Quali-Sign
Specialists in mobile apps for eID and Strong Customer Authentication

SGM CONSULTING
Digital transition expertise for financial services

Michael Adams

Stéphane Mouy

RETAIL CBDCs - DIGITAL CASH FOR WHAT PURPOSE?

The use of retail digital currencies (CBDCs) as digitised cash heralds a structural shift towards decentralised payment interactions but should not obscure the central question of its benefits for users in an already crowded digital payments landscape.

As is well known, digital currencies are the subject of investigations by central banks. Both the ECB and the Bank of England are currently focusing on *retail* rather than *wholesale* use cases. This may seem illogical, as European citizens already have diversified and efficient digital payment methods, but it is a response to the gradual erosion of cash's position in retail payments, which is more marked in the Nordic countries than in the rest of Europe. If left to the market, this development could eventually lead to the marginalisation of central bank money in trade and the emergence of alternative payment solutions provided by private players. Additionally, in the longer term, the role that CBDCs could play in the internationalisation of currencies - like the e-Yuan in China's alternative strategy to the dollar - draws attention to their geopolitical dimension in an environment marked by growing tensions. In short, there are objective reasons why central banks are interested in retail CBDCs.

Banknotes and coins: lasting advantages and growing disadvantages

Although banknotes and coins have undeniable advantages linked to their status as legally protected bearer instruments (legal tender) and remain relevant in many situations because of their ease of use. These advantages should not overshadow characteristics that are increasingly out of step with the uses and needs of economic actors faced with the accelerated digitisation of their interactions.

-The first is the intrinsic anonymity of cash payments, which is favourable to illicit uses. In addition to this aspect, to which the public authorities are trying to respond by limiting their use for many payments, there are risks of loss and significant handling costs for economic agents, not to mention the health risks in times of pandemics;

-The second is the difficulty and cost of reconciling cash balances with economic flows, which require laborious physical counting;

- Finally, while cash is easy to carry, in practice it involves face-to-face contact and is unsuitable for remote exchanges.

Retail CBDCs: like cash... in a wallet

While retail CBDCs have real kinship with banknotes and coins (direct debt to the issuing institution, inclusion in M0, priority distribution to retail customers via financial intermediaries, and even legal tender), structural differences mean that they will not be a direct substitute for banknotes. The latter are still marked by specific physical and legal characteristics and cater for particular needs, for example, of people with low digital literacy or non-residents. The most likely scenario is therefore that of the coexistence of cash and CBDCs over time, although it is not possible to predict at this stage how quickly CBDCs might supplant cash in payment uses.

In China, where the deployment of the e-yuan is a tangible reality however still its pilot phase, it is available in dedicated payment cards (*hard wallets*) or in smartphone applications (*digital wallets*). The latter format seems to be the one considered as a priority in Europe, where it will compete with other mobile payment solutions,

including of course the X-Pay solutions promoted by major digital players and banking or electronic money applications. To complete the picture, we should also note the forthcoming arrival of digital identity wallets, which will also cover payment authorisation use cases. In short, payment wallets are already deployed and are not waiting for the arrival of retail CBDCs, which are still uncertain in Europe.

A CBDC wallet will therefore have to find its place in a host structure (e.g., mobile terminal/device) by offering a differentiating service to its users. Within this environment, user experience is key and the challenges facing the introduction of CBDC are real and important.

What is the value proposition for users?

As we have seen, the introduction of retail CBDCs addresses legitimate concerns of central banks. But is this enough to guarantee their success? In fact, their deployment will take place in an environment already containing numerous electronic payment solutions: cards, transfers and direct debit authorisations, electronic money, instant payments, etc. In a world where X-pay solutions already offer an accomplished point-of-sale experience on a mobile terminal, what will be the key proposition of a retail CBDC for users that would enable it to position itself as a relevant payment alternative? User adoption remains an essential condition for success, also it is hard to see how a CBDC that does not meet the real expectations of economic agents could prosper. If there are no decisive use cases and if the economic model for distributing and managing CBDCs has not been stabilised, success is anything but guaranteed.

In this context, we believe that CBDC users will prefer to manage their digital payment methods from a common mobile application or process rather than ones dedicated to each payment method. In the same way that merchants will include CBDCs as one payment option among others, CBDC users will prefer to manage them as a simple alternative to other payment solutions available within their wallet. For this to be possible, CBDCs will have to share a common interaction protocol (online and offline) with that applicable to instant or card payments.

But whatever the choice of user interface, CBDCs will need to offer ease of use that is comparable to that of cash and, in order to secure buy-in, far superior to existing digital interactions.

Offline mode and its challenges

Cash settlements obviously do not require an internet connection and the same should be true for CBDC settlements, as is the case in China with the e-yuan. In practice, the offline mode of wallets implements proximity exchange protocols (based on QR Code, NFC, Bluetooth and soon ultra-wideband) and implies, for retail CBDCs, an immediate and final transfer for the parties involved – implementing the principle of finality of payments.

While offline mode may seem anecdotal, we believe that it is crucial, and it is difficult to see the point of a retail CBDC that does not manage offline mode. Without an offline capability, what would be its attraction when competing with payment wallets that already operate offline or instant credit transfers which will be widely available within existing wallets or banking applications?

In addition to allowing localized settlements on wallets, the offline mode offers decisive advantages in white or poorly connected areas (basements, car parks, etc.), where speed of interaction is essential (points of sale, large events, etc.) but also in interactions between individuals. Moreover, while the Ukrainian context shows to what extent the resilience of networks is essential in times of conflict, offline mode offers appreciable additional flexibility.

Indeed, the offline mode opens up a new perspective for electronic payments - beyond the reach of card or credit transfer payment schemes - by allowing the offline credited party of CBDCs to reuse funds received immediately

offline and without waiting for the payments to be recorded on the books of the issuing central bank. In practice, this approach implements a decentralised settlement architecture with deferred reconciliation on the books of the issuing institutions.

Digital cash better than real cash?

If they aim to go beyond traditional payment schemes, can CBDCs offer more than cash? The situation that comes to mind is the recovery of CBDCs in case of failure, loss or theft of the mobile device. Unlike banknotes, where loss or theft is usually permanent, CBDC management schemes will need to allow for the recovery of recorded balances. It is difficult to see how it could be otherwise, given that users' confidence in wallets whose technical operation they are unaware of implies a mechanism guaranteeing the continuity of CBDC holdings in the event of failure or loss of the user's mobile terminal.

The possibility of recovering one's CBDC assets in the event of the loss of a wallet, which appears to us a key requirement for its distribution to, and acceptance by, a wide public, nevertheless has profound implications for the architectures for implementing CBDCs. Indeed, this implies a so-called '*account-based*' schemes in which each exchange of CBDCs is *ultimately* recorded in a central register managed at least in part by the central bank and which entries make it possible, if necessary, to determine the CBDC assets linked to each wallet. The other option generally considered, based on anonymous tokens whose exchanges depend solely on the knowledge of private cryptographic keys, poses real problems of consistency with AML/CFT rules and does not seem to us to be able to respond satisfactorily to situations where a wallet is lost.

Europeans are aspiring to a high level of personal data protection, a concern reinforced by the comparison between retail CBDCs and banknotes, for which the confidentiality of payment interactions is absolute.

Privacy: a political issue at the heart of technical issues

In practice, an *account-based scheme* implies a central registry that identifies, directly or indirectly via financial providers, the CBDC holdings of each wallet and is fed with information on CBDC exchanges when the wallet is online. This raises the question of the information that should be communicated and the level of protection of personal data offered in the context of CBDC interactions.

Europeans are aspiring to a high level of personal data protection, a concern that is reinforced by the comparison between CBDCs and banknotes, for which exchanges are completely confidential. In fact, if retail CBDCs are intended to serve as a digital substitute for cash, for which no information on exchanges between economic agents is reported to the issuing institution, then the level of privacy should logically be as high as possible. However, it should be noted that this comparison downplays the numerous legal restrictions on cash payments, designed to prevent their use for money laundering or terrorist financing purposes.

But how can this privacy be organised in practice while preserving the possibility of reconstituting CBDC assets in the event of the loss of smartphones? The debate is still open and has not yet settled on a consensus solution.

One solution that is regularly mentioned is to set limits (on transactions and/or holdings of CBDCs), below which data confidentiality would be total or very significant. While this solution is technically possible, it does not completely solve the problem. If I lose my mobile device with which I manage my CBDCs, the fact that I can recover them implies the possibility of linking them to my wallet and my wallet to my civil identity.

Digital identity wallets: a solution for CBDCs

The forthcoming arrival of digital identity wallets could offer a relevant solution, by ensuring the link between wallet and civil identity with a high level of assurance, without having to go through a third party and while guaranteeing a high level of privacy. These wallets aim to allow the communication of identity attributes and other certified attributes, but also to authenticate the parties in such a way as to guarantee that each of them is in a close or online relationship with the person they claim to be. Furthermore, by applying relatively simple privacy protection techniques based on data minimisation and pseudonymisation, it is possible to limit the information exchanged and to decorrelate the uses between counterparties to enhance privacy and avoid surveillance of digital interactions.

These considerations explain the interest in digital identity wallets, especially when they are based on a local (internal to the smartphone) storage scheme of identity data allowing information to be shared both online and offline under enhanced security conditions, i.e. with a high level of assurance.

We are not there yet and many aspects remain to be clarified, in particular, at the technical level, the conditions of use of the offline mode and the possibility of accessing the *Secure Elements* of mobile phones to allow secure interactions. These issues are currently considered during discussions on the implementation of eIDAS 2.0 digital identity wallets and the related payment use case.

In the long term, the horizon that is emerging could therefore be that of a convergence between identity and digital payments within wallets to meet the challenge of digitalising payment interactions under acceptable conditions of privacy and based on local and decentralised schemes and architectures. There is no doubt that it will bring major innovations that are still difficult to imagine today.

The French language version of this article was published in the January 2023 edition of *Revue Banque* – click on logo

---

In need of more information? Feel free to contact us:

Michael Adams
Michael_adams@quali-sign.com

Stéphane Mouy
sgmouy@sgmconsultingservices.com

03 January 2023