

# Offline solution for CBDCs

Give your Central Banks Digital Currency the same versatility as cash



# W

ith 86% of central banks throughout the world now developing their own digital currency, offline capability is becoming a must-have for a successful deployment

\*source: newsweek.com

## Why are CBDC offline payments needed?

Card payments may not be available exceptionally (when the payment or telecom network is down) as users can still fallback to cash. But cash itself cannot afford to go down, as there is no backup. For that reason central banks need to find a solution to allow for secure offline payments when connection is not available.

Telecommunications network outages can happen for a multitude of reasons; worse yet, natural disasters could knock down the network infrastructure at the exact moment when cash is needed most.

Additionally, offline payments allow larger transaction volume by reducing the load on servers.

## The IDEMIA CBDC offline payments solution

In a two-tier CBDC model, money is loaded into the secure wallet by the bank. The IDEMIA CBDC solution leverages the use of secure hardware to prevent fraud and double spending with no compromise on usability.

Our solution works with any consumer device: smartphones of course, but also feature phones, biometric payment cards, SIM cards, wearables and even connected machines—making CBDC truly available to all.

A smart contract enforces security and the central bank policy, including privacy.

## Benefits



### Always on

Allows anyone to always be able to pay anywhere, even without a network connection.



### Highest security

No compromise on security: prevent double spending with government grade secure hardware.



### Privacy + AML

Protects privacy while maintaining Anti Money Laundering (AML) requirements. Enforces maximum balances.

## Why IDEMIA?

As a global leader in identity technology with a local payments footprint in over 28 countries around the world, IDEMIA's expertise in secure elements enables banks, FinTechs, payment networks, retailers and transport operators to unlock new payment experiences.

IDEMIA technologies facilitate billions of frictionless interactions between people, objects, companies, governments and everything in between in both the physical and digital worlds — at scale and in total security.

## How it works

The IDEMIA offline solution uses public key cryptography and allows payment from a secure device to any device, secure or not. The flexibility of the protocol allows it to work with both centralized and decentralized architectures.

After user onboarding, using Know Your Customer (KYC) biometrics checks, the wallet is securely paired to the same user's biometric features. When the wallet is used, the payer's identification and authentication can be securely assessed.

Users can initiate offline payments with double spending protection, by exchanging over a NFC channel or QR Code with the payee. The hardware security mechanisms prevent fraudulent money creation. Payments can also be received with or without internet or ledger connection with the secure wallet. All payments are securely logged

to prevent fraud, including the digital identity of the payer to apply anti-money laundering controls while maintaining privacy.

The secure wallet can recycle its memory full of payment logs, without disrupting the secure offline payment service for the user nor compromising its security.



## Case study: an offline demonstrator for the digital euro

### Delivering an offline digital euro proof of concept to the ECB and the European National Central Banks

IDEMIA has developed a full demonstration an offline version of a decentralized ledger (blockchain) based the digital euro at the request of the European Central Bank, the Bundesbank, the Banque de France, the Banca d'Italia and other National Central Banks.

The demo allows for purchases using a smart phone or a smart card. For an even higher level of security, the smart card access can be protected with biometric authentication via an onboard fingerprint reader.

This showed that security can be achieved offline with protection against double spending while offering great convenience and a high level of customization based on regulation and use cases defined by the central bank and/or the wallet provider (e.g. commercial banks).



### Currency grade security

- › Hardware security has been proven over time in the field.
- › Hardware based security is frictionless and supports a variety of devices and use cases including payments by card, by phone, by an IoT\* device, etc.
- › Hardware security is the only technology available to address the security level required for digital currency.
- › Secure hardware (e.g. card) access can be secured by an onboard fingerprint reader.

IoT: Internet of Things



### Serving central banks

IDEMIA also offers:

- › A wide range of payment devices to act as CBDC bearers.
- › Digital identity solutions to enforce KYC (Know Your Customer) requirements when onboarding customers.
- › Biometric-based solutions to enforce AML (Anti Money Laundering) requirements.