Giesecke+Devrient
Creating Confidence

Beyond Secure Elements

Security aspects of Digital Cash

Lars Hupel
Java Card Forum Webinar
2025-12-18

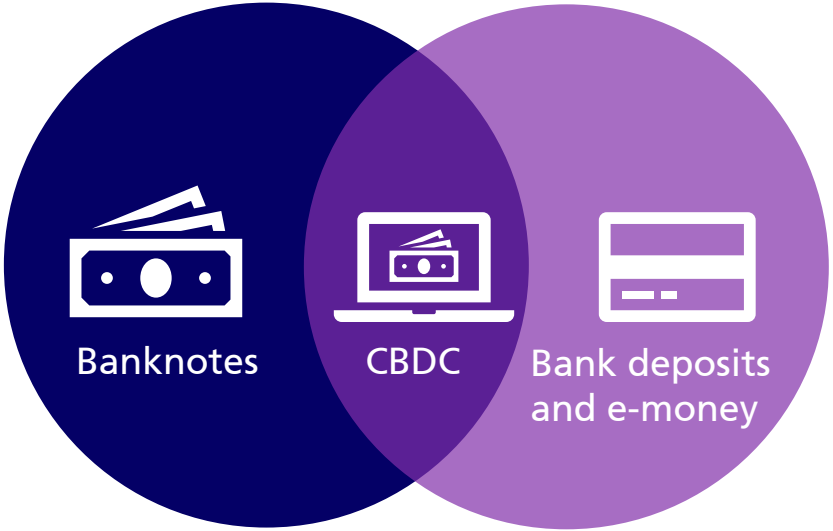
- What is it?
- How is it designed?
- How to make it secure?
- Who is issuing it?

What is digital cash?

1. … stored in digital wallets
2. … offline-capable
3. … fungible
4. … privacy-preserving
5. … peer-to-peer transactable
6. … tamper-resistant

Central Bank Digital Currency

Issued by the central bank



Digital money

The move towards CBDC is gaining momentum

91%

of central banks worldwide are actively engaged in CBDC work

67% are experimenting and/or running pilots

89% of adv. economies work on both retail & wholesale

CBDCs progressed in tandem with regulations for stablecoins and other cryptoassets

Source: Bank for International Settlements, 2024-25

"pilot exercise could start in 2027 and the Eurosystem should be ready for a **potential first issuance … during 2029**"

Offline card payments should be possible no later than 1 July 2026

PRESS RELEASE The Riksbank and representatives from the payment market have today reached an agreement to increase the possibility to make offline card payments for essential goods.

https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/press-releases/2025/offline-card-payments-should-be-possible-no-later-than-1-july-2026/

UPI Lite X: The Next Generation of Payment Solutions

Last Updated: September 16, 2025

> UPI Lite X is an innovative feature that enables users to both send and receive money even without internet access thus enabling them to proceed with secure and successful transactions even in areas with lesser connectivity such as rural areas.

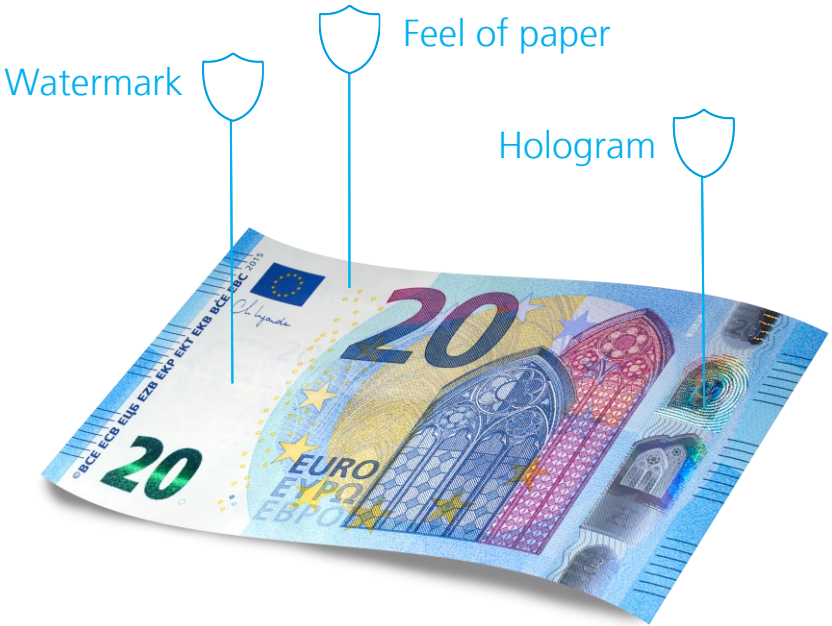
UNIFIED PAYMENTS INTERFACE

https://paytm.com/blog/payments/upi/upi-lite-x/

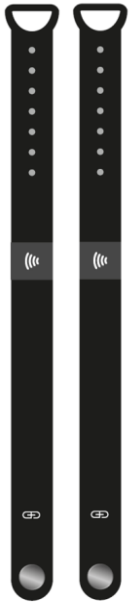
Technical design of digital cash

Giesecke+Devrient
Creating Confidence

Modelling digital cash after physical cash



Wallet form factors



Security aspects

Giesecke+Devrient
Creating Confidence

No hardware can guarantee **100% security.**

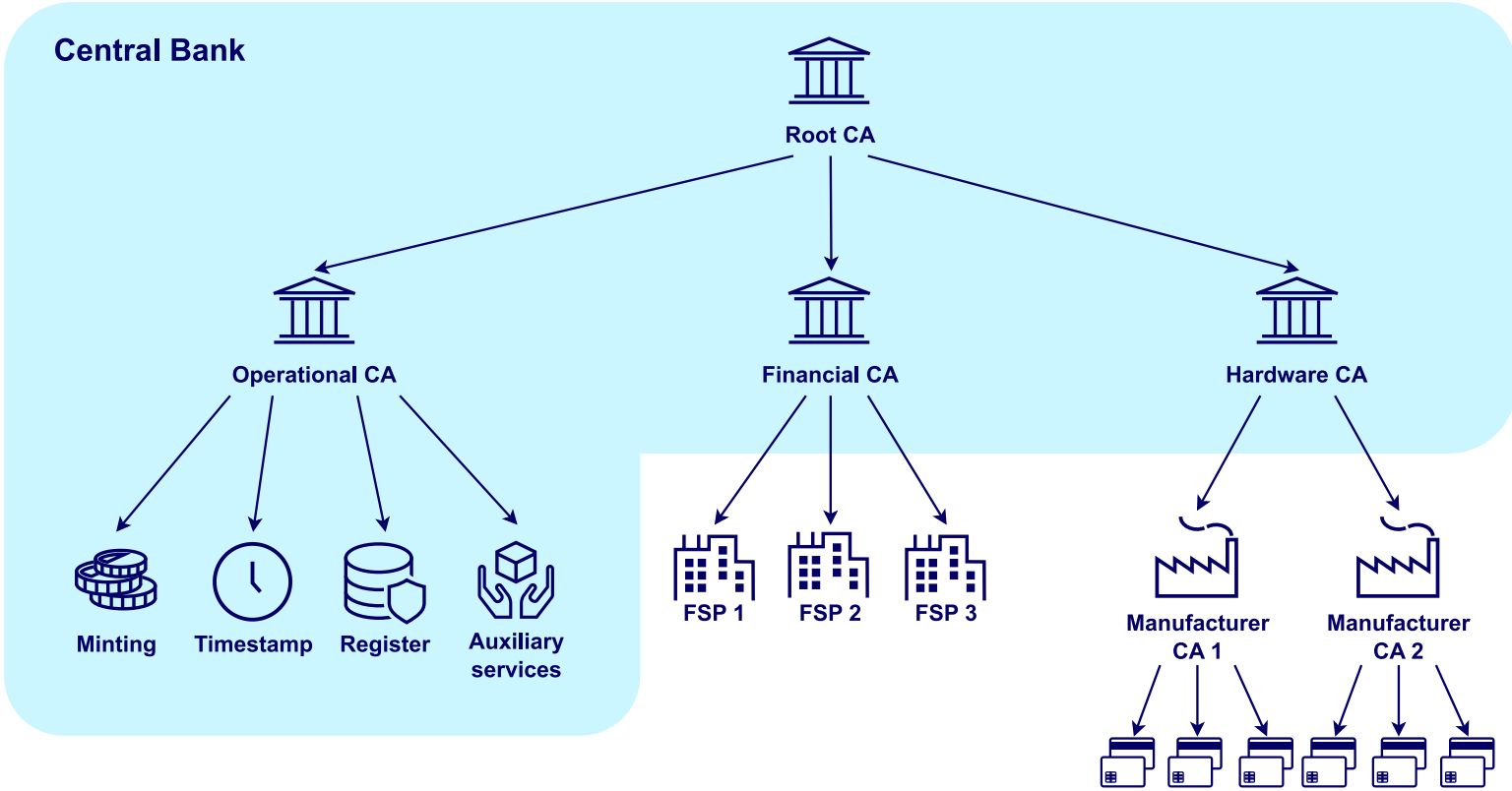
It is **difficult to ringfence** fraud in an account-based system.


Issuer as the final authority
Secure payment protocols & channels
Strong hardware security

Public Key Infrastructure is instrumental

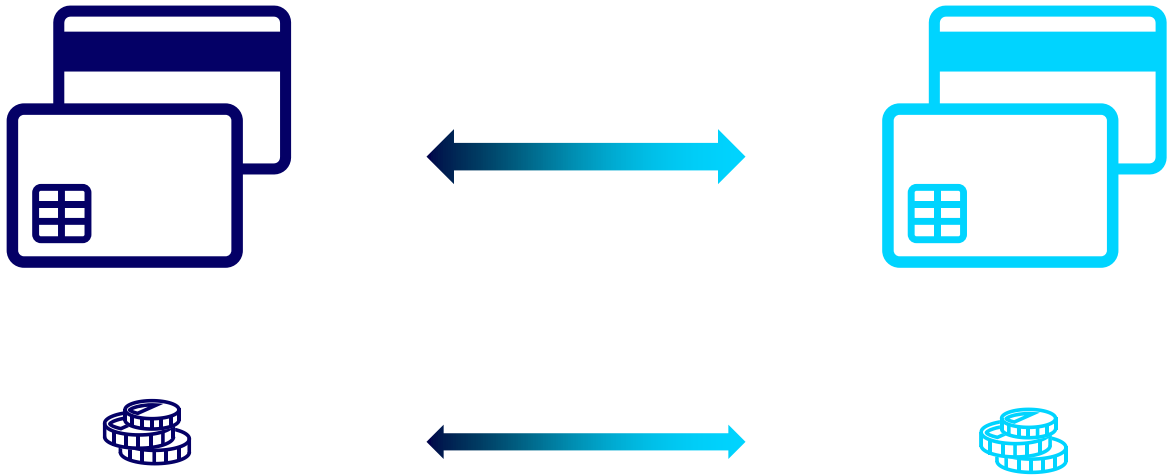
- there are many entities that require authentication:
  - issuer/central bank
  - intermediaries/banks
  - user wallets
  - merchants
  - card manufacturers
  - OEMs
  - …
- authenticates communication *and* application layer

https://arxiv.org/abs/2412.04051

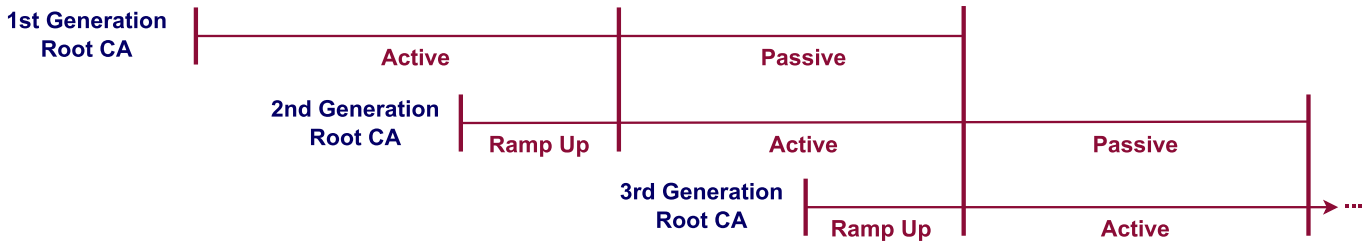

Central Bank
Root CA
Operational CA
Financial CA
Hardware CA
Minting
Timestamp
Register
Auxiliary services
FSP 1
FSP 2
FSP 3
Manufacturer CA 1
Manufacturer CA 2

(PQC) migration

- digital cash is by definition offline
- what happens if a wallet is offline for a long time?



→ wallets and tokens may need to evolve separately

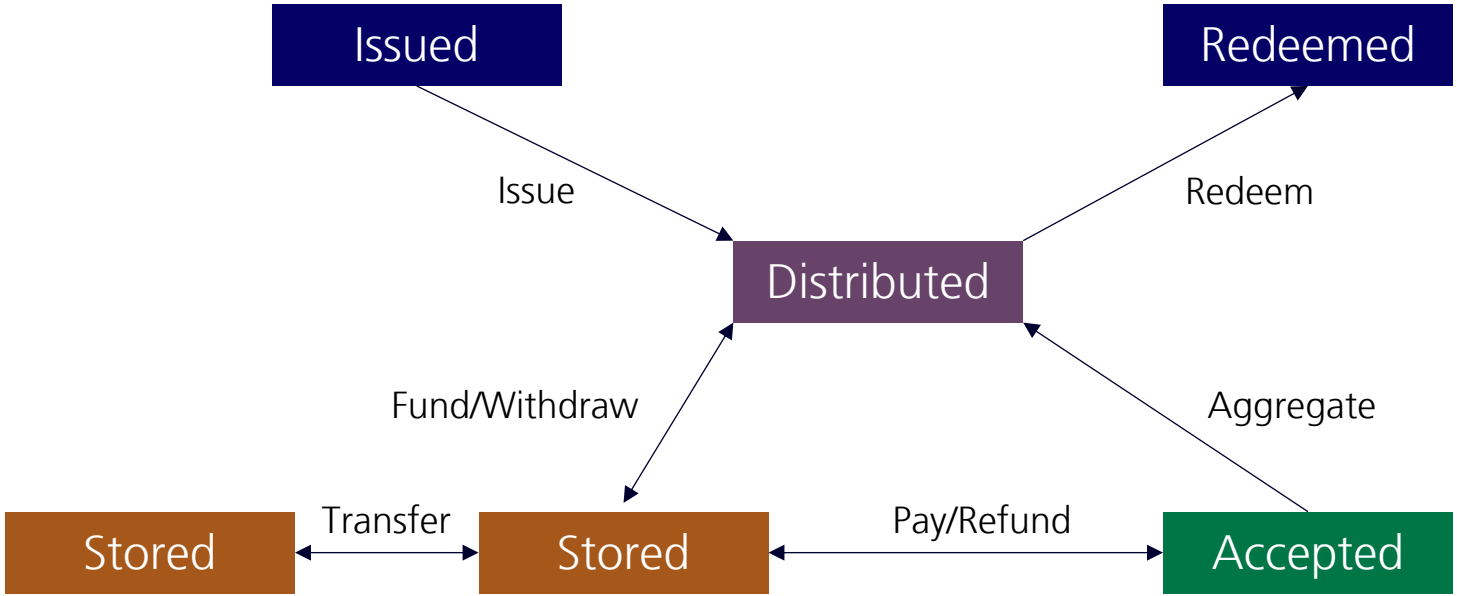

1st Generation
Root CA
Active
Passive
2nd Generation
Root CA
Ramp Up
Active
Passive
3rd Generation
Root CA
Ramp Up
Active
...

Digital cash issuance & lifecycle

Giesecke+Devrient
Creating Confidence


1001
DATE
15 02 2018
$
1600 00
Charity

Token lifecycle (ISO/DIS 13133)



Federal Office
for Information Security

Technical Guideline BSI TR-03179-1: Central Bank Digital Currency

Part 1: Requirements on backend systems

ISO

DRAFT
International Standard

ISO/DIS 13133

Financial Services — Security Reference Model for Digital Currency Hardware Wallet (SRM-DCHW)

ICS: 35.240.40

ISO/TC 68/SC 2

Secretariat: BSI

Voting begins on:
2025-08-29

Voting terminates on:
2025-11-21

This document has not been edited by the ISO Central Secretariat.

Reference number
ISO/DIS 13133:2025(en)

Conclusion

Giesecke+Devrient
Creating Confidence

Questions?
Answers!

Lars Hupel
https://lars.hupel.info
lars.hupel@gi-de.com