ALLURING BUT RISKY

ARE CASH-LIKE OFFLINE DIGITAL EUROS WORTH THE GAMBLE?

Stéphane Mouy (SGM Consulting) and Michael Adams (Quali-Sign)

Whereas the European Parliament has recently advocated the offline use case of digital euros through the issuance of non-ledger tokens, in effect bearer-like instruments offering a 'cash-like level of privacy' which can be stored and exchanged without relying on internet connectivity, the ECB and EU Council have taken a more nuanced position but not clarified what offline digital euros would entail. The purpose of the article is to consider the options available and the role that could be played by the forthcoming European Digital Identity Wallets in digital euro interactions. Whilst the authors agree that strong privacy is desirable, they take the view that implementing a non-ledger approach is fraught with considerable difficulties and reconciling full privacy with other legitimate priorities may be too great a challenge, especially if offline digital euros are treated as bearer payment instruments.

The retail digital euro proposal has faced significant criticism from the financial sector with one of the main contentions being that it would offer unclear added value when compared with existing private solutions and effectively commit taxpayers' money to unfairly compete with them. The point has been noted by the European Parliament in its 3rd November draft report advocating an offline digital euro that would guarantee continued access to central bank money in the digital era without competing with the private sector and not entail risks of bank disintermediation or have a negative impact on the financing capacity of European businesses or households.

> *"the offline digital euro is understood as a tokenised version of cash, not account-based, but operating through "device-to-device" payments. It guarantees privacy, resilience, and universal accessibility even in times of network failure or crisis. Stored and transferred locally on secure devices, it preserves the right of citizens to hold central-bank money in all circumstances. In short: digital cash."* *(explanatory statement)*

Could a cash-like offline digital euro indeed be a valuable solution? But, first, what is contemplated by an "offline payment" and what is or rather could be an "offline digital euro"?

An offline payment can generally be construed as a transfer of value between devices that takes place without requiring connection to any ledger system. In its simpler form, it implements a mutual agreement between payer and beneficiary to irrevocably transfer value with settlement depending on online connection – think of a digital cheque presented for payment when one of the parties gets online – whereas more elaborate approaches imply that the beneficiary is immediately credited with digital euros whilst both parties are still offline – similar to what happens in cash interactions. A defining aspect is that there is usually no reliance on the internet but on proximity communication protocols such as near-field communication (NFC) or, alternatively, Bluetooth Low Energy (BLE) or quick response (QR) codes, hence the fact that offline interactions usually imply physical proximity between payer and payee, as is the case for cash interactions.

Various CBDC offline variants are presented and discussed in the 2023 BIS Project Polaris report – A handbook for offline payments with CBDC outlining three main offline alternatives ('Fully offline', 'Intermittently offline' and 'Staged offline') all allowing offline irrevocable payment consents but with two of them – Fully offline and Intermittently offline - in addition implementing offline value transfers (i.e. final settlement occurs offline). These will be considered further in the second part of this article.

PART 1 – THE CASH-LIKE FULLY OFFLINE (NON-LEDGER) APPROACH – GREAT PROMISE, HUGE CHALLENGE

All for the 'fully offline' model - The EU Parliament's and ECB advocate a token-based non-ledger approach for digital cash

As stated earlier, the EU Parliament report refers to "*the offline digital euro […] understood as a tokenised version of cash, not account-based, but operating through "device-to-device" payments*". This echoes the position taken by the ECB in its latest digital euro progress report confirming that, for the offline functionality "*Payments would be settled directly between two devices (such as mobile phones or smart cards) by the near-instantaneous transfer of cryptographically secure tokens. The transfer would not involve any online system – a key innovation that does not yet exist in the market – and tokens would remain securely on the device*" (30th October 2025 progress report).

The exclusion of account-based approaches implies that no payment details are recorded by banks, payment service providers or central banks – highlighting the focus on full privacy for offline interactions, just like for cash. This implements a fully offline approach as defined by the BIS Polaris report or a '*non-ledger electronic cash'* framework as discussed in the *Technical Examination of Non-Ledger-Based Payment Systems*, IMES - Institute for Monetary and Economic Studies Bank of Japan – see figure 1.

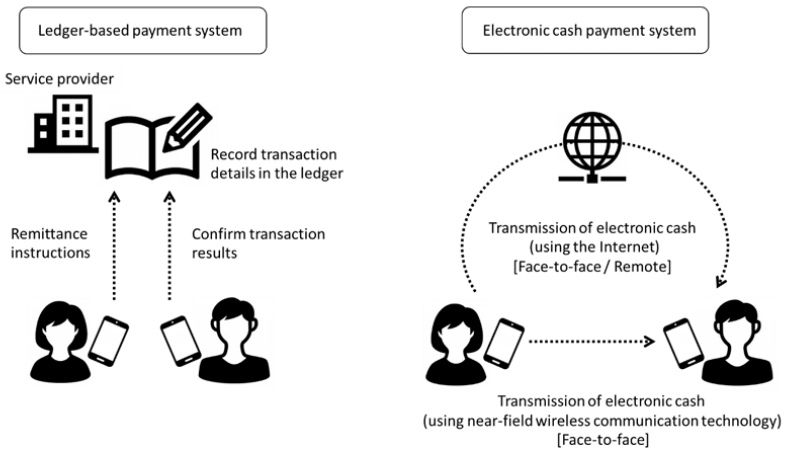


Figure 1: Comparison of ledger-based payment system and electronic cash payment system

It should als
cash) payment systems in that, in a non-ledger (e-cash) payment system, the proof of asset ownership or payment can only be derived from the wallet records and nothing else, whereas in a ledger-based system, the ledger usually is the authoritative reference – only entries on the ledger are recognized as

valid proof of asset ownership or payment (as illustrated in Figure 1 above) – but part 2 will show an alternative where the ledger just serves a back-up/reference for risk and audit purposes. Whatever option is chosen has a considerable impact on recourse provisions.

Although not directly mentioned in the Parliament's or ECB's reports, it is thought the contemplated token-based approach would make use of UTXOs (Unspent Transaction Outputs) where self-contained units of value are transferred directly between users with no history documented beyond their current money transfers. Transfers occur by 'unlocking' the UTXOs with the user's private key. Whilst not completely assimilable to bearer instruments for which 'who holds, owns and can enforce' and where legal entitlement flows from possession, in a token-based approach, whoever controls the private key is in practice able to exercise ownership rights over the tokens. Physical possession (for banknotes and coins) is replaced by its digital equivalent (control of the private keys). Another important aspect is that token transfers are final, non-reversible and without recourse. They cannot practically (and, it is thought, legally) be revoked and once implemented, the recipient of the new token value is deemed a bona fide owner, enjoys all attributes of ownership and can retransfer at will the value received, which we see as a matter of structural importance.

Privacy as a core requirement

The European Parliament and ECB have in mind a token-based, non-ledger approach for offline digital euros offering the highest level of privacy to European citizens. The focus on privacy is prominent in both the Parliament draft report and ECB Progress report and appears to be a key deciding factor in the choice of technical implementation solution. To quote the ECB:

> *"Key areas of work included the design of the offline functionality – a crucial innovation allowing payments to be made even when internet connectivity is lost, thus making the European payment landscape even more resilient* ***and providing a cash-like level of privacy****"*

Privacy is a major plus and, needless to say, a key attraction of cash, although not always for legitimate reasons. And indeed, privacy is an embedded feature of digital token for which transfers are not recorded in a public or central ledger, bear no transaction history and offer the highest level of anonymity, second to none when it comes to digital instruments. However, unfettered anonymity is an illusion as there will always be wider privacy limitation guidelines for payment interactions, in the same way that cash payments are today subject to numerous usage limits. So privacy will in any event have to be balanced with, notably, AML/CFT requirements in order to offer a level playing field with other payment instruments. We therefore expect that storage and possibly transactional limits will be set by the ECB. Setting those at too low a level will reduce the interest of digital euros, especially if the ECB maintains a strictly 'offline-use-case-only' policy for token-based euros.

We note that less-privacy intensive solutions offering many of the benefits of offline interactions also exist – these will be discussed in the second part of this article. We are in favor of privacy, which we see as inherently desirable for private-sector interactions, but as will become clearer later, believe that the focus on 'cash-like levels of privacy' will in effect conflict with other legitimate policy objectives and bring too high a price for a payment scheme aiming at mass distribution.

1.1 THE GREAT APPEAL OF A CASH-LIKE OFFLINE DIGITAL EURO

Beyond privacy, let us consider the other pluses of fully offline, token-based digital euros, which are undeniable and clearly relevant when considered from the central bank or users' perspectives.

First and foremost, **cash resemblance**. Offline payments mimic cash payments and are very flexible in that they can be implemented "anywhere, anytime" without any network dependency. They are also opening up the person-to-person (P2P) use case of great relevance to European citizens' daily lives and until recently underserved by digital payments solutions. The same applies to micro and small businesses or professionals, which can offer services at very low cost and without all the constraints and risks of handling cash amounts. So not only would an offline digital euro emulate the experience offered by cash interactions, but improve on them by offering more security.

Resilience is also a key factor. As its very name indicates, an offline digital euro does not depend on internet connectivity, implements instead a proximity communication protocol (usually NFC and possibly BLE or QR code) allowing direct interactions between wallets and can therefore be used in white zones, in crowded environments or during power outages – situations once viewed as marginally relevant in Europe where network coverage is extensive but taking new relevance in an increasingly volatile geopolitical environment.

Other factors are also mentioned, such as **financial inclusion**, when individuals are unable to access payments using mainstream options and **lower transaction costs**, which can be a significant financial burden on micro-businesses. Whilst often mentioned as additional benefits of cash-like digital interactions, quantifying them meaningfully today appears difficult and is fraught with uncertainty.

Even better than cash?

But not only would a fully offline digital euro be bringing many of the benefits of cash into the digital sphere, it could also offer additional services currently impossible with cash transactions. The first one that comes to mind is the proximity limitation inherent to cash interactions. Indeed, a token-based approach can support proximity interactions but does not require proximity and can equally support online (i.e. remote) interactions. This implies that, at least in theory, a token-based digital euro could be used between parties based in different locations, including different countries. a perspective which would potentially bring lower transactional costs and greatly facilitate cross-border remittances but also blur the distinction between an offline and an online digital euro. We are aware that the possibility is considered with caution by the ECB and that it would prefer to maintain a token-based approach to proximity offline interactions but the potential remains and may be of interest to central banks.

The other aspect where a fully offline digital euro could bring additional value compared to cash is with respect to security, i.e. protection from theft. It's a truism that cash, if unattended, is at great risk and one of the benefits of digital wallet interactions is that user-binding mechanisms available with mobile devices can be used to protect access to digital euros stored in them. We will see later that this protection is not absolute and should therefore not be overestimated, but it does indeed offer a valuable line of defense against a range of low to medium severity threats.

Lastly, an offline digital euro would offer services that are not today available with private-sector payment solutions. As mentioned earlier, this appears to be a deciding factor in the European Parliament's report to promote an offline digital euro that does not create an uneven playing field for payment solutions by committing public funds to one competing solution.

1.2 A NON-LEDGER, FULLY OFFLINE SOLUTION ALSO BRINGS CONSIDERABLE CHALLENGES

Unfortunately, the clear benefits of a fully offline token-based digital euro proposal must be related to risk factors that appear significant, indeed challenging, in our view putting a question mark over its marketability and viability. From a practical standpoint, we see three major issues that any offline solution would have to address and satisfactorily resolve.

1.2.1 An 'offline-only' digital euro?

The first issue relates to the proximity (face-to-face) requirement which is viewed by the European Parliament report as key to ensure that an offline digital euro would not directly compete with a private-sector online payment solution. As stated by Professor Tibor Jager in his expert opinion *'the Digital euro and its token-based offline modality'*, digital systems cannot "see" distance, therefore "*enforcing physical proximity in a digital currency (regardless whether online or offline) is intrinsically hard, because digital communication channels are location-agnostic*". Whilst no one is claiming that an offline-only digital euro cannot be implemented, no practical implementation has been suggested to that effect, so this remains today an untested proposal. Indeed, corralling digital bearer-like instruments into specific proximity use cases and preventing their wider online usage, including in cross-border situations, appears especially challenging. In the end, it may or may not be a problem depending on the political acceptability of token-based online interactions.

However, if an offline & online digital euro is considered, which is a possibility contemplated by the ECB, the European Council as well as the European Parliament, although in the latter case as a second-best solution, a unified online and offline approach would no doubt be preferable to two distinct ones, one for offline (and possibly online) payments, the other for online-only payments. An account-based approach for online payments and a token-based approach for offline payments would create implementation complexities as they would implement two different and non-fungible approaches for the same claims on the central bank. From a user's perspective, this raises the prospects of two different digital euro balances (one for token-based digital euros, the other for account-based digital euros) that cannot be merged and would rely on a third party's involvement in order to switch from one category to the other. Convincing European citizens of the benefits of a digital euro proposition already appears to be a challenge, especially for online payments where the value proposition compared to existing payment solutions is uncertain. Suggesting two non-fungible retail digital euros of the same monetary value, representing the same claim on the European Central Bank but with different functionalities may be a step too far. Unfortunately, this does not seem to be the approach considered by the EU Council in its 17 December 2025 Mandate for negotiations with the European Parliament on the digital euro (the EU Council Mandate document) "*The digital euro, held online or offline, shall be convertible at par between each other, at the request of the digital euro users*."

1.2.2 Your only security is your wallet – is it really safe?

The second issue has to do with the need to protect against the risks of counterfeit, i.e. a malicious actor cloning or creating 'look-alike digital euros' and distributing them to innocent victims, double-spending where a legitimate digital euro is used more than once and theft where genuine digital euros are stolen from a wallet.

Theft – stealing legitimate digital euros - poses a significant threat when applied to bearer or bearer-like instruments such as fully offline digital euros. For these, proof of asset ownership or payment can only be derived from the wallet records and there is no ledger to go back to in order to ascertain ownership. In short, protection from theft resides entirely on the devices themselves. This implies in practice that the private keys allowing digital euro transfers are very securely kept and managed.

Beyond theft issues which are mostly relevant to end users, counterfeit and double-spend are issues of great importance for central banks – trust in the value of the currency must be maintained at all cost and cannot be compromised by wallet interactions, including in the likely situation where fraudsters happen to be wallet users themselves.

Counterfeiting through the production of false banknotes is now at a historic low in Europe as modern banknote designs with advance security features make counterfeiting very challenging and less attractive compared to other fraud opportunities, especially in the digital sphere - phishing, social engineering, deepfakes and synthetic identity frauds are easier to implement and therefore now pose greater risks. It follows that mobile devices need to manage double-spending, counterfeiting and theft risks, especially considering that fraudulent schemes will involve fraudsters acting as legitimate wallet user.

This topic is being actively considered and assessed by various central banks but will likely require significant research and investment before the use case can be deployed at stage. It will most likely require smartphone secure elements that are proven to withstand most if not all anticipated attacks with a high level of confidence – no doubt a tall order. In this connection, the IMES discussion paper states that "*The security of electronic cash systems largely depends on the security of digital signatures, and as such, the use of devices capable of securely managing the private keys used for digital signatures is a prerequisite. A tamper-resistant device makes it difficult even for its legitimate owner to illicitly extract the private key stored within or to tamper with the application. This ensures that fraud, such as double-spending of electronic cash, can be prevented. However, malicious users may deliberately use non-tamper-resistant devices to commit fraud. Therefore, service providers may need to verify the tamper resistance of user devices. For example, user registration could be allowed only if the tamper resistance of the user's device is confirmed, thereby excluding users who attempt fraud*."

We expect bearer-like token security requirements to be significantly tightened for one overriding reason: once issued and distributed, central banks lose control of, and have no access to, the tokens representing their own currency and must assume that they will be tested to the full by fraudsters looking for vulnerabilities to be exploited. They are in effect 'flying blind' and cannot easily remedy any deficiency or currency tokens. This would imply, for example, that quantum-resistant public-key algorithms be used in order to defeat future attacks. Whilst the situation is arguably the same for

banknotes – once distributed, the central bank does not control their circulation – they integrate multiple security features built on decades of practice, in marked contrast to what happens with digital tokens, which can end up being stored in compromised devices (some no doubt will). In this context, the simple reliance on cryptographic technology may be viewed as an act of faith warranting extra caution.

Although there is a clear trend towards deploying secure elements, especially eSIMs, in smartphones, not all mobile devices are equipped today and, more to the point, there is currently no dedicated certification scheme available for this purpose. The ECB is considering whether "*digital euro-specific certifications would be required (e.g. for the offline solution)*" (30 October 2025 update on the work of the digital euro scheme's Rulebook Development Group) which puts a question mark over the time horizon contemplated for mass-market deployment – preparing a certification scheme is a lengthy process and only smartphones released after it becomes official would be eligible. An indication of the challenge involved can be found with the current European Digital Identity (EUDI) wallet specifications for Wallet Secure Cryptographic Devices (WSCD) and Wallet Secure Cryptographic Applications (WSCA) currently dedicated to local external devices (smartcards) or remote hardware security modules but which today do not address 'local internal' environments.

A practical yet partial solution could be considered with smartcards, i.e. 'local-external' rather than 'local-internal' (smartphone-based) hardware wallets which are clearly contemplated by the ECB as an alternative to smartphones storing token-based digital euros. However, these are likely to be seen as providing insufficient convenience and flexibility for users, especially those already using X-pay wallet applications for payments. Although data remain sketchy, e-Yuan hard wallets are deployed in China but appear limited to certain use cases (e.g. mass transit systems) or categories of users (Elderly, children, foreign tourists and migrants…).

1.2.3 Your smartphone suddenly stops working. Have you lost everything?

The third challenge is affecting users and related to 'loss' situations. It's a well-known fact that, barring special circumstances, when cash is lost for any reason, there is no way for the user to claim back his/her banknotes and coins. Avoiding losing cash usually means implementing common-sense measures that are within reach of most users, meaning that loss of cash can often be attributable to negligence or reckless behavior and may explain or justify the absence of recourse. Applying the same principle to offline digital euros should therefore not, in principle, raise significant concerns given that they are widely viewed as digital cash. Unfortunately, the implicit causality between negligence and lack of recourse becomes much less obvious for mobile devices that are complex systems-on-chips integrating dedicated subsystems (radio, sensors, storage, display, power, software, etc.), all interacting together and depending on each other in ways wholly beyond the control of smartphone users. In short, mobile devices can suddenly malfunction and prevent wallet users from accessing their digital euros. Would malfunction situations prevent wallet users from claiming their digital euros back? The compelling logic of a non-ledger token-based digital euro approach would imply a positive answer as only users' devices can give meaningful and legally enforceable evidence of their digital euro balances, meaning that when access to the relevant device data is lost, there is no back-up ledger to get to. The

second part of the article will show that this is an aspect which can be addressed in the so-called intermittently offline model, but which implies less privacy.

Requiring wallet users to take the full risk of smartphone malfunction, over which they have no control, and lose all their offline digital euros if their digital wallets cease to function for any reason may well prove difficult for the wider public and could well be a major brake on adoption at scale. In addition, there is a risk that this negative scenario could be exploited for political gain by presenting the central bank as its ultimate beneficiary of system malfunctions through one-off seigniorage gains.

1.3 A NON-LEDGER FULLY OFFLINE APPROACH: A STEP TOO FAR

A fully offline non ledger approach is the only one that can offer cash like convenience and privacy, where neither the PSPs nor the ECB have any visibility of the individual transfers between wallets. They only have visibility of funding and defunding transactions.

However, its drawbacks include:

1. everyone has to accept the payer will lose their balance if they lose their device or if it breaks – which we see as an especially difficult selling proposition, especially considering the benefit is eventually captured by the issuing central bank;
2. the need to have complete faith that technology can't be compromised, i.e. it can prevent double spend and it can enforce holding and transaction limits and it guarantees that offline digital euro transactions can only be made between two devices in proximity, again mimicking cash.

The importance of 2 cannot be underestimated as it is the only protection against AML/CFT fraud and other abuses. If the faith in technology happens to be misplaced, and someone finds now or in the future a way around the build-in limitations, there is no second line of defence and bad actors cannot be readily identified as offline payments are always off-ledger, without knowledge of either the central bank or payment service providers (banks). This makes the reliance on technology absolutely critical – if this fails or is misplaced, all protections disappear. The problem is compounded by the fact that CBDCs are deployed directly on the internet with the highest level of risk.

Indeed, whereas the double-spending protection inherent to crypto assets has proven to be reliable, at least when it comes to large, well-established crypto networks (Bitcoin, Ehtereum and the like), there is much less certainty for offline CBDC security models primarily relying on hardware trust assumptions such as smartphone secure elements.

To quote the 2025 academic research paper On the Operational Resilience of CBDC: Threats and Prospects of Formal Validation for Offline Payments" *If we compare the effects of counterfeiting between physical cash and an offline CBDC... a striking difference in the capacity to scale counterfeiting becomes evident... Once the offline CBDC system has been compromised, it is virtually possible to generate an unlimited number of tokens at a cost that is essentially zero, as the only physical resources necessary are a computer and/or smartphone*."

The problem is even worse for holding and transaction limits and the 'proximity requirement' that appears especially prone to relay attacks. To illustrate: what if it is determined that you cannot prevent

innovative solutions appearing in the marketplace that will easily overcome the proximity restrictions. Each wallet will continue to believe it is interacting with a counterparty wallet in proximity, whereas in fact they are interacting with a proxy which forwards the communication to a remote counterparty. What are the implications of this? Have we just created a highly convenient anonymous payment facility that will allow bad actors to transfer money between two wallets on opposite sides of the world?

But what about the holding and transaction limits? will these help? How do we prevent the transfer of a large sum of money via a series of smaller linked transactions designed to work within the limits? The existing AML regulations require PSPs to identify a series of linked transactions. If a digital euro wallet can be used to achieve a private transfer, then this will likely prove highly attractive to users who wish to keep these transfers private.

Lastly, what happens when someone decides the initial design is untenable and it has to change? How will this impact the design of the CBDC? The severity of these questions in our view disqualifies the non-ledger approach for CBDCs and the digital euro. The position taken by the European Parliament of the offline digital euro as a “tokenized version of cash, not account-based” is in our view untenable if it implies no ledger whatsoever.

In contrast to the European Parliament, the other European institutions involved in the digital euro debate (the EU Commission, the EU Council and ECB) have not clearly articulated a firm position regarding the use of tokens for the offline digital euro. Indeed, whilst references are made by the ECB and the European Council to the offline digital euro offering a ‘cash-like level of privacy’ through the implementation of ‘bearer payment instruments’ taking a different form than standard book entries considered for the online digital euro, the term token is conspicuously absent from recent reports and communications regarding the preparation of the offline digital euro. We assume concerns about the lack of visibility over non-ledger transactions and the implementation challenge of ensuring tamper-proof transaction and holding limits may have played a part in that position. The point is summarized in the EU Council Mandate document: “While offline digital euro payment transactions have similarities with transactions in cash and should be treated in a similar way in terms of privacy, specific holding and transaction limits for offline proximity payments are essential to mitigate AML/CFT risks.“

So, if a fully offline, non-ledger digital euro is viewed as too risky, what could be considered that would go some way towards mitigating the concerns raised? In order to assess this, let us consider the various alternatives to the fully offline model.

PART 2 – MITIGATING RISKS IMPLIES DIFFICULT CHOICES

2.1 ALTERNATIVES TO A FULLY-OFFLINE APPROACH

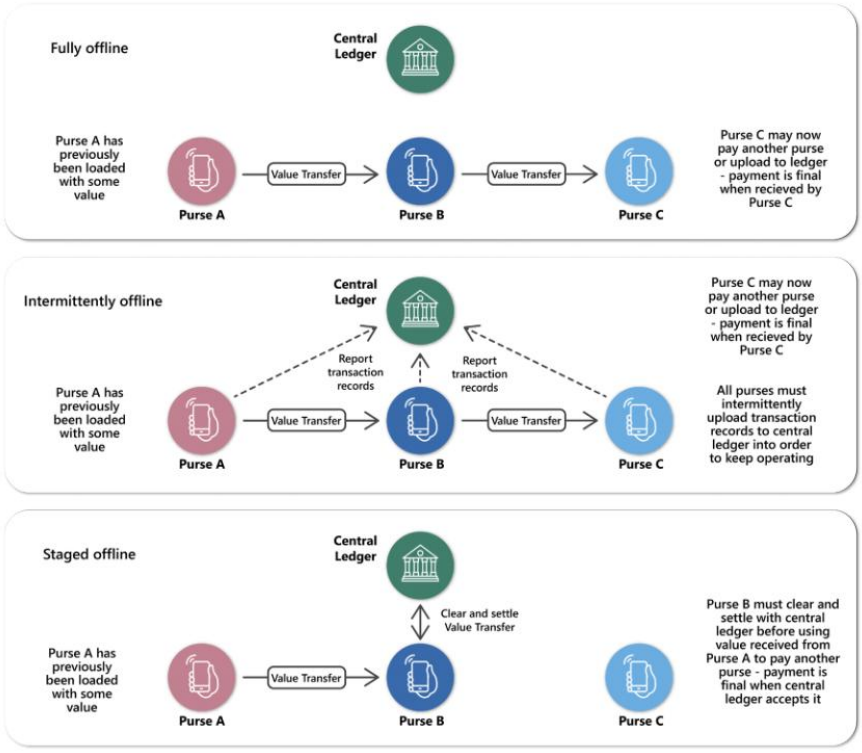
2.1.1 Fully offline, intermittently offline and Staged offline approaches

The BIS Polaris report referred to above mentions two alternatives to the Fully-offline approach, both involving a ledger component, but with only one offering offline settlement. These are:

- the **intermittently offline approach** bearing similarities with the fully offline approach. Payer and payee do not need to connect to a ledger system to complete a payment and the payee can then retransfer offline to a third party the payment received, with the important caveat that there is in addition a ledger providing an online representation of the parties' CBDC holdings which must be accessed online from time to time for reconciliation and/or audit purposes. The ledger cannot always accurately reflect the parties' positions – only their smartphones will offer conclusive evidence of their CBDC positions when offline - but is updated when one of them goes online.
- The **staged offline approach** is a less comprehensive perspective in that whilst the payment contract – the irrevocable agreement to make and receive a payment - can indeed occur when both payer and payee are offline, settlement – the payee receiving the funds – only occur when the payee is online and is therefore deferred until this happens. It follows that the payee can only retransfer the funds after it has been online.

The three 'fully-offline', 'intermittently offline' and 'staged offline' approaches are summarized in the table below

Modes of offline payment — Figure 2



2.1.2 tokens versus accounts

The BIS Polaris report recognizes that digital assets can be a 'plain balance' – a book entry – or a 'cryptographically computed digital coin (token)', therefore illustrating the two main approaches discussed earlier – an account-based or token-based approach. However, it also states that "*Offline payment solutions for CBDC are often referred to as either "account-based" or "token-based". For this handbook, this distinction has not been used as most solutions are either or both.*".

Tokens (for practical purposes UTXOs) are in essence digital bearer instrument implementing 'possession' (i.e. control of the private key) as key ownership determinant and not relying on a central or bank-delegated registry for transfer implementation – they enable peer-to-peer transfers without intermediaries. This leads to a number of structural differences with account-based payment solutions:

- Tokens do not involve financial intermediaries, payment system operators or ledger operators. Payment consent and payment instructions are purely local to the mobile devices involved and do not need interacting with third parties other than the payer and payee.
- There is no inherent KYC requirement for token-based (non-ledger) transfers. On-chain transfers are pseudonymous and protocol-based and only see addresses and UTXOs, not real-world identities or previous transaction history, and anyone with a key pair can receive or send without protocol-level KYC.
- In a more legal perspective, the absence of a ledger offering an account-based CBDC implies no unified legal framework for payment interactions. Token CBDCs should be viewed as a form of property for which the location of the private key (i.e. the smartphone) or of the person who controls it are strong candidates for determining *situs* (location) – a key determinant of the law governing the payment (in the absence of an express choice of law between payer and payee) and collateral arrangements. The approach is broadly in line with cash payments – payment interactions are usually not governed by the law of the currency involved and collateral arrangements such as pledges critically require determining the location of cash and securing access to it.

2.1.3 Are cash-like bearer payment instruments reconcilable with key policy objectives?

If tokens or other cash-like bearer payment instruments are used at scale in a CBDC framework, it is essential that these are not giving fraudsters a new tool for avoiding payment detection. The concern is certainly not new and has also applied for years to interactions with banknotes, hence the numerous caps and limitations applicable to cash payments. In the digital sphere, it is hoped that holding and transaction limits to offline CBDCs can be applied in order to prevent abuses. We have seen earlier that this implies great faith in technology solutions.

Bearer payment instruments are usually understood as financial documents where legal ownership and rights to payment are vested solely in the person who physically holds the document, without any requirement for prior registration or identification of the owner and where there is no need to register with a central registry to legally implement the transfer. Their digital equivalent are tokens (especially UTXOs) where ownership is determined by possession of the corresponding private key and there is no

central ledger implementing transfers. In both cases, the control mechanism – whether physical or cryptographic – is the sole determinant of ownership.

On the other hand, holding and transaction limits viewed as key guardrails against AML and other frauds are in essence identity-based. They need to track down the total CBDCs held by a single person across all devices and wallets, which implies that CBDC users are identified and authenticated. There is therefore a structural conflict between bearer payment instruments facilitating anonymous payment solutions and the meaningful implementation of AML/CFT requirements.

As stated by the Bank of Canada in its Central bank digital currency for offline payments, there is an irreducible tension between offline capability, security and privacy requiring clear tradeoffs "*A balance must be struck between compliance, security requirements and user needs... Adopting a security posture in terms of limits, controls and functionality, where risks are sufficiently mitigated, is still a challenge for technology available today.*"

How that tension is resolved for offline CBDCs remains unclear today. Regarding the digital euro, the key messages from EU authorities show a desire to go as far as possible towards cash-like privacy and convenience for the offline digital euro, but without necessary realizing that implementation may jeopardize key AML/CFT objectives. For example, the EU Council Mandate document refers to '*privacy inherent to the offline functionality of the digital euro*' and confirms that "*the digital euro should be available offline, with a level of privacy vis a vis payment service providers which is comparable to withdrawals of banknotes at automatic teller machines. The settlement of digital euro transactions should be designed in such a way that neither the European Central Bank nor national central banks can attribute data to an identified or identifiable digital euro user.*"). In addition, the very concept of an '*offline bearer payment instrument'* mentioned by the ECB October 2025 Closing report of the preparation of a digital euro goes in the same direction.

In significant contrast to the position taken by the EU Parliament, the recent ECB digital euro reports and the EU Council Mandate document have been careful not to explicitly mention tokens when considering the offline functionality. However the Giesecke+Devrient (G+D)-led consortium mandated in October 2025 by the ECB with the task of providing an "*end-to-end solution to make digital euro payments offline available to users and merchants across Europe*" may well, and in our view is likely to, draw on the G+D Filia Unplugged solution based on digital tokens "*providing seamless offline-capable digital payments that can be integrated into an existing payment system such as retail CBDC*" and framing the tokenized design as a way to support cash-like features (privacy, finality, resilience). (G+D FIlia Unpluged Secure offline digital payments – July 2024).

In view of the overriding public policy objectives supporting a sound AML/CFT framework as well as the compelling need for central banks to monitor double spend risks and other potential abuses as well as detect bad actors, we believe digital 'bearer instruments' are not a viable option, at least as the bearer term is generally understood and that the need for a ledger (central and/or shared with payment serviced providers) remains critical. This in our view calls into question the use of tokens, especially UTXOs when other identity-based transfer alternatives can be considered.

2.1.4 Staged offline – a digital cheque approach

The staged offline, also known as deferred offline approach can be viewed as a limited, 'partially offline' approach – indeed payment settlement does not occur offline, meaning that the payee will only receive the transferred value when he/she is online. In European countries with extensive network coverage, this may not be a major constraint considering that smartphones are usually always online. However, certain situations warrant specific attention, such as payments in crowded areas, in white zones or during network disruptions. This may explain why the EU Council Mandate document appears to rule out the Staged offline approach for the digital euro by stating that "*Online and offline digital euro payment transactions shall be settled instantaneously, 24 hours a day and on any calendar day*".

Does this mean that the Staged offline approach brings no benefits? We do not think so, but we believe benefits may be more relevant for conventional private sector payment solutions than CBDCs. Indeed, the Staged offline approach de facto implements a digital cheque solution in its current non-negotiable version where the payee can cash the cheque whenever ready to do so.

The staged offline approach should be related to various public and/or private-sector initiatives aiming at advancing offline payment capabilities to enhance resilience against cyber threats, infrastructure failures, and geopolitical risks. For example, 5 Nordic countries are developing an offline card payment system which could serve as a backup in the event of power outages amidst a steady rise of cyber security attacks. In France, the Cartes Bancaires (CB) network operates one of Europe's most mature offline payment ecosystems, with EMV chip parameters governing transaction authorization. Cards bearing the CB logo support "offline preferred" mode, allowing payments without systematic authorization requests.

An important consequence is that a 'staged offline' approach should not be seen as the exclusive preserve of public CBDCs and could well be provided by private-sector solutions. In fact, we see significantly more potential for a staged offline solution in the private sector than for CBDCs, and a prime candidate for a staged offline service could be SEPA Instant Credit Transfers, a solution which would reinforce the attraction of the SCT Inst scheme vis-a-vis card payment solutions. The solution could be coupled with a payment guarantee attribute issued by the payer's bank and communicated to payees, confirming that offline payments made by the payer below a certain amount will be honored in all cases.

2.1.5 Intermittently offline – the compromise solution

As first look, the intermittently offline solution looks more complex in that it combines both a solution implementing offline settlement (as with the fully offline approach) and a central online ledger to which synchronization is to be made intermittently directly or indirectly through their payment services providers or after a set number of transactions or when certain value thresholds are met.

The purpose of the connections is to update the central view of CBDC balances and apply controls through reconciliation processes. It is therefore a model regularly providing transaction data in order to allows the detection of double spending, irregular patterns and device tampering, as well as support financial integrity requirements. A key difference with the fully offline approach is that, whilst central banks are not instantly informed of all payment interactions, they get sufficient data in order to

monitor and police CBDC interactions, for example by identifying bad actors. They are therefore not 'flying blind' as would be the case with the fully offline model, where no information is transferred to the central bank issuing the CBDC.

In addition, the intermittently offline model offers a workable solution for the situation where mobile devices experience disfunction or stop working altogether, which would otherwise prevent their users from claiming the CBDCs stored in them. Indeed, as most smartphones tend to be connected to the internet on a frequent, indeed near permanent basis and with the likelihood of payer and payee smartphones breaking down at the same time remaining low, the central ledger should have enough information to reliably confirm 'which mobile device owns what'. Losing CBDC data locally would therefore not leave users without remedy and should allow them to claim back their CBDC entitlement to a new smartphone.

However, the intermittently offline approach presents two downsides that must be recognized.

- The first one is that it is inherently less privacy protective than the fully offline model as the payer and payee smartphones are recognized by the ledger when connecting to it – although this may be limited to the smartphone identifiers and not extend to identity attributes of the digital euro wallet users. It therefore cannot offer full 'cash-like privacy'. Whether this will be viewed as a major drawback or simply as the acceptable price to pay in order to benefit from, inter alia, recourse in loss (smartphone malfunction) situations will depend upon how users view the privacy risks involved and the trust they are willing to put into the overall CBDC framework;
- The second one is more technical in that the intermittently offline handles significantly more data during payment interactions as the whole history of offline payments has to be communicated. This has been shown to be problematic with NFC interactions requiring uninterrupted data flows. A possible alternative would be to use another proximity communication protocol, notably, Bluetooth Low Energy with a far greater communication range (up to 10 meters) but in need of a power source – so this would not work with stand-alone smartcards.

2.2 A CAUTIOUS APPROACH FROM THE BANK OF ENGLAND

A good illustration of the concerns expressed at a fully offline approach comes from the Bank of England in its recent Offline Payments Design Note for a potential digital pound which it views as overly risky. "*The Bank [of England] does not have an equivalent for 'fully' offline, as there is an expectation in the digital pound design that, due to risk based or technological limits, there will always be a need to eventually return online*". This clearly rules out the fully offline model in favor of some version of the intermittently offline one. However, the Bank of England has not yet given indications as to how often wallet users would be required to return online.

More generally, the Bank of England takes a cautious view of what it defines as 'Device offline payments' – the functional equivalent of the intermittently offline model outlined in the BIS Polaris report - where "*The money is taken off the online system and stored on a device, then transferred directly to someone else's device at the time of payment. These funds can be immediately onward spent*

within risk based and technological limits. The online system doesn't see the transaction until a device reconnects sometime after the transaction. Like with physical cash, there is a need to guard against counterfeit funds being spent, and the risk of loss due to theft. Safeguards can help to manage these risks, including secure hardware and software, transaction limits and tamper detection, but their efficacy is as yet unproven". This leads the Bank of England to come to the conclusion that "*the case for device offline payments is not yet clear […] because the benefits are uncertain and hard to quantify when weighed against the complexity of implementation, the level of maturity of the technology, and the additional risks compared with online payments*" and it therefore does not expect offline payments to be part of the functionalities of a digital pound at launch.

2.3 USING EUROPEAN DIGITAL IDENTITY WALLETS FOR DIGITAL EURO INTERACTIONS

A good starting point for the purpose of assessing the role European Digital Identity wallets (EUDIWs) could play in digital euro interactions is the EU Council Mandate document stressing the need for interoperability between digital euro interfaces and the EUDIWs and mandating smartphone manufacturers and telco operators to "*allow providers of digital euro user interfaces, providers of European Digital Identity Wallets and third-party technical support providers acting on their behalf effective interoperability with […] the hardware features and software features that are necessary for the secure processing and execution of online or offline digital euro payment transactions*". This is a position we fully support as we believe EUDIWs can and should be seen as a fundamental building block to the digital euro.

The full assessment of the role EUDIWs could play in digital euro interactions is well beyond the scope of this article, but a number of comments can be made:

- As a reminder, EUDIWs are to offer a strong customer authentication (SCA) functionality complying with EU payment regulatory requirements which the eIDAS regulation requires banks and other payment services providers to accept whenever activated by EUDIW users. Whereas in current payment interactions, SCA is relied upon by payment service providers in order to release funds without incurring liability and is therefore a key determinant of the payer/PSP relationship, offline settlement does not involve a third party but in our view needs to offer meaningful protection to payers so that they are fully informed about payments made and, in case of dispute or litigation, can provide reliable evidence of their payments. We would therefore recommend that dynamic linking, currently not a requirement for offline interactions but technically possible with EUDIWs, be mandated for all offline payments. The same should apply to mutual authentication offering meaningful protection, especially for Person-to-Person (P2P) interactions – but then, would EUDIW users acting as payees be issued with the equivalent of an access certificate required for EUDIW relying parties, which is currently not contemplated by the eIDAS regulatory framework?

- EUDIWs will no doubt play a critical role in meeting Know-Your-Client and Customer-Due-Diligence requirements with the communication of Personal Identification Data and electronically attested attributes greatly facilitating client onboarding processes. However, their involvement in payment interactions is still a matter of discussion. Expectations are that the European Banking Authority will clarify the role EUDIWs play in payments as part of the forthcoming Regulatory Technical

Standards to be prepared for the soon-to-be adopted Payment Services Regulation, but this is realistically unlikely to happen before the end of 2027, i.e. the deadline for the mandatory acceptance of EUDIWs in payment interactions. The current payment use case specifications of EUDIWs outlined in the eIDAS Architecture and Reference Framework (ARF) document setting forth technical guidelines for EUDIWs appear primarily designed to cater to organized or contractual payment schemes (notably card payments) by giving third parties a key role in the implementation of SCA and limiting the EUDIW's role to a two-factor authentication tool (see Specification of Strong Customer Authentication (SCA) Implementation with the Wallet). This approach appears at odds with open banking principles reaffirmed by the soon-to-be published payment services regulation. As it relies on a third party summarizing the payment message, it limits the role played by the EUDIW in SCA interactions and would not in our view be a realistic option for the offline use case where SCA is both needed and cannot be implemented independently of a third party. Granted, the current position taken by the ARF may evolve – the ARF is a 'work-in-progress' iterative document, not a final state of – but this would clearly need to happen if EUDIWs are to play a meaningful role in digital euro payments.

- EUDIWs can also play a significant role in facilitating digital euro and other CBDC interactions by securing the storage and management of high-quality credentials, including for that matter value-bearing credentials. This is a major attention area for the ECB, notably for the purpose of ensuring that wallets storing digital euros are not compromised and, inter alia, that holding limits are applied and enforced. Although no decision appears to have been taken, the ECB clearly contemplates a certification framework for devices and applications used in digital euro transactions. However, devising such a framework takes significant time especially considering that it would need designing from scratch, being approved by certification authorities, adopted by smartphone manufacturers and providers of mobile operating systems, put into production and sold to users. In light of this, it is not clear whether the certification timeline is consistent with a contemplated launch of digital euros in 2029. However, using EUDIWs could help in this respect as significant work has already gone into the key notions of EUDIW Wallet Secure Cryptographic Devices (WSCD) and Applications (WSCA) which are trusted hardware (WSCD) and trusted software (WSCA) ensuring tamper-resistant storage and management of cryptographic keys for wallet instances via a secure cryptographic interface, in line with the High Level of Assurance required for EUDIWs. A remaining challenge today is that WSCD/A are in the process of being specified for either local external (i.e. smartcards) or remote cloud-based solutions which are either impractical (for local external solutions) or inconsistent with offline interactions (for remote solutions). There is little doubt that the increasing availability of secure elements or eSIMs in smartphones will make the 'local internal' a solution of choice for CBDC interactions, a topic also actively considered by the Global Platform, a technical standard organization focused on security architectures and certification for secure components and devices used in digital services. Another option that could be considered for the intermittently offline model would be to rely on the secure hardware of mobile devices to create trustworthy digital signatures (in practice eIDAS qualified electronic signatures based upon a local-internal qualified signature creation device) and build a digital euro functionality on top of this without requiring additional complicated logic in the trusted hardware.

TIME TO CONCLUDE AND SUMMARIZE OUR THOUGHTS

1. We concur with the EU Parliament's view that an online-only digital euro raises significant competition concerns, may disrupt private-sector solutions and is unlikely to bring sufficient value to users to be meaningfully adopted at scale. The offline functionality is therefore a significant, indeed critical plus, especially for the P2P use case where real value can be offered to users;
2. However, it needs to be capable of transferring value offline and have the recipient respend it before going online themselves. This therefore excludes Staged offline solutions which remain very relevant for the private sector, especially for credit transfers solutions and should be implemented as an enhancement of SEPA instant payments where they would implement a modern, digital version of the cheque;
3. The fully offline, non-ledger CBDC model does not appear to be a realistic approach worth considering for the digital euro. It is too risky to be contemplated and must be combined with a ledger-based approach. In practice, this implies an intermittently offline model which we believe is the only realistic option for the digital euro given that offline settlement is mandated;
4. The offline functionality with immediate settlement will in our opinion require SCA to be implemented with dynamic-linking to better protect payers and give them a robust proof package of what they have approved. The current SCA exemption for proximity payments – designed for physical card payments - appears unjustified for wallet-based interactions. However, this implies that wallets are able to implement SCA in an embedded manner, which has not yet been meaningfully contemplated;
5. Offline payment interactions will require stringent technical requirements preventing double counting, digital euro thefts and mobile devices being compromised and likely lead to dedicated CBDC certification schemes. The specifications being developed for EUDIWs, especially with respect to wallet secure cryptographic devices (WSCD) and applications (WSCA) offer an interesting perspective but today are not focusing on 'local internal' (i.e. internal to smartphones) WSCD/A and will take time to be developed. This topic appears to be a major challenge for the timely deployment of the offline functionality as part of the initial release of digital euros. Another approach would be to work with the constraints of the qualified electronic signatures based on local internal (i.e. smatphone-based) qualified signature creation devices.