online, as is usually the case for point-of-sale payments. Note however that it appears ruled out by the ECB in its fourth progress report (footnote 34 : "[offline] *transactions are settled immediately between devices to align with the legal tender status*").

At the other end of the spectrum, the full offline version assumes that offline transactions may never be reconciled with the central ledger, a situation that, as highlighted by the Bank of England, increases 'double spend risk', i.e. the risk that the same funds could be spent more than once but also makes dealing with contingencies, notably the loss, destruction or theft of the mobile device problematic for end-users. In those situations, how can a legitimate holder of CBDC have value restored, which we believe will in practice be a 'must-have' functionality for mass deployment, if the central ledger (or for that matter any third party) has no information about the CBDC value held by that person?

This leaves the Intermittent offline model as a more realistic approach for CBDC implementation, although a number of questions remain, such as which risk minimisation (offline limits) and risk detections (transaction recording) parameters should be deployed in order to keep counterfeit, double-spending and other risks under control. A related topic is, when consecutive offline payments are made, whether a record of previous offline transactions should be passed along with each new offline transaction (transaction history), which we believe will be needed to minimise risks but may have to be reconciled with privacy requirements.

A related question is whether CBDCs can, in addition to smartphones, be stored into plastic cards (the so-called "hardware CBDC wallets" option contemplated by the PBOC in China). Whilst the answer is most likely positive and cards are today used in offline (NFC) mode routinely, the limited data that can be transmitted via an NFC 'tap' may likely prevent the transmission of transaction history, thus ruling out the "Intermittently Offline" option. By contrast, the "Staged Offline" mode without the need to support history may well be able to utilise existing EMV protocols, which would be well suited for card interactions, including contactless 'tap and go' payments.

The need for a truly secure 'secure element' for offline interactions

Offline payments, especially when value is transferred immediately, imply that the mobile devices used for the payments are secure enough, a topic considered in some detail in the BIS Polaris report. As stated in the report: *The ability of user devices to protect data stored in purses is critical for offline payment solutions. Any solution will depend on the tamper resistance of the user device to protect against physical and cyber-attacks*. In practical terms, given that the use of external hardware or tokens is unrealistic for mass retail use, this implies relying on the so-called 'secure element' of the smartphones, i.e. a dedicated chip that is, by design, protected from unauthorised access and runs a limited set of applications as well as store confidential and cryptographic data, similar in this respect to those found in EMV payment cards.

Whilst secure elements are not yet available on all smartphones, they are increasingly common and already found in many devices sold to the public. It is also possible, indeed likely, that the announcement of the digital euro or other CBCD in Europe requiring a secure element on smartphones would make them a standard feature of new mobile devices.

As already mentioned, the fourth digital euro progress report refers to the need to use 'secure hardware' to settle digital euro payment transactions, a looser term that includes secure elements and may also possibly refer to so-called *Trusted Execution Environments* of smartphones that are secure enclaves within the main processor guaranteeing confidentiality and integrity of code and data loaded inside. Trusted Execution Environments are more common but less tamper-resistant than secure elements.

A related aspect is that secure elements are 'limited purpose' environment and primarily designed to keep cryptographic private keys safe. Whilst keeping the master cryptographic keys protecting payment and authentication processes safe is indeed vital, it is not obvious to us that all other CBDC data can or indeed should be located in secure elements, as appears to be suggested by the BIS Polaris report.

Strong User Authentication – the embedded option

The role of the secure element is not limited to ensuring that CBDC holdings are protected but also involves authentication, ensuring that the person having access to the CBDC holdings is the legitimate user of the mobile device, so that, for example, if the smartphone is lost and subsequently found by a third party, the finder should not be able to make a payment with it.

As for other payment situations, authentication is therefore a key requirement for CBDC interactions but the difference is that in offline interactions, authentication can only be device-embedded, i.e. cannot rely on a third party, as is the currently case with 'authentication by redirection' involving banks (account servicing payment service providers – ASPSPs in PSD2 terminology). Indeed, as the payer has no internet access, authentication, including two-factor authentication required for payments under the PDS2, must rely on the mobile device in order to be implemented. This can be done in a tamper-proof manner when the authentication process uses cryptographic keys located in the secure element of the smartphone.

But authentication does not stop with the wallet user and also involves the other party to the CBCD interaction, especially when acting as payee. This is where mutual authentication comes into play, and in our view should be a standard feature of all CBDC payment interactions, especially for P2P interactions where 'knowing who one is dealing with' must be seen as a key requirement. Contrary to what happens to point-of-sale card payments implementing on-sided authentication (only the card is authenticated by the payment terminal), the BIS Polaris report recognised "*mutual authentication through tamper-resistant purses and cryptographic protocols [as an] enduring requirement*". This is certainly welcome.

Conclusion

The BIS Polaris report brings an extremely valuable contribution to the offline functionality that we view as critical for CBDC deployment but remained in the shadows of CBDC developments. It illustrates that central bank policymakers will need to choose between fully offline and intermittent offline depending on whether they are prepared to allow offline CBDC payments greater anonymity. If, as we suspect, the answer is negative, the intermittent offline model appears as the only realistic solution to facilitate the recording of offline transactions on the central ledger.

Whilst not addressing all offline-related topics nor providing all answers, the BIS Polaris report's relevance and importance cannot be underestimated and extend far beyond the CBDC environment, especially considering the practical importance of offline (non-CBDC) payments today as well as the contemplated development of payment-enabling identity wallets.

Michael Adams **Stéphane MOUY**

Michael is the founder and managing director of Quali-Sign, a consultancy firm focusing on wallet-based e-signature solutions.
Stéphane is the founder and president of SGM Consulting, a consultancy firm focusing on eIDs, eKYC and digital financial services.