Offline-Capable Central Bank Digital Currencies as a Key Enabler of a Resilient Digital Payment System

Wolfram Seidemann* Lars Hupel*† Paula Martins*

April 2, 2026

Central Bank Digital Currencies (CBDCs) support the creation of a resilient and inclusive digital payment ecosystem. We investigate the role of offline-capable CBDCs in ensuring universal access to financial services, especially in times of crisis when conventional digital systems are disrupted.

We assess technical feasibility of offline capabilities, following an approach by the Bank for International Settlements (BIS). We further discuss the token-based design of CBDCs and contrast it with traditional account-based systems. Such a CBDC design can preserve the two-tier distribution model known from the current cash cycle. Security requirements are addressed through a layered security architecture comprising hardware security, robust payment protocols, and double-spending protection by the central bank.

Practical experiences from various pilot studies demonstrate the operational effectiveness and user acceptance of offline CBDCs across different regions and use cases. We argue that such currencies will not only complement existing monetary systems but also foster a more equitable financial landscape. Finally, we put the proposed architecture into historical context, describing the evolution of digital payments, and illustrate their renewed relevance to global financial stability and inclusivity.

1 Introduction

Integration of digital technologies into monetary systems has changed the way we carry out financial transactions. Over the past few decades, banks and businesses have streamlined cumbersome and time-consuming processes, making them more efficient and less

*Giesecke+Devrient GmbH, Prinzregentenstr. 161, 81677 München, Germany
†lars.hupel@gi-de.com

time-consuming. With increasing digitalization in all areas of life, most people expect payments to be fast and convenient, above all else. According to a survey by Bitkom, Germany's digital association, 25% of internet users never read the terms and conditions of online services (Bitkom, 2024). Many people take security for granted and might not realize that they are trading personal information for convenience with many payment service providers.

The transition towards digital payments creates significant risks. The major blackout in Spain and Portugal in April 2025, affecting tens of millions of people, illustrated this. It paralyzed all forms of electronic payment methods. Consumers and businesses were unable to conduct transactions, grinding the economy to a halt. This incident was a real-world stress test for our digital society, showing the fragility of our digital infrastructures.

In the absence of functional digital systems, cash typically serves as the sole reliable medium for transactions. There is a notable increase in demand for cash during periods of technological uncertainty—such as during the millennium change—, financial crises, and natural disasters like hurricanes or COVID-19 (Rösl and Seitz, 2024; Spicer, 2017).

Any disruption, whether caused by technical glitches or natural disasters, highlights the current digital payment systems' lack of resilience and the need for infrastructures that can withstand similar challenges in the future.

Moreover, payment services, which are largely driven by network effects and the benefits of widespread adoption, are a highly attractive business model. This fuels competition among providers, each seeking to grow their user base, which often leads to market fragmentation. In such an environment, various proprietary systems emerge, which limit interoperability and user choice.

A publicly provided platform based on common standards could counter this trend by serving as a neutral infrastructure layer. It would allow the private sector to build and offer innovative services while ensuring broad accessibility and compatibility. This open foundation would promote healthy competition focused on user-centric innovation rather than proprietary lock-in, ultimately fostering a more inclusive and efficient digital payment ecosystem.

2 The evolution of monetary systems

The monetary system has evolved alongside societal developments. Changes in economic structures, political priorities, and technological innovations had a significant impact on the monetary system.

In its earliest form, goods and services were exchanged directly. However, there was neither a common measure of value nor a reliable way to store wealth.

Money is a convention. Communities defined conveniently exchangeable objects of value as money such as grain or shells. As a result of political and economic development, emerging sovereign entities established dedicated monetary systems which facilitated trade and economic expansion.

The rapid increase in population, coupled with urbanization and industrialization, further spurred trade and heightened the demand for money. Private banks, and later sovereign entities, introduced paper money as a type of bond backed by commodities.

The departure from the gold standard marked a significant move towards the abstraction of value. Over time, money has evolved from tangible assets to digital and abstract forms.

2.1 From physical to electronic transactions

One of the earliest forms of digital payment dates back to the 1870s and the advent of telegraphy. Western Union offered to transfer money via telegraphic messages (Western Union, 2025).

According to their own account, the first credit card payment occurred in 1950 with the introduction of the Diners Club card, ‘the birth of the world’s first multipurpose charge card’ (Diners Club, 2025).

An even more remarkable event was the ‘first legitimate online transaction’, which occurred in 1994 (Fessenden, 2015). This is because the modern concept of digital payments is closely linked to the development of computer and internet technologies. This significant milestone in e-commerce paved the way for the explosion of online shopping. The sector’s robust worldwide growth is a major driver of cashless payments.

New technologies have significantly impacted the landscape of cashless payments. Chips based on *EMV (Europay, MasterCard, Visa)* standards have increased security for credit card payments and created a global standard for card payments. *NFC (Near Field Communication)* technology has cut down transaction times at the point-of-sale, allowing consumers to pay by simply tapping a card near a payment terminal. Recently, the proliferation of mobile payment apps and digital wallets—such as Apple Pay, Google Wallet, and Samsung Pay—lets users transact on card rails from their smart mobile devices.

As digital technology has expanded into most aspects of life, people increasingly expect a great user experience, including for financial transactions. This paved the way for the success of instant payment systems, which provide real-time, secure, and convenient app-based financial transactions. They address the demand for speed and efficiency. *A2A (account-to-account)* payments built on real-time payment rails are shaping the payment landscape in major emerging economies such as Brazil and India. This has led to a decline in cash usage at the point of sale. According to Bruno et al. (2024) ‘global cash usage now stands at 80 percent of 2019 levels and continues to decrease at 4 percent a year'.

Yet, we can observe an increase of cash in circulation. According to official figures, the total cash circulation within the Eurozone amounted to € 1.578 trillion in April 2025. This is almost 28% more than six years ago (€ 1.229 trillion in April 2019), growing at a faster rate than inflation would suggest.[1] Antti Heinonen, former Director of Banknote at the ECB, estimates that the number of banknotes in circulation globally is significantly higher than 900 billion pieces (Heinonen, 2025). This 'paradox of banknotes' (Bailey, 2009) can be explained by a shifting demand for cash: away from transactions, towards store of value (Zamora-Pérez, 2021).

Presently, cash remains the only public payment method that can be used independently from the issuer. But electronic transactions typically involve third-party providers that may charge fees or use personal data. Payment providers often impose requirements—such as credit scores or a minimum age—that exclude large parts of the population. The COVID-19 pandemic exacerbated this problem and underscored the necessity for more resilient, accessible, and efficient payment systems.

A digital version of cash promises to complement existing means of payment and to extend universal access to everyone.

2.2 The genesis of digital money

In the 1980s, David Chaum developed *DigiCash*, an electronic, anonymous payment scheme (Chaum, 1983). But the concept of using cryptographic protocols to represent value only took off in the late 2000s with Bitcoin.

The global financial crisis of 2008 revealed significant vulnerabilities in the financial sector: excessive leverage, a lack of transparency, inadequate regulation, immense complexity, and the risks posed by institutions deemed 'too big to fail.' Public trust in established financial institutions eroded.

Cryptocurrencies, more specifically Bitcoin, emerged as a direct response to the crisis in 2008. In conjunction with blockchain technology, they were developed to address these perceived shortcomings. Nakamoto (2008) criticized that 'commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments.' In response, they outlined principles of a peer-to-peer electronic cash system operating independently of financial institutions.

While cryptocurrencies have proliferated largely unbothered by regulation, a combination of long-term trends and specific events has led to new developments. The increasing digitalization of the economy, coupled with the COVID-19 pandemic, accelerated the

[1] ECB statistics on banknotes and coins circulation: https://www.ecb.europa.eu/stats/policy_and_exchange_rates/banknotes+coins/circulation/html/index.en.html

need for innovative, but resilient and stable financial solutions. This has catalyzed the development of *CBDCs (Central Bank Digital Currencies).*

2.3 Towards a Tokenized Financial System

Tokenization—representation of value in digital format—is becoming increasingly prominent, with central banks, commercial banks, and multilateral organizations playing significant roles. Ravi Menon, former Managing Director of the Monetary Authority of Singapore and current Chairman at the Global Financial Technology Network, highlighted tokenization's transformative impact on finance in his keynote speech at the Point Zero Forum (Menon, 2024). This is not a transient phenomenon; it's a structural change of financial market infrastructure that adds a new paradigm to the traditional, siloed architecture.

We can witness the tokenization of traditional instruments such as cash (in the form of CBDC), deposits and securities. This enables real-time, programmable, and interoperable value exchanges.

Central banks are spearheading a series of global experiments. Prominent initiatives such as *Project Agora, Project Rialto,* or *Project Meridian FX* address cross-border settlements, among other use cases. They enjoy support by the BIS to foster global exchange and standardization.

These efforts have not only offered technical insights but have recently culminated in the BIS' 'Finternet' concept: a cohesive, interoperable network of tokenized monies and assets, spanning the public and private sector. According to Carstens and Nilekani (2024), the 'Finternet would be designed to empower individuals and businesses by placing them at the centre of their financial lives.'

3 Why Central Bank Digital Currencies Matter

In a tokenized financial system, public money is not just an option, it is essential. The absence of a universally accepted, risk-free reference asset can leave the system vulnerable. Private digital currencies might struggle to maintain par, especially across various platforms and jurisdictions.

This discrepancy introduces exchange rate and counterparty risks. It also jeopardizes the fundamental concept of fungibility, crucial for a stable financial environment. Dominant private issuers have the potential to establish closed ecosystems that restrict user options and limit interoperability, thereby stifling competition.

A well-designed CBDC, issued as tokenized public money, directly mitigates these risks. Distributed through financial service providers, including commercial banks and non-bank institutions, CBDCs stabilize the monetary and financial system. They would not only complement cash as a public means of payment, but also serve as a platform for innovation, forming the cornerstone of the digital economy.

3.1 Core requirements of a successful CBDC

Security A CBDC must adhere to a comprehensive security framework. This should include internal security protocols, external security assessments, and ongoing penetration testing (security by design). The BIS 'has leveraged the NIST cyber security framework but with two additional steps, namely prepare and adapt' (BIS Innovation Hub, 2023a). CBDCs also have unique requirements: Unlike traditional banking infrastructure, a CBDC would operate continuously, 24/7, allowing very little room for maintenance or downtime (Rafiee and Hupel, 2025). To maintain the ongoing trust of all participants within the system, a strong and scalable *PKI (Public Key Infrastructure)* is essential.

Data Privacy CBDCs must prioritize users' privacy by safeguarding personal and transactional information against unauthorized access and breaches. They can offer greater privacy than commercial digital payment systems, which often rely on monetizing user data. Central banks have no (commercial or otherwise) interest in that, hence, they can design CBDC as public infrastructure with privacy safeguards. For example, operational, transactional, and administrative data can be separate. At the same time, CBDC must comply with rules on anti-money laundering and financial governance rules. Central banks should carefully balance transparency and anonymity to foster trust and acceptance among users.

Interoperability A CBDC system needs to integrate smoothly with current infrastructures (Hupel, 2023). This allows financial institutions to seamlessly integrate digital currency into their ecosystems, which fosters the development of innovative applications. Cross-border interoperability would reduce costs and complexities, and significantly lower settlement and default risks for international transactions.

Offline functionality Like cash, CBDC must function universally and without interruption. This allows it to achieve legal tender status, driving adoption. It should operate independently of network connectivity, bank accounts, or continuous access to electricity. It should not require high-end smartphones. CBDC promises a strong potential of financial inclusion to the many people left out of today's digital financial system. Offline functionality is a tangible example of strong privacy protection by design: it enables anonymous, cash-like transactions while still operating within a secure and regulated framework.

3.2 The importance of offline CBDC

Zooming in on the last requirement, offline functionality is central to achieve many central banks' policy objectives.

People should have access to a secure and reliable digital payment method. Offline functionality—through a well-designed CBDC and/or as an add-on to a national payment system—addresses this.

In a 2023 survey, 98% of central banks saw offline payment as either vital or advantageous for a retail CBDC (BIS Innovation Hub, 2023b).

Resilience and universal acceptance of a national currency, whether physical or digital, are critical to its function and trustworthiness. Integrating offline functionality from the outset ensures that a CBDC remains functional without reliance on smartphones, network connections, internet access, or electricity.

Cash sets a high standard for its digital counterpart, which central banks intend to issue as legal tender. The European Central Bank (2020) notes that '[l]egal tender status would require that users be able to receive incoming payments through means that are as user-friendly as banknotes, for example by using a simple physical device that can also be used offline.'

By offering offline capabilities and simple, low-cost wallet formats like feature phones or chip cards CBDC helps ensure that everyone, regardless of their circumstances, has access to secure and convenient digital payments—anytime, anywhere.

4 Technical Feasibility

Many central banks have, or are currently, investigating CBDC designs that include some degree of offline capability. The BIS, in Project Polaris, distinguishes three types of offline capability, in increasing order of ambition (BIS Innovation Hub, 2023b):

- **staged,** in which two parties can transact offline, but the receiving party cannot subsequently use funds received offline;
- **intermittently,** in which parties can transact offline without intervening online connection, but limited by risk parameters—such as a mandatory online integrity check after a fixed number of transactions—;
- **fully,** in which value circulates offline indefinitely and no online connection is ever required.

As an analogy, cash is in the last category with some aspects of 'intermittently' because—while there is no mandatory check on banknotes—they would typically return to the central bank after a certain period of use, particularly when becoming unfit for circulation. Payment cards, on the other hand, can be classified as 'staged,' because settlement is delayed and requires online connectivity (Hupel, 2024). Further, we assume that 'offline' means that both parties are not connected to the internet (sometimes referred to as 'dual offline').

The following details are based on design experiences gained in CBDC pilot projects. The approach—intermittently offline, re-spendable—has been tested intensively in Ghana, Thailand, and Hong Kong.

4.1 Use cases for retail CBDC

In its most basic form, retail CBDC should cater for everyday payment scenarios. In their eCedi design paper, Bank of Ghana (2022) describes the following user journeys:

1. Person-to-person transfers between unbanked people with hardware wallets
2. Purchases of goods and services with hardware wallets (point of sale)
3. Person-to-person transfers using bank-provided online wallets, possibly remotely
4. Purchases of goods and services using bank-provided online wallets, point of sale or e-commerce
5. Wallet funding (and redemption) with cash, e-money, or deposit accounts

If we consider the last point to be a 'special case' of a purchase, we can group the scenarios according to Figure 1. All scenarios should support different form factors. Except for e-commerce, they should also work offline.

The eCedi pilot report confirms the need for the ability to re-spend funds received offline, 'providing opportunities for persons living in off-grid communities to access digital forms of payments and improve their livelihoods' (Bank of Ghana, 2024). This is sometimes called 'consecutive offline,' to emphasize that a series of payments can happen without intervening online connection.

But it would be wrong to assume that only emerging economies seek such features. The above scenarios, coupled with an intermittently offline model, also matches closely what the ECB envisions for the digital euro (European Central Bank, 2024).

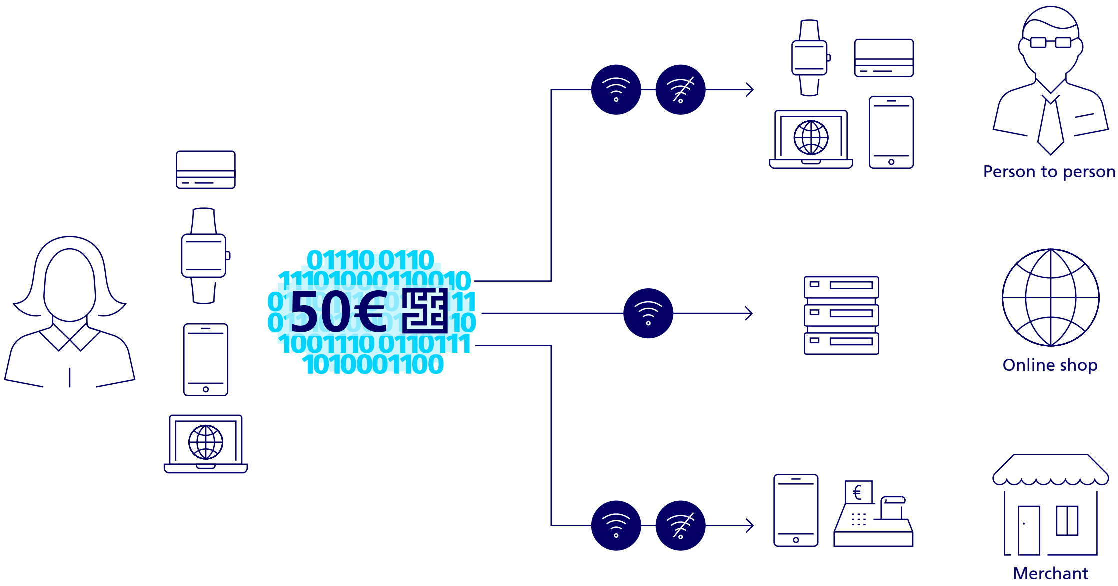

Figure 1: Basic payment scenarios for retail CBDC

4.2 An offline-capable token protocol

In the world of credit (or debit) cards, payments are always based on identities. A customer uses a payment card as a credential to authenticate towards their bank, which then confirms the transaction. But as opposed to cash, settlement is delayed, which means that funds are not immediately transferred.

Consequently, it makes more sense to model CBDC based on cash. This is often referred to as a 'token-based system,' because money is represented as individual cryptographic tokens bearing a value.

Each token comprises a public-private keypair and a denomination. As opposed to banknotes, we are not confined to a fixed set of denominations. A wallet could—for example—hold three tokens worth € 5, € 9, and € 13 respectively.

As Bank of Ghana (2022) succinctly writes: 'Payment is done by transferring the [token] from one person to another. The concept is similar to cash payment transactions, where payment is done by transferring banknotes and/or coins from person A to person B.' Of course, the transfer is handled by the wallets, which abstracts away the implementation details from the user.

This contrasts with an 'account-based system,' in which value is tied to an account. Transactions work by debiting the payer account and crediting the payee account. Traditional banking uses this model, managing an assignment of account numbers to balances. But it has limits, which is why the Bank of Ghana and others opted for the token-based model (more details below).

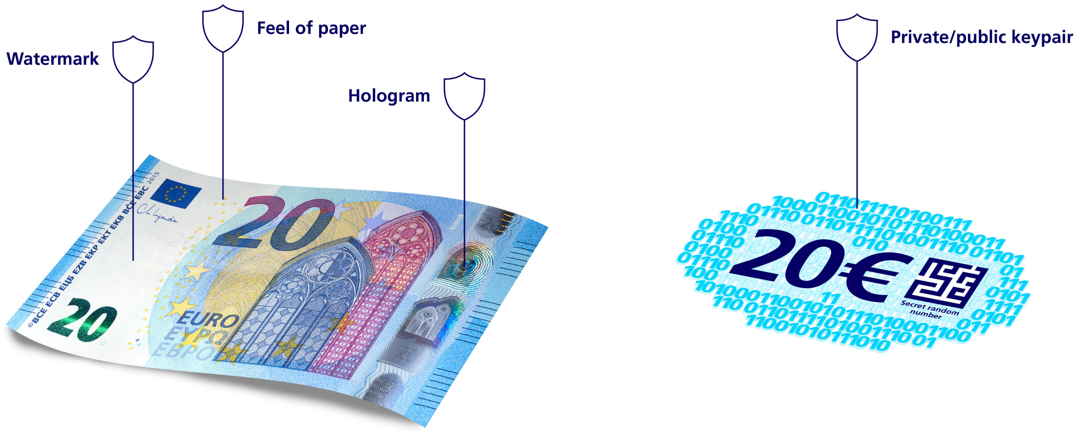

Figure 2: Modelling digital cash after physical cash

Should a wallet not have the correct change available, tokens can be split into smaller denominations. In this, the input token is consumed and loses its validity, whereas two output tokens are freshly created. This is of course only admissible if the combined output values are equal to the input value.

For example, if the wallet holding € 5, € 9, and € 13 were to pay € 10 to another wallet, it could use the first two tokens, but split the € 9 first into 5 + 4, keeping the € 4. Each token receives an individual cryptographic keypair and can therefore be recognized by the central bank (more about this in §4.3).

Yet, the underlying token management is hidden from the user, who only sees an aggregate balance. Wallets can optimize holdings and split and merge tokens according to technical requirements. This does not rule out micro-payments: tokens can have an arbitrary precision as configured by the issuer.

This design has multiple advantages. Among them is increased **privacy**: while each token has a digital fingerprint, they are not associated with the wallet holder's identity. Tokens have a short life and are replaced quickly. This is a **cryptographic advantage**, because it shortens an attacker's time window during which they can attack a particular piece of money. Finally, it allows to **ring-fence** compromised value. An invalid token can be isolated, without affecting many transactions, whereas a compromised account would need to be replaced entirely. Put simply, accounts unduly conflate 'identity' and 'value'.

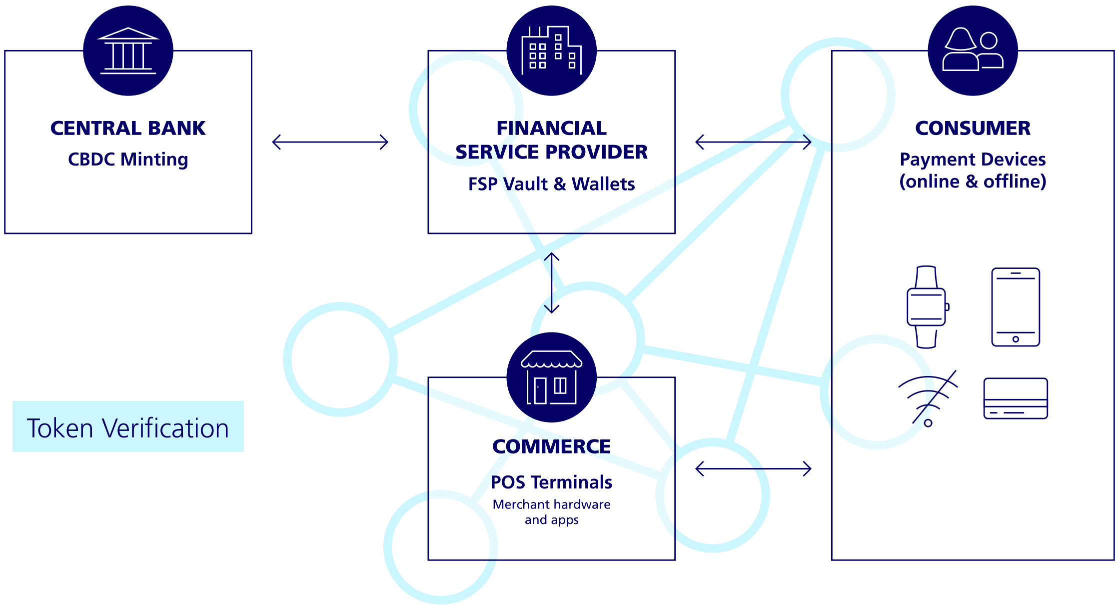

Figure 3: Two-tier distribution model from minting to usage

4.3 Two-tier distribution model

Bringing CBDC into circulation mirrors the current two-tier financial system. It consists of *minting* and *distribution* and closely resembles the current cash cycle.

The central bank is the only entity that is allowed and able to mint CBDC. This cryptographic process is performed in an air-gapped, standalone environment. Freshly-minted tokens are physically transported to the central bank's digital vault.

FSPs (Financial Service Providers), including banks and other institutions, can request CBDC from the central bank against reserves. This would be part of their routine liquidity management, just like cash.

Finally, tokens are distributed to consumers' wallets on a variety of form factors. This can happen

- through existing mobile banking apps to which CBDC capability has been added through a SDK,
- on dedicated hardware devices such as chip cards, or
- online-only wallets hosted by an FSP of the consumer's choice.

From those wallets, consumers can transact CBDC for a range of use cases, for example, sending money between two smartphones using NFC.

Merchants receiving CBDC at the point of sale can redeem them with their bank, which will credit the value to their bank account. The token stays with the bank and can be 'recycled'—i.e., distributed to another customer—or sent back to the central bank for monetary policy reasons. Any transaction, no matter whether it is large value (e.g. between FSPs) or small value (e.g. between users), is end-to-end encrypted, protecting the tokens in transit.

Central banks should, as far as possible, enable FSPs to provide wallets on existing hardware and software platforms. For the former, the use of Secure Elements is state of the art (§4.4). For the latter, FSPs can integrate CBDC functionality into their apps and devices through SDKs.

Unbanked people can also participate in the system. For that, they need to obtain a hardware or software wallet, as specified by the issuing central bank. For example, the draft legislation on the digital euro envisions post offices or government authorities could act as non-bank intermediaries that provide basic CBDC services (European Commission, 2023).

The core verification system allows all participants in the CBDC ecosystem to confirm that received tokens are valid. In the online scenario, this verification happens on the spot, while in offline mode, it is asynchronous: tokens from past offline transactions are checked as soon as any transacting party is online again.

4.4 Security aspects in an intermittently offline model

The European Central Bank (2024) states very clearly that the 'Eurosystem must maintain ownership and ensure integrity of its balance sheet,' which requires that (offline) CBDC must be protected '[a]gainst double-spending and undue money creation.' For that, they propose two key ingredients: a Secure Element in the wallet, whose 'tamper-resistant features protect the information stored on the device and allow mutual device authenticity checks;' and an occasional online integrity check that 'provides ultimate line of defence as the authenticity of [...] offline digital euro is checked.'

In the following, we elaborate on this model and insert an additional layer (Figure 4), together forming a 'defense in depth' approach.

But let us first consider the main threat to digital currency—*double-spending*—which can be explained using an example attack on a wallet:

1. An attacker records the storage contents of the payer wallet.
2. The attacker performs a payment to an unsuspecting payee.
3. Now, the attacker resets the storage contents and performs a second payment.

If the payees are offline, they would be unable to detect this. Therefore, the security of offline CBDC payments hinges on stopping the attack from occurring in the first place. This is where the security model comes into play.

The model's bottom layer is **strong hardware security** based on *Secure Elements*. Those are standardized, tamper-resistant chips that protect against extraction, reset, manipulation, cloning, and other related attacks. For example, they have special shielding and coating and can detect physical attempts to break into the chip. The purpose of a Secure Element is to safely store cryptographic keys and other sensitive data, including the token keys (as described in §4.2). Software-only approaches, i.e., designs that do not incorporate hardware security, not only exclude offline use cases, but are also widely considered to be not secure enough (Allen et al., 2020; Christodorescu et al., 2020).

In the middle, **secure payment protocols and channels** provide protection against attacks when money is being moved. For example, wallets should always employ end-to-end encryption to prevent eavesdroppers from cloning tokens. The European Central Bank (2024) mentions this implicitly in the form of 'mutual device' authentication. But there also need to be mechanisms to resolve interrupted transactions which should not result in a situation where both payer and payee believe that they are in the possession of the money transferred.

Finally, the central bank must always be able to tell **authentic from counterfeit money**. This is very easy with a token system because every token can only be used once. In essence, this is the issuer acting as the final authority, just like for banknotes.

This final layer would not work in 'fully offline' mode (§4), because if value circulates offline indefinitely, by definition the central bank would be unable to act as the 'validator of last resort.' Yet, even if the transacting parties are offline—and therefore cannot reach the central bank—the other layers provide a high level of assurance.

Users need to be aware that with this approach, we cannot restore lost funds. This was proved by Kahn et al. (2021) in general for any payment system: out of the three desirable properties (i) protection against double-spending, (ii) offline capability, and (iii) loss recovery, only two are achievable simultaneously.

For example, debit cards compromise on offline capability. To avoid overdrafting an account, transactions must be processed online. Paper cheques and credit cards work offline, but at the expense of potential double spending. But with CBDC being a central bank liability, this compromise is unacceptable.

The fact that tokens stored in a lost offline wallet cannot be recovered introduces an important aspect of user risk management. Users are unlikely to store large amounts of CBDC in offline wallets, knowing the potential for irreversible loss. This implies a natural differentiation in usage patterns: Offline CBDC will likely serve for smaller, everyday transactions, while online CBDC—with recovery mechanisms and stronger safeguards—will be prioritized for higher-value use cases.

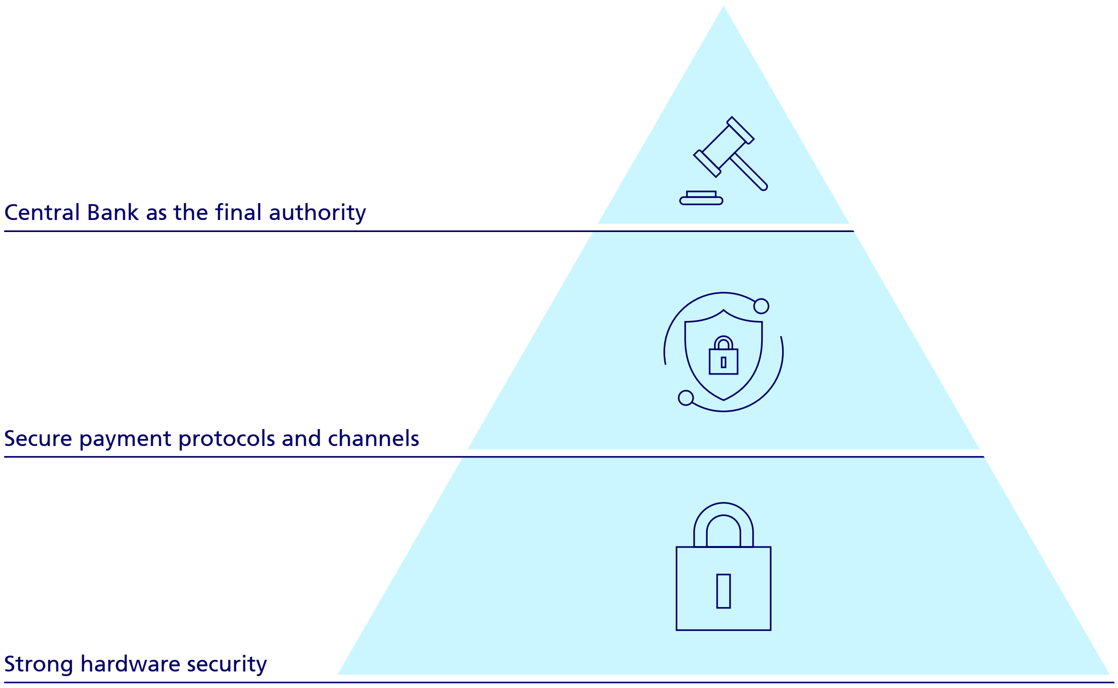

Figure 4: A security architecture with three lines of defense

In summary, this leaves a cash-like CBDC, supporting 'intermittently offline' payments while protecting against double-spending, to be the design sweet spot.

4.5 Practical pilot experiences

In this section, we describe experiences gathered in CBDC experimentations and pilot projects that encompassed both online and offline use cases.

In **Ghana,** the focus of the eCedi project was on 'financial inclusion, minimization of disruption to the financial service architecture, avoidance of financial disintermediation, safeguarding financial stability, ensuring regulatory certainty, system resilience and integrity and user-centric approach' (Bank of Ghana, 2024). Field testing over four months in three regions—urban, peri-urban, and rural—was accompanied by user acceptance research. Of the 2,923 total participants, 173 were offline (all in the rural region). Consumers and merchants received smartcards and POS terminals, respectively, to transact with each other. In this offline context, the report notes that 'technical feasibility was demonstrated,' and the utilized form factors were 'easy to use and intuitive.' Independent research by the Consultative Group to Assist the Poor corroborated the findings (Bank of Ghana, 2024).

Shortly after a 2021 report on their vision for a retail CBDC, Bank of **Thailand** conducted a pilot project to 'to assess technological readiness and fundamental functions

Figure 5: Payment terminal with two card slots for card-to-card transactions; prototype device

Figure 6: Phone with attachable card reader, allowing for card-to-card payments without special devices

[. . .], evaluate the potential [. . .] in harnessing financial innovation beyond the existing payment infrastructure, explore whether CBDC infrastructure can safely enable open access for both banks and non-banks, and assess whether Retail CBDC can be an alternative payment infrastructure in the retail payment sector' (Bank of Thailand, 2021; Bank of Thailand, 2024). Besides testing a variety of standard payment use cases, the Bank also hosted an 'innovation track' to discover new applications through a public hackathon. This track enjoyed active industry participation, 'attract[ing] over 100 proposals.' In terms of offline functionality, the report attests 'the capability to handle hundreds of transactions during periods of disconnection before requiring synchronization with the core validation system' (Bank of Thailand, 2024).

In these two projects, we could practically validate the above CBDC design, with the use cases set out in §4.1.

There is ample literature about experiments of other central banks around the world that investigate security architecture and user experience. For example, using various communication channels such as NFC, *BLE (Bluetooth Low Energy)* and QR codes (Bank of England, 2025). The **British** study found that BLE can be used for transactions between phones[2] and NFC for transactions between a phone and a card. The Bank also employed Secure Elements to protect against double spending. They considered a similar security architecture as described in §4.4 as mitigation against security risks.

[2] NFC is also technically possible, but Bank of England considered it to be out of scope.

While the Bank was very conservative about possible security problems, the **ECB** is more confident in this state-of-the-art approach (European Central Bank, 2024). Like banknotes, it is not 100% possible to prevent counterfeiting; however, individual counterfeits do not pose a systemic risk for the currency system. The ECB believes that the combination of secure hardware and online integrity checks helps the 'Eurosystem [...] maintain ownership and ensure integrity of its balance sheet.'

As part of their investigation, the ECB also examined card-to-card transactions, which requires special devices with two card slots (as tested in **Ghana**, see Figure 5). This idea is not novel: in the 1990s, the 'Mondex' electronic cash system relied on smartcards and bespoke transfer devices. As Stalder (2002) describes, '[f]or a transaction, both Mondex cards were to be inserted in a card-reading device.' Top-ups and withdrawals required use of ATMs. Lack of infrastructure and cumbersome user experience were contributing factors to Mondex' lack of success.[3] But today, smartphones could fulfill all these functions. Attachable or wireless card readers even allow for card-to-card transactions (Figure 6). This should greatly simplify deployment and user experience.

5 Towards a resilient and inclusive future

The development of offline CBDC undoubtedly contributes to a resilient digital payment infrastructure. Past incidents—including blackouts and natural disasters—have already highlighted the weaknesses of (exclusively) online systems and the necessity for robust, offline-capable solutions.

CBDC, designed to be re-spendable offline, has undergone successful testing in pilots. The technology is mature for production deployment and satisfies all performance requirements.

The five 'A' framework—access, acceptance, availability, authenticity, and affection—serves as a useful basis for evaluation of payment systems in general (Seidemann and Mitchell, 2023). We apply it to CBDC as follows.

Access is significantly broadened, as CBDC wallets can work without a bank account or advanced devices. This greatly enhances financial inclusion. Users can rely on cheap commodity hardware like a chip card. The lack of connectivity requirements fosters **acceptance,** by allowing transactions under any circumstances. Similarly, **availability** is ensured because offline tokens enable transactions even in situations where digital systems might fail, such as during power outages. In an offline CBDC, use of tokens provides **authenticity.** The security approach eliminates single points of failure and mitigates risks effectively, ensuring operational integrity even if hardware is compromised. Finally, the offline functionality promotes **affection** for CBDC as a digital form

[3] Additionally, Mondex—an account based-system—provided unclear security guarantees (see also §4.4) and suffered from long transaction times, both problems that are solved now.

of cash that is always accessible, in all places, and by all individuals. It supports privacy, increases the number of use cases, and allows users to transact independently of the issuer. This positions offline CBDC as a versatile and widely acceptable medium of exchange, facilitating its adoption across diverse scenarios.

In conclusion, offline CBDC is not merely an alternative to, but a necessary evolution of the digital payments landscape, mirroring the resilience and ubiquity of cash while harnessing the benefits of digital technology. Its readiness for widespread deployment could mark a significant shift towards a more inclusive and resilient financial system. Integrating offline functionalities from the inception of system design is crucial for achieving a digital payment system that is truly equitable and robust.

Acknowledgements We thank our colleague Miria Heinrich for her support. We would also like to thank Michael Salmony for thorough review and feedback.

References

Allen, Sarah et al. (July 2020). *Design choices for Central Bank Digital Currency: Policy and technical considerations*. URL: https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf.

Bailey, Andrew (Dec. 6, 2009). *Banknotes in Circulation: Still Rising: What Does This Mean for the Future of Cash?* URL: https://www.bankofengland.co.uk/-/media/boe/files/speech/2009/banknotes-in-circulation-still-rising.pdf.

Bank of England (Apr. 10, 2025). *Digital pound experiment report: Offline payments*. URL: https://www.bankofengland.co.uk/report/2025/digital-pound-experiment-report-offline-payments.

Bank of Ghana (Mar. 2022). *Design paper of the digital Cedi (eCedi)*. URL: https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf.

— (Oct. 2024). *A report on Bank of Ghana's Central Bank Digital Currency Pilot Project*. URL: https://www.bog.gov.gh/wp-content/uploads/2024/10/The-eCedi-Report-221024.pdf.

Bank of Thailand (Apr. 2, 2021). *The Way Forward for Retail CBDC in Thailand*. URL: https://www.bot.or.th/content/dam/bot/documents/th/financial-innovation/cbdc/20210402_BOT_RetailCBDCPaper.pdf.

— (Mar. 2024). *Retail CBDC Conclusion Report*. URL: https://www.bot.or.th/content/dam/bot/documents/en/financial-innovation/cbdc-digital-currency/Update_Release_ENrCBDC%20Conclusion%20Report.pdf.

BIS Innovation Hub (July 2023a). *Project Polaris: a security and resilience framework for CBDC systems*. URL: https://www.bis.org/publ/othp70.pdf.

— (May 2023b). *Project Polaris: handbook for offline payments with CBDC*. URL: https://www.bis.org/publ/othp64.pdf.

Bitkom (2024). *Allgemeine Geschäftsbedingungen werden meist weggeklickt.* URL: https://www.bitkom.org/Presse/Presseinformation/AGB-meist-weggeklickt (visited on 09/09/2025).

Bruno, Philip et al. (Oct. 18, 2024). *Global payments in 2024: Simpler interfaces, complex reality.* URL: https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-in-2024-simpler-interfaces-complex-reality.

Carstens, Agustín and Nandan Nilekani (Apr. 15, 2024). "Finternet: the financial system for the future". In: *BIS Working Papers* 1178. ISSN: 1682-7678. URL: https://www.bis.org/publ/work1178.htm.

Chaum, David (1983). "Blind Signatures for Untraceable Payments". In: *Advances in Cryptology.* Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Boston, MA: Springer US, pp. 199–203. ISBN: 978-1-4757-0602-4.

Christodorescu, Mihai et al. (2020). *Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies.* DOI: 10.48550/ARXIV.2012.08003.

Diners Club (2025). *75 Years of Diners Club History.* URL: https://www.dinersclub.com/about-us/history/ (visited on 09/09/2025).

European Central Bank (Oct. 2020). *Report on a digital euro.* URL: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

— (Apr. 11, 2024). *State of play on offline digital euro.* URL: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.degov240411_item3updateofflinedigitaleuro.en.pdf.

European Commission (June 28, 2023). *Proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro.* URL: https://eur-lex.europa.eu/resource.html?uri=cellar:6f2f669f-1686-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

Fessenden, Maris (Nov. 30, 2015). *What Was the First Thing Sold on the Internet?* URL: https://www.smithsonianmag.com/smart-news/what-was-first-thing-sold-internet-180957414/ (visited on 09/09/2025).

Heinonen, Antti (June 10, 2025). *Does the Number of Banknotes in Circulation Already Exceed 900 Billion?* URL: https://cashessentials.org/does-the-number-of-banknotes-in-circulation-already-exceed-900-billion/ (visited on 09/09/2025).

Hupel, Lars (2023). "Interoperability aspects of CBDC across ecosystems and borders". In: *Journal of Payments Strategy & Systems* 17.4, pp. 422–432. ISSN: 1750-1814. DOI: 10.69554/MBDJ6710. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4636197.

— (2024). "A conceptual model for point-of-sale payment with Retail CBDC". In: *Journal of Payments Strategy & Systems* 18.4, pp. 381–394. ISSN: 1750-1814. DOI: 10.69554/ETQK2745. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4912865.

Kahn, Charles M., Maarten van Oordt, and Yu Zhu (2021). "Best Before? Expiring Central Bank Digital Currency and Loss Recovery". en. In: DOI: 10.34989/SWP-2021-67.

Menon, Ravi (July 2, 2024). *Asset Tokenisation, Artificial Intelligence, Quantum Computing*. URL: https://gftn.co/insights-pzf/asset-tokenisation-artificial-intelligence-quantum-computing-pzf-2024 (visited on 09/09/2025).

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". In: URL: https://bitcoin.org/bitcoin.pdf.

Rafiee, Makan and Lars Hupel (2025). "How to Design a Public Key Infrastructure for a Central Bank Digital Currency". In: *Proceedings of the 22nd International Conference on Security and Cryptography*. SCITEPRESS - Science and Technology Publications, pp. 696–704. DOI: 10.5220/0013562300003979.

Rösl, Gerhard and Franz Seitz (2024). "Uncertainty, politics, and crises: The case for cash". In: *Latin American Journal of Central Banking* 5.3, p. 100128. ISSN: 2666-1438. DOI: 10.1016/j.latcb.2024.100128.

Seidemann, Wolfram and Astrid Mitchell (Apr. 3, 2023). *Building a Resilient Cash Infrastructure*. URL: https://currency-news.com/news/2023/apr/03/building-resilient-cash-infrastructure/ (visited on 09/09/2025).

Spicer, Jonathan (Sept. 15, 2017). *Cash demand doubled for Fed in hurricane-hit Florida*. URL: https://www.reuters.com/article/business/cash-demand-doubled-for-fed-in-hurricane-hit-florida-idUSKCN1BQ2L0/ (visited on 09/09/2025).

Stalder, Felix (2002). "Failures and Successes: Notes on the Development of Electronic Cash". In: *The Information Society* 18.3, pp. 209–219. DOI: 10.1080/01972240290074968.

Western Union (2025). *About Us*. URL: https://www.westernunion.com/corporate/about-us.html (visited on 09/09/2025).

Zamora-Pérez, Alejandro (2021). "The paradox of banknotes: understanding the demand for cash beyond transactional use". In: *ECB Economic Bulletin* 2021.2. URL: https://www.ecb.europa.eu/press/economic-bulletin/articles/2021/html/ecb.ebart202102_03~58cc4e1b97.en.html.