# Showcase of offline payments for digital currencies

**Lauren Del Giudice**

IDEMIA

27/01/2023

# Plan

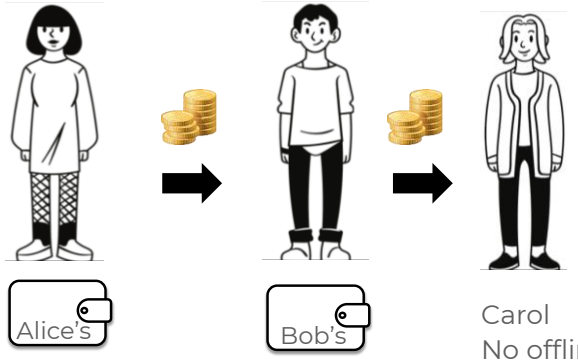
1. **Consecutive offline payment**
2. **Funding and defunding**
3. **Selecting the right secure elements for your offline wallet**
4. **Feedback on practical experimentation**
5. **Video**

# 1. Consecutive offline payment

# Overview

## Consecutive offline payment

OFFLINE

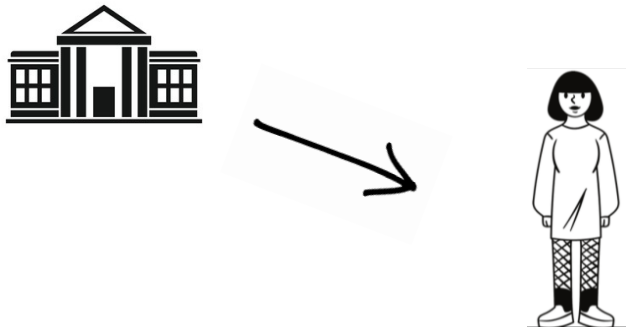



## Funding/defunding

ONLINE


## Financial aid

OFFLINE



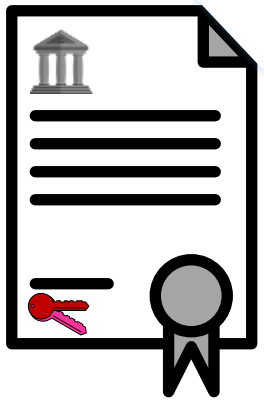
## Controls on offline payments

OFFLINE

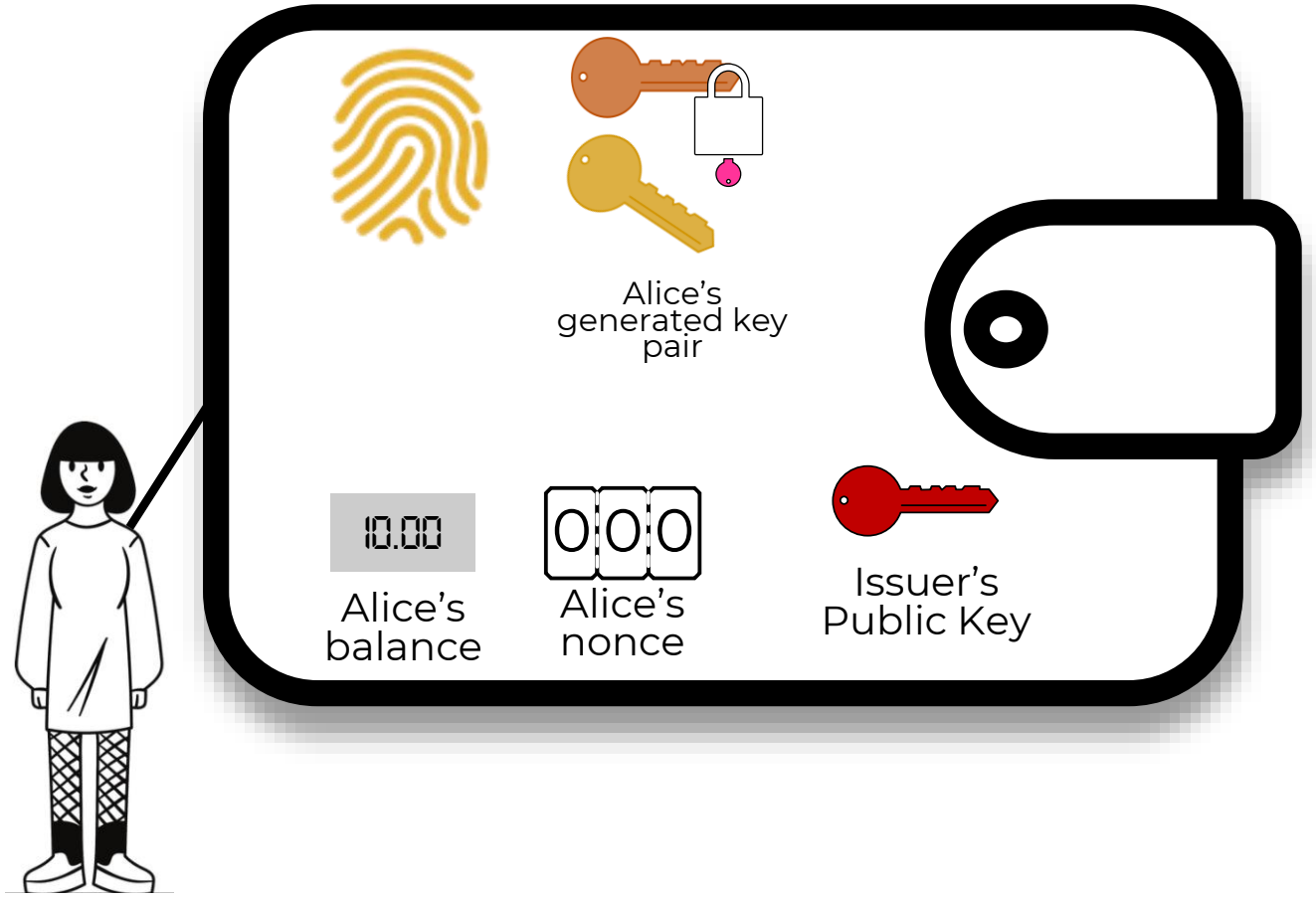
# Consecutive offline payment

- Immediate settlement finality
- Decreasing the load on server side

# Alice obtains her offline wallet

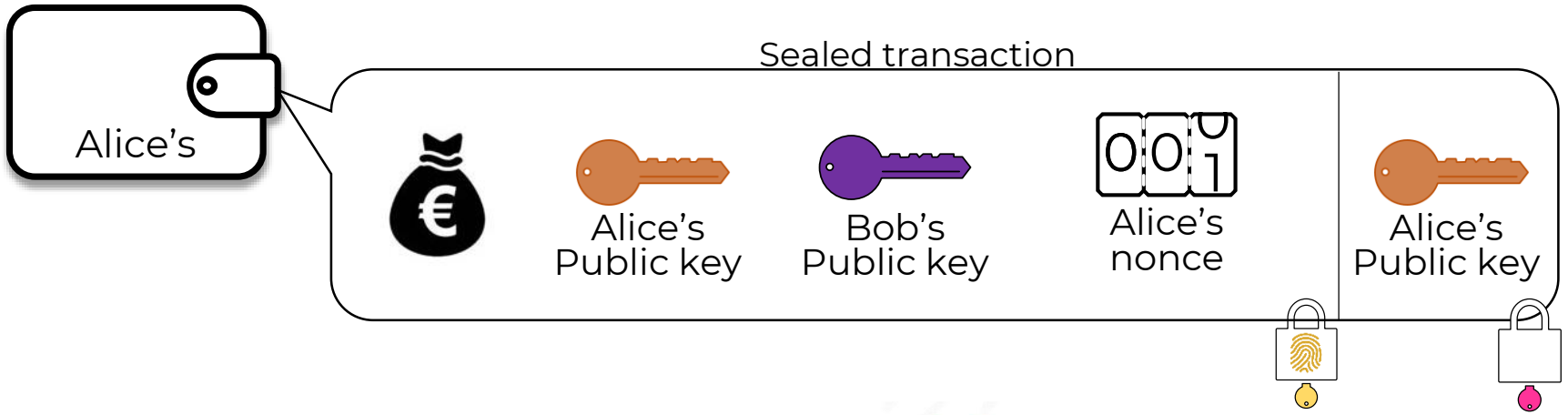


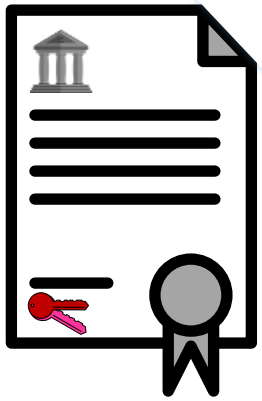
Original Issuer
Decentralized or centralized authority

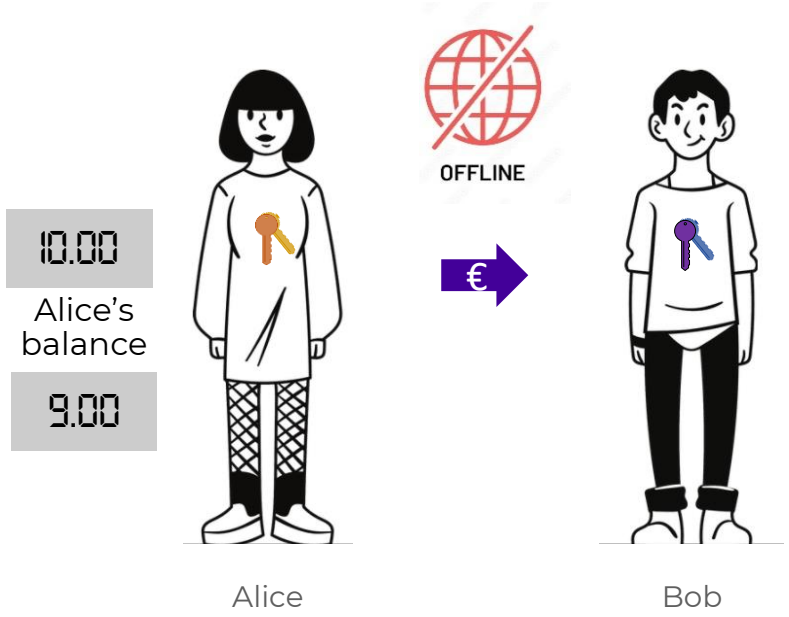



Alice

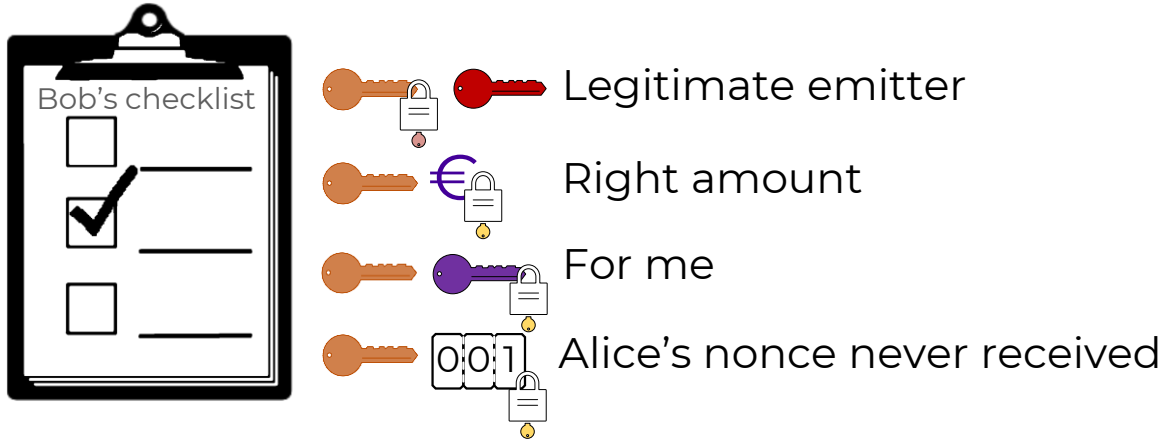
# Alice *seals* one payment for Bob

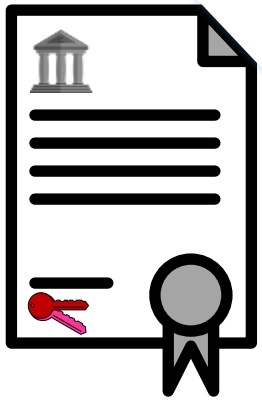


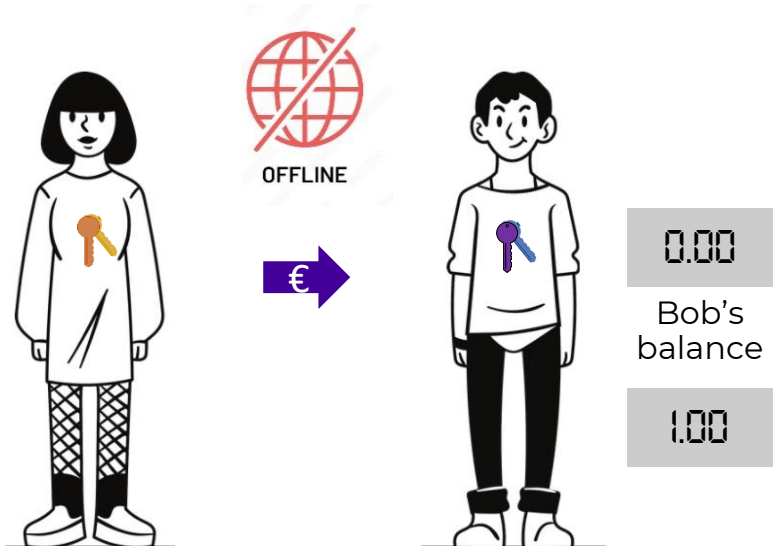





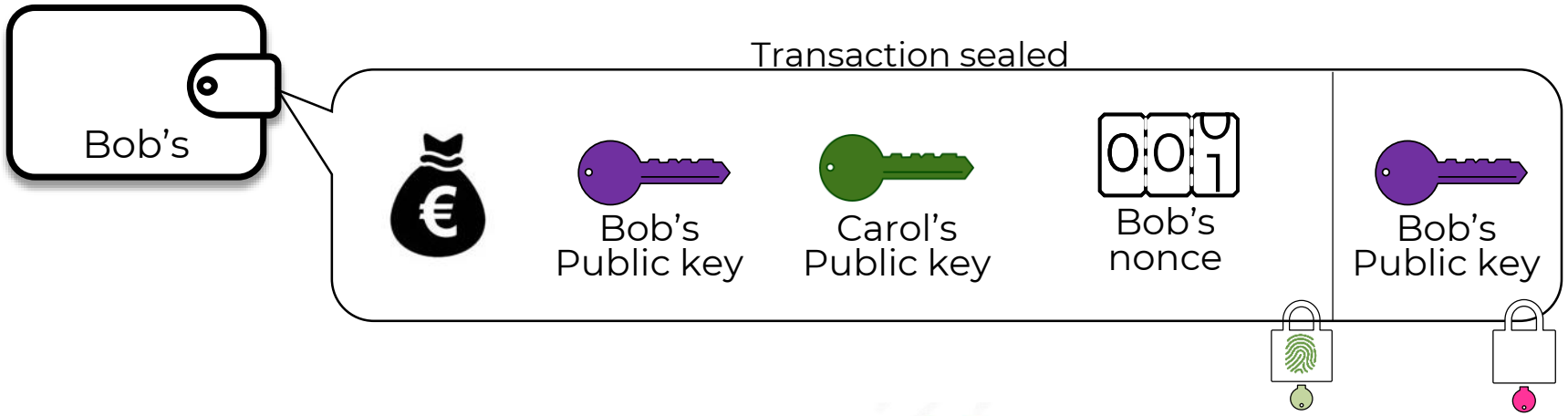
# Bob credits his offline wallet

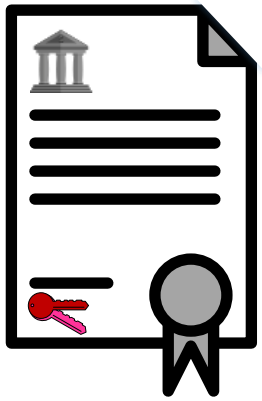


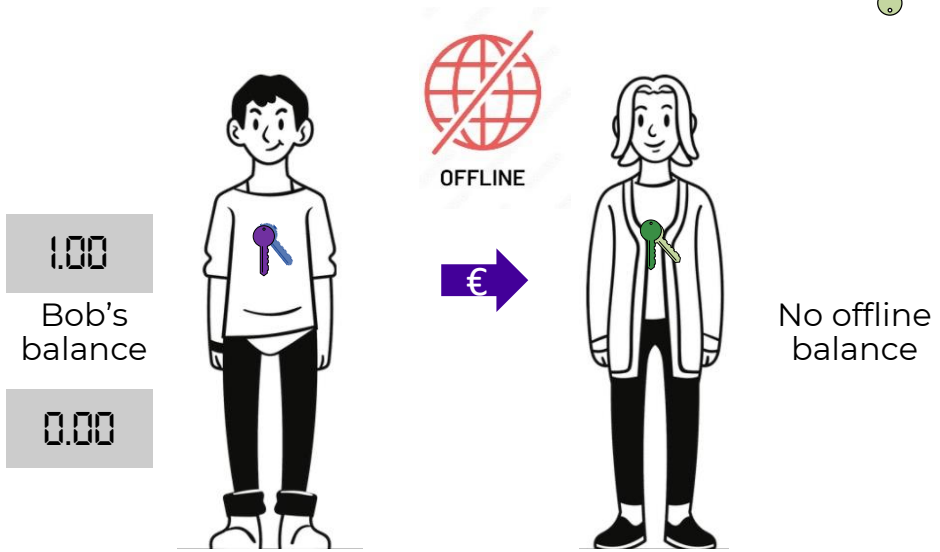





# Bob *seals* one payment for Carole

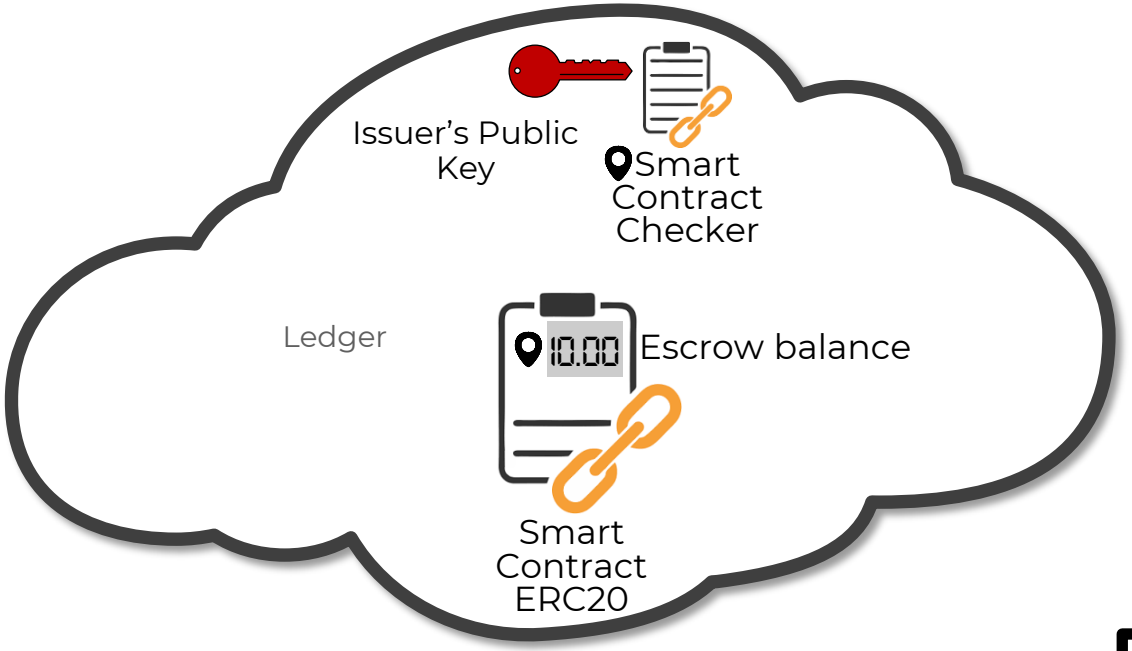


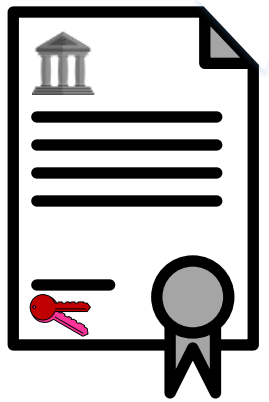





# 2. Funding/Defunding

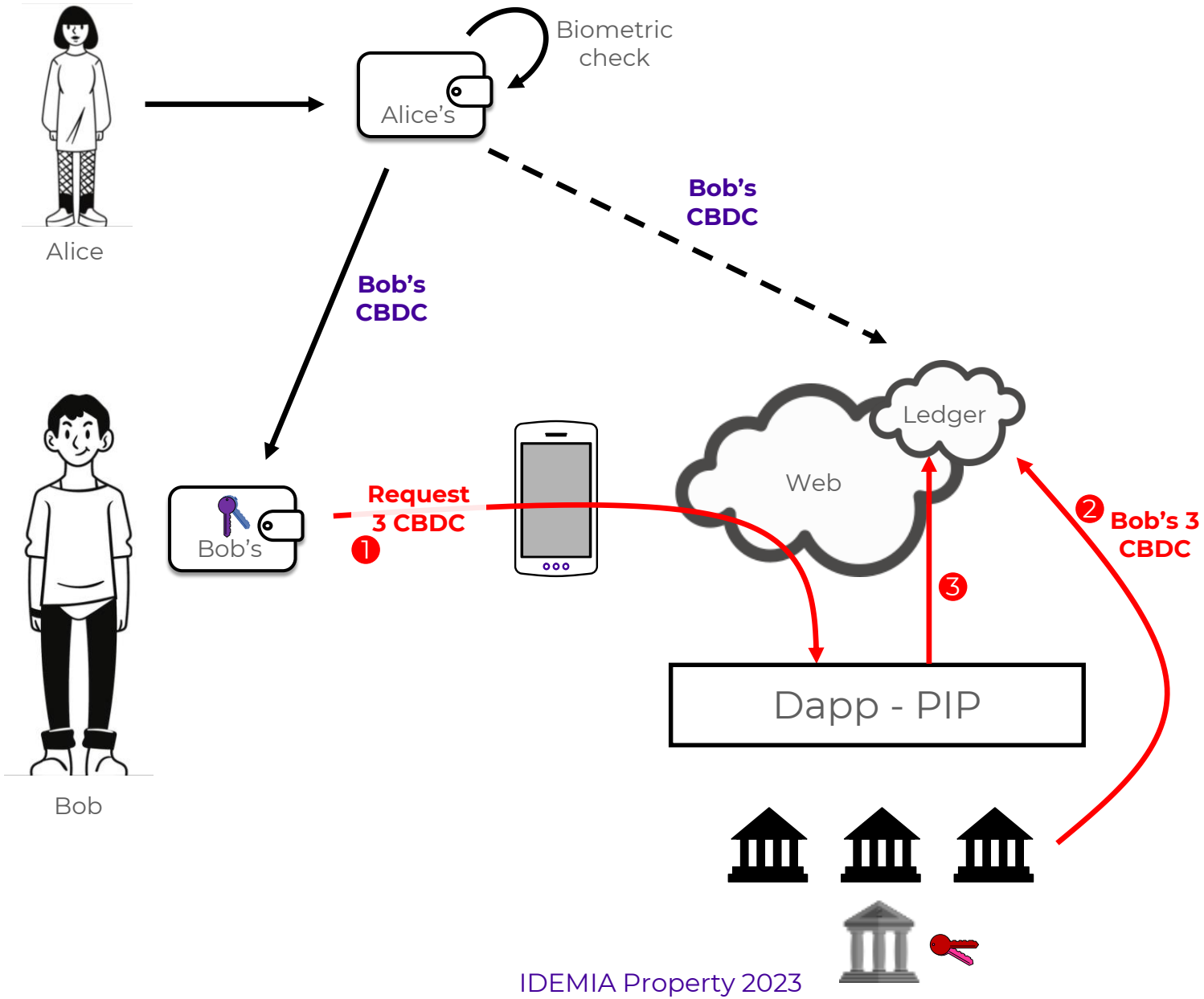
# Online



Original Issuer
Decentralized or centralized authority

# Bob's funding online → offline

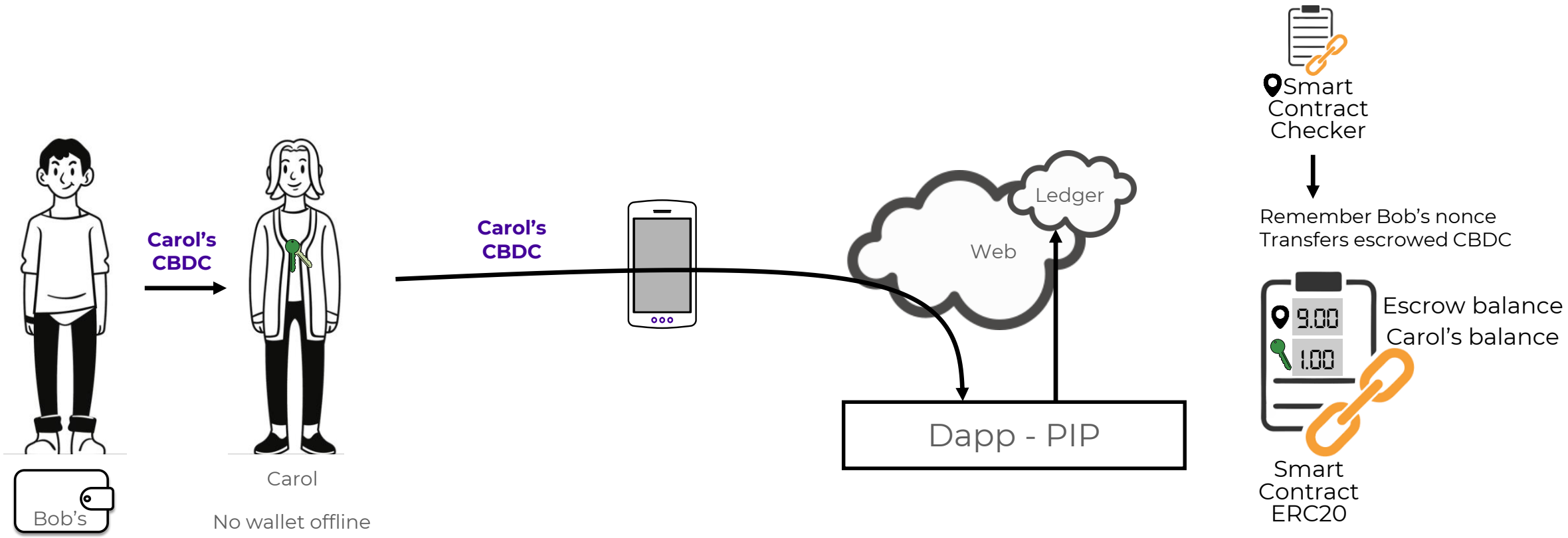



Transfer +3 CBDC to escrow

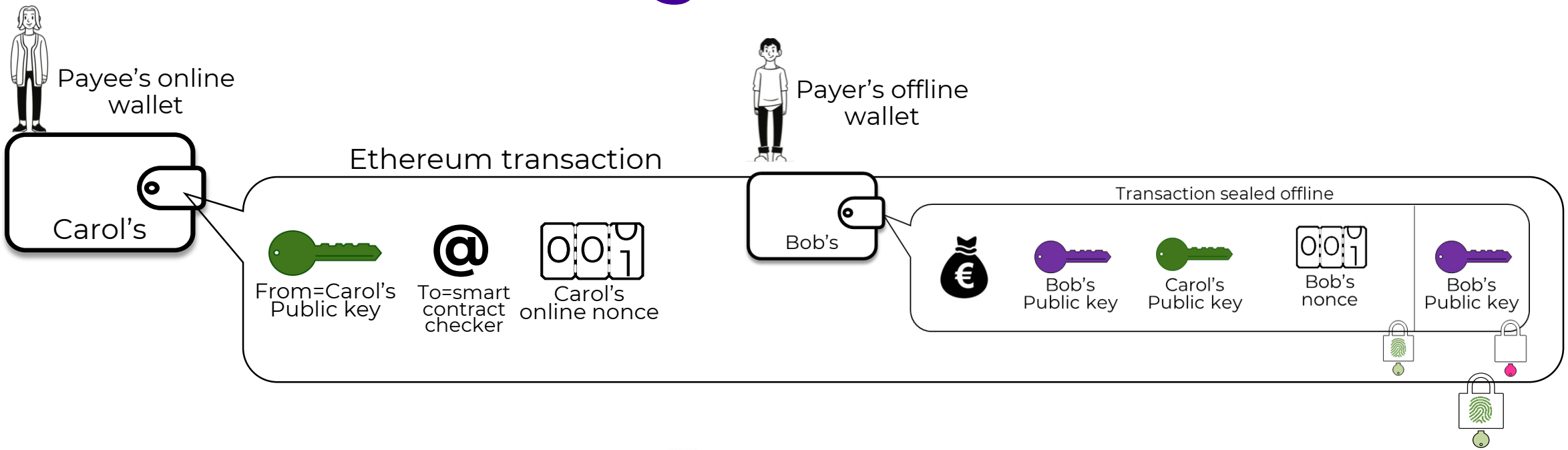

Escrow balance

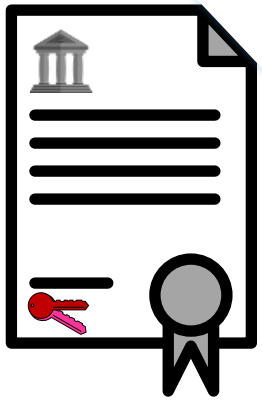
Smart Contract ERC20

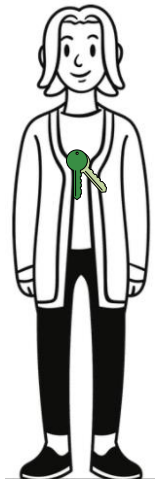
# Carol's defunding offline → online



# Carol's defunding



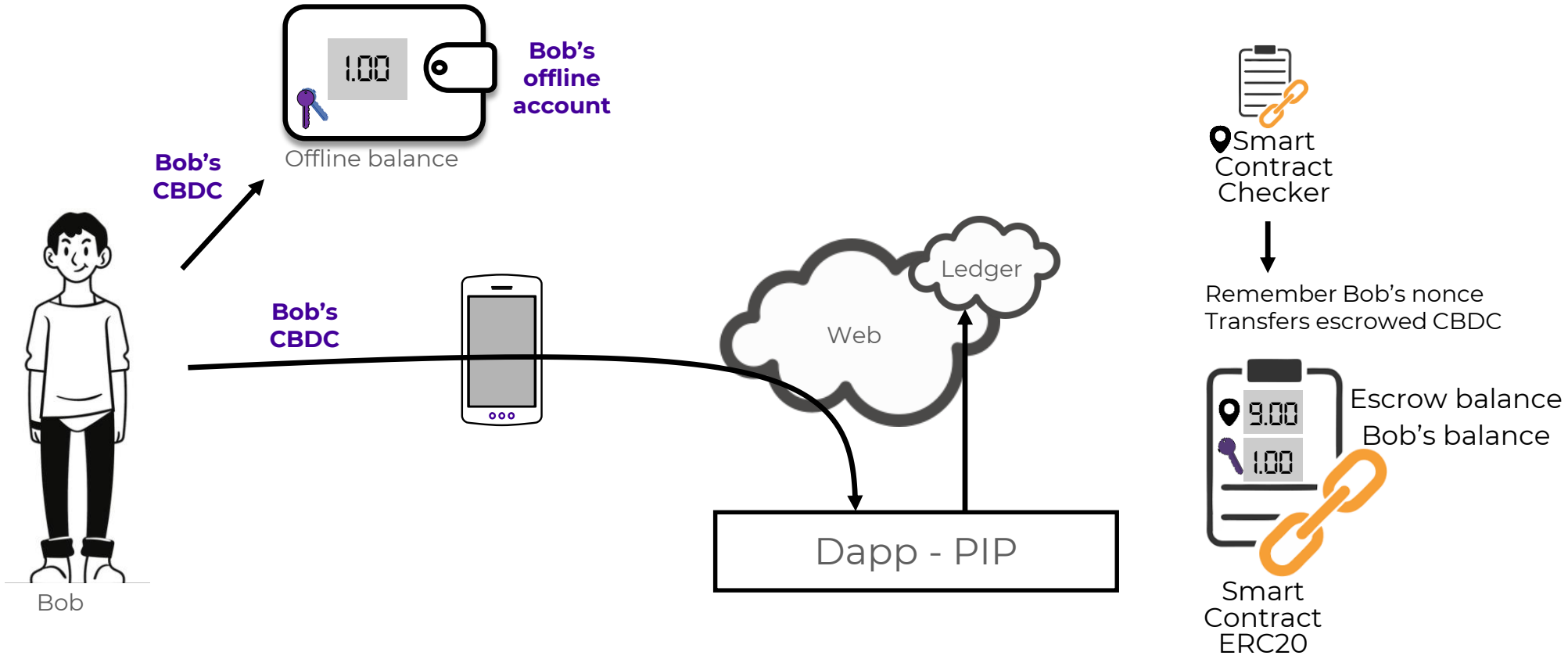


Carol

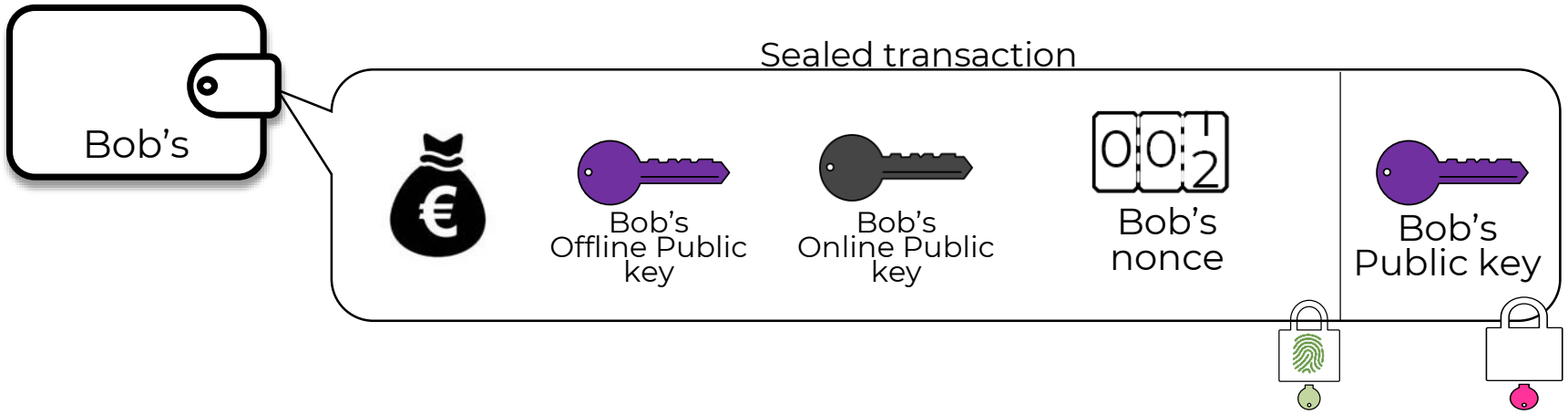
# Being ledger agnostic

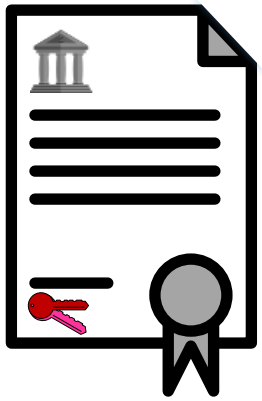
- Programmability
- Cryptography
- Account based or token based: does it matter?

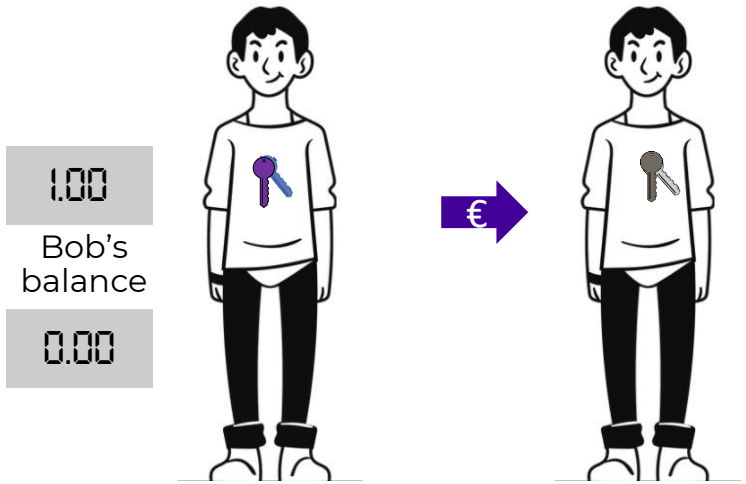
# What if Bob frauds? Double income



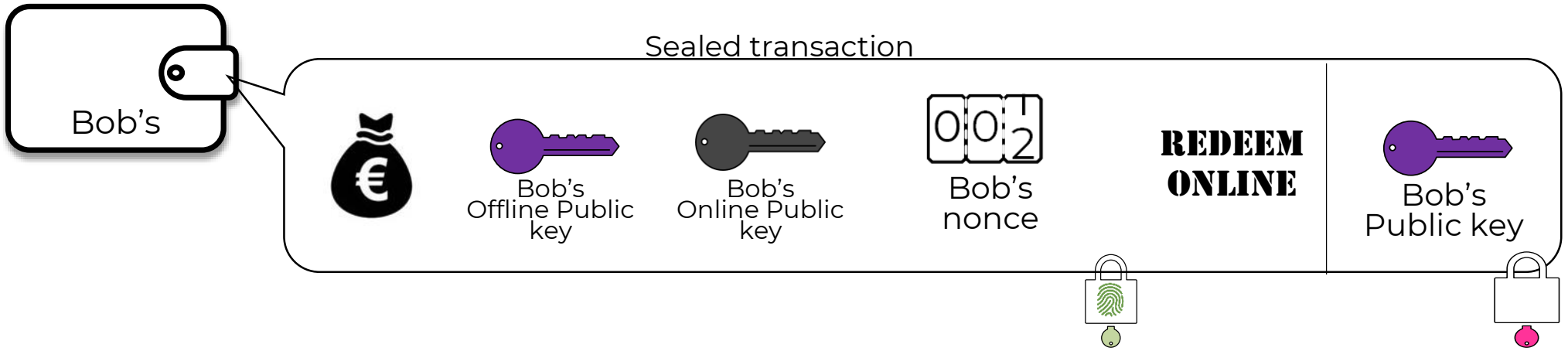
# Bob *seals* one payment for Bob

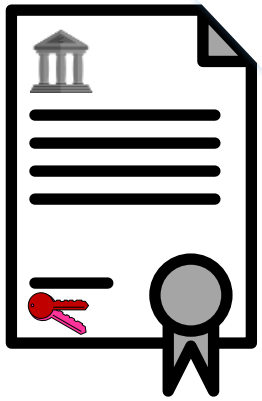


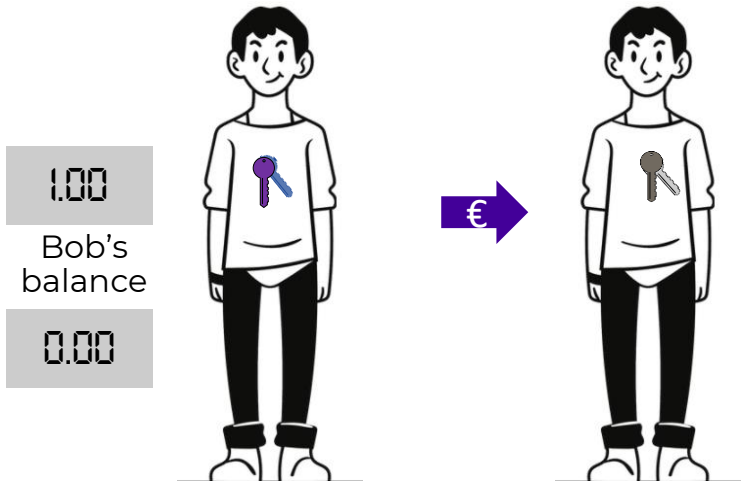





# Bob *seals* one payment for Bob - Amd

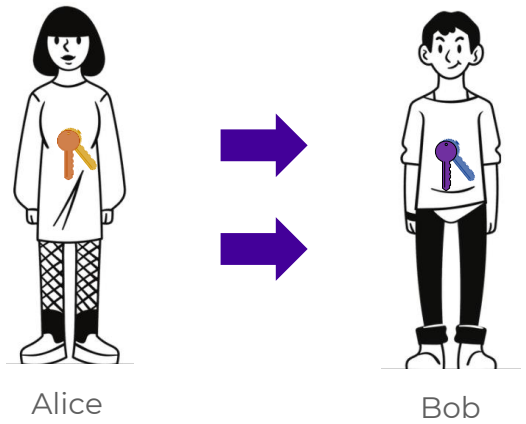


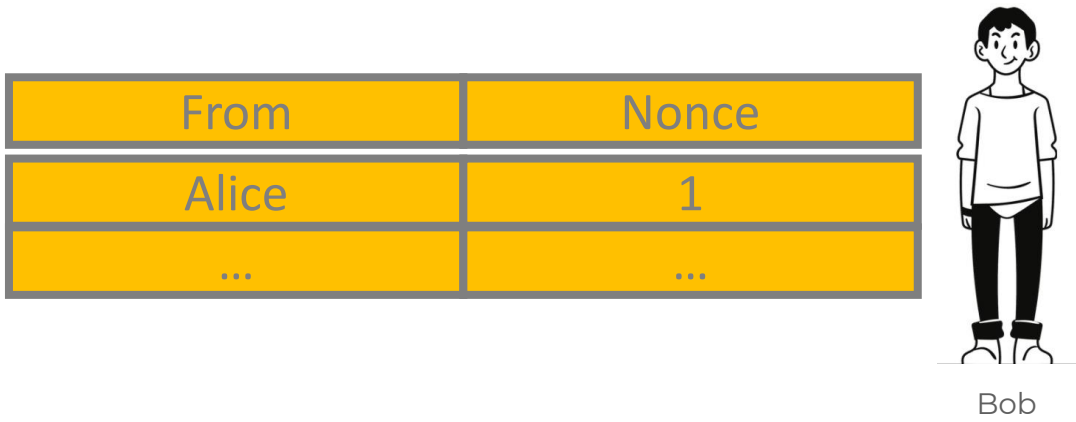





# Replay

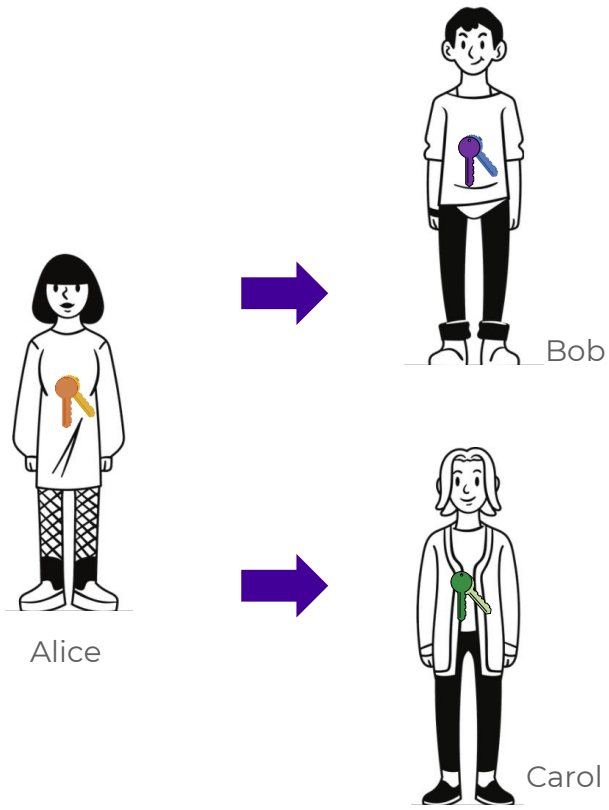
- Alice re-sends the *same* transaction to Bob
  - **Offline** - The payee's device needs to track the previously received nonces
  - **Defunding online** - The smart contract Checker needs to track the previously received nonces



# Double spending

- Alice sends the same token twice with the same nonce
  - Different recipient
  - Different amount



# Double spending (con’t)

- Alice has no access to her private keys
  - No way to generate a transaction bypassing the offline wallet

Alice

# 3. Selecting the right secure elements for your offline wallet

# Offline wallet on the field: required protection

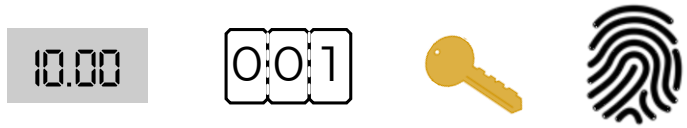
Modification of data, code
**T.Phys-Manipulation**

Malfunction due to stress
**T.Malfunction**

Abuse of Functionality
**T.Abuse-Func**


Disclosure of data by physical probing or leakage (emanations, variation in power consumption, changes in processing time, …)
Cloning
**T.Phys-Probing, T.Leak-Inherent**

Deficiency of random number (e.g key generation)
**T.RND**




Assets

**Risk: generating money**

# Choosing the right security

**Rich Execution Environment**

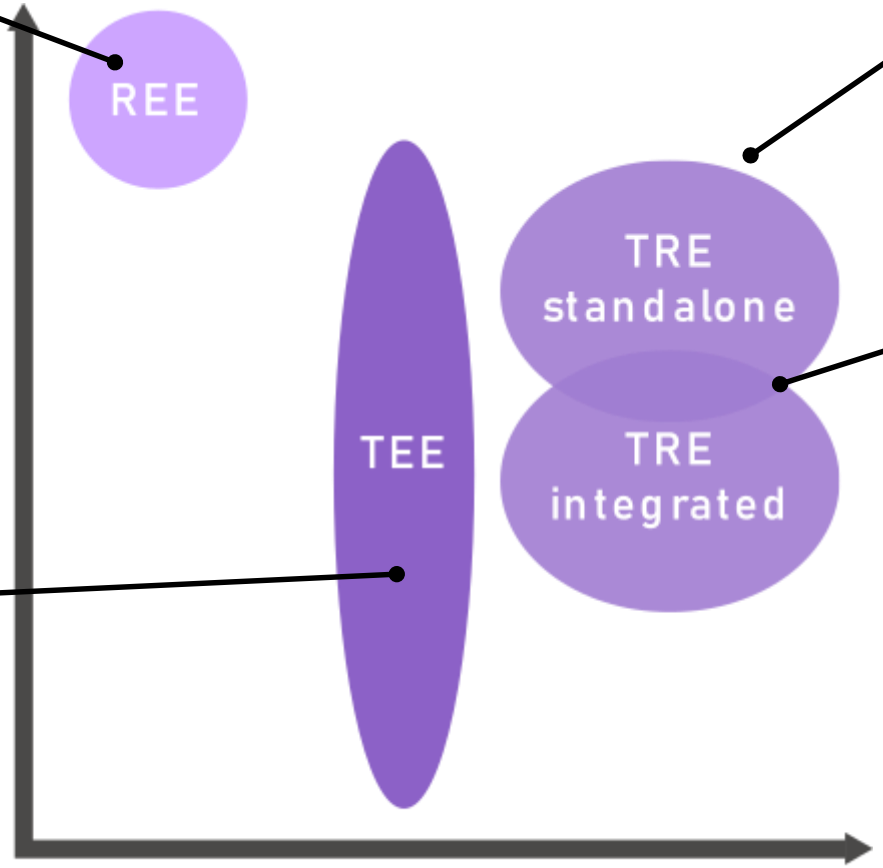
Microsoft Windows

android

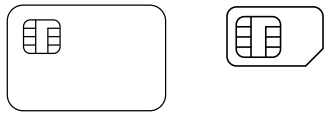
**Trusted Execution Environment**

intel SGX

TrustZone® System Security by ARM



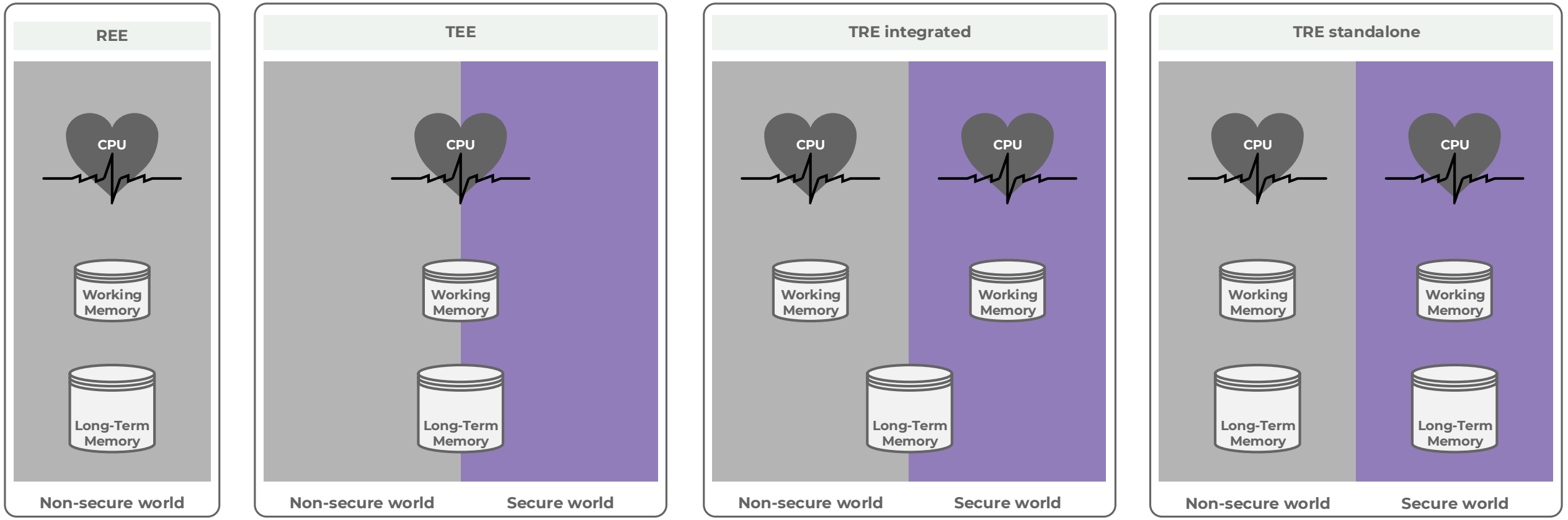

**Tamper Resistant element standalone**



**Tamper Resistant element integrated**

SEP

Qualcomm SPU


REE
CPU
Working Memory
Long-Term Memory
Non-secure world
TEE
CPU
Working Memory
Long-Term Memory
Non-secure world
Secure world
TRE integrated
CPU
CPU
Working Memory
Working Memory
Long-Term Memory
Non-secure world
Secure world
TRE standalone
CPU
CPU
Working Memory
Working Memory
Long-Term Memory
Long-Term Memory
Non-secure world
Secure world

# Payer vs payee

- The payer needs a secure element
- The payee does not

# 4. Feedback on practical experimentation

# Payer-Payee Communication

- QR codes: Reduce data size for easy scanning!

  Binary to Text encoding to generate QR code
  - EMV: TLV and Base64 encoding (Textual representation)
    - Represents binary data (=a sequence of 8-bit bytes) in sequences of 24 bits
  - We chose TL and ISO 8859 encoding
    - Keeps binary data (=a sequence of 8-bit bytes) in a sequence of 8 bits

  - Simple versus mutual authentication
  - Asynchronous is convenient

# Communication (con’t)

- BLE
- NFC