Webinar

Java Card Forum

Secured hardware for digital currencies

Timo Lisk

System Architect
Java Card Forum Board Member

Agenda

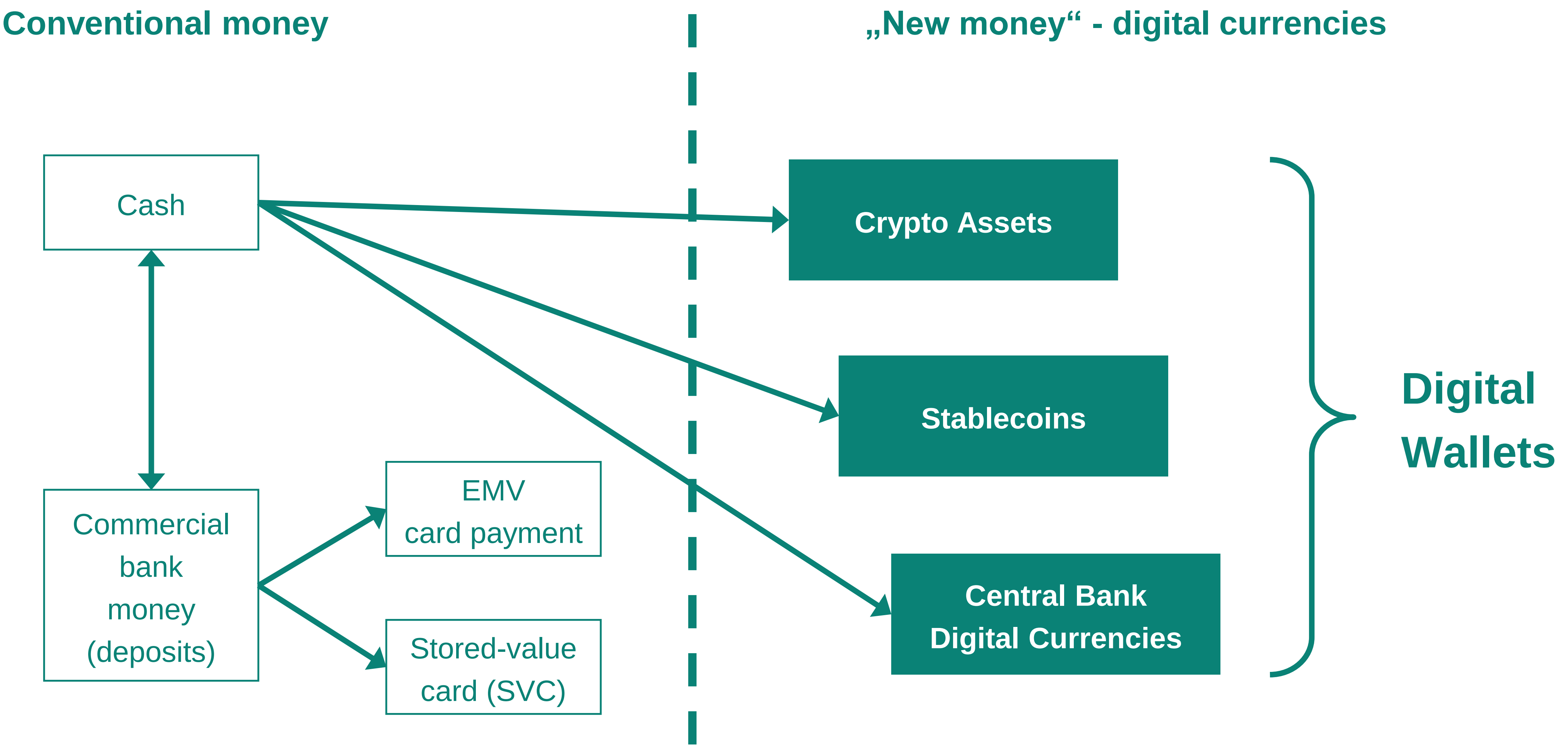
1 Introduction to different types of digital currencies

2 Types of secured hardware devices to protect digital transactions

3 Java Card support for digital currency cryptography

Introduction to different types of digital currencies

Digital Currencies – a new form of money



Conventional money

„New money“ - digital currencies

Cash

Commercial bank money (deposits)

EMV card payment

Stored-value card (SVC)

Crypto Assets

Stablecoins

Central Bank Digital Currencies

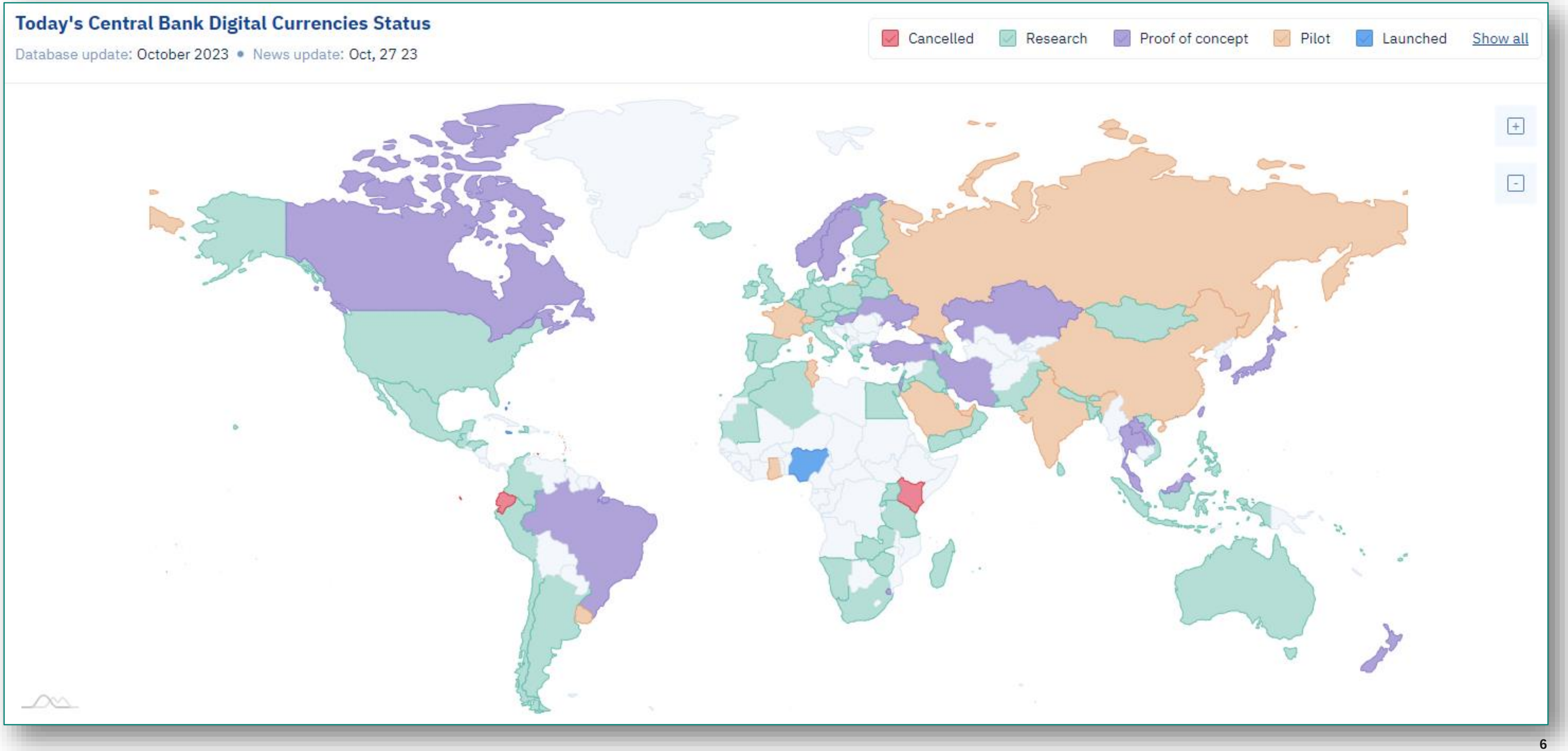
Digital Wallets

Digital Currencies – „New forms of money“

Crypto Assets	Stablecoins	Central Bank Digital Currencies
$ 1 trillion market capitalization	$ 125 billion market capitalization	A CBDC is, besides cash and bank deposits, a third form of money available for the general public that is meant to be used as a means of payment (example: Euro Area). A CBDC provided by the central bank has to tackle a specific user need and has to have advantages compared to private sector alternatives so that citizens indeed use it.
Largest project: – Bitcoin (50% market share)	Largest project: – USDT (70% market share) – Latest project announcement: PayPal stablecoin PYUSD	
Use cases: • New asset class • Digital store of value (scarce digital asset) • Means of payment	Use cases: • Cross-border payments • PoS, e-com, P2P payments • M2M payments • Hedging instrument	

Credits: Dr. Jonas Gross, Digital Euro Association

CBDCTracker.org



Today's Central Bank Digital Currencies Status

Database update: October 2023 • News update: Oct, 27 23

🟥 Cancelled 🟩 Research 🟪 Proof of concept 🟧 Pilot 🟦 Launched Show all

Some of the risks involved when using digital currencies

Lost value

- „you are your own boss“
- no 3rd party can help
- protect your keys!

Double-spending

- P2P transactions in offline mode
- trust on sender and recipient devices without relying on connectivity

Cyber fraud

- wallets are connected to the internet
- the internet is an entrance gate for all kind of cyber attacks

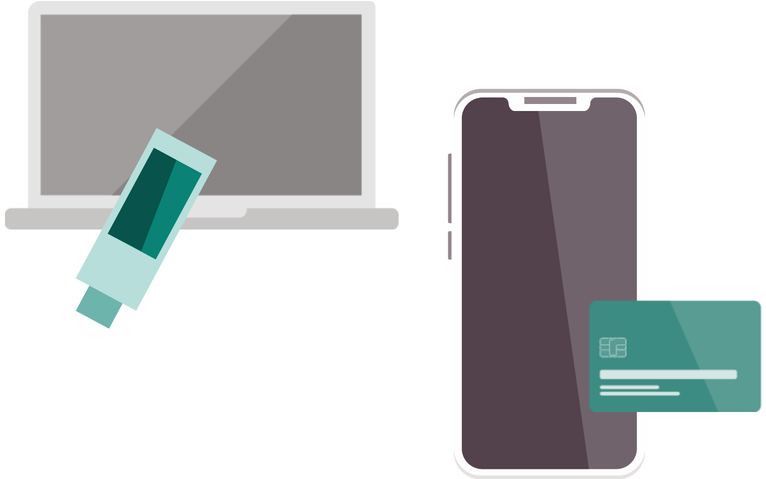
Impersonation

- identity theft
- weak passwords
- second-factor authentication!

Types of secured hardware devices to protect digital transactions

Examples with Hardware-based Security

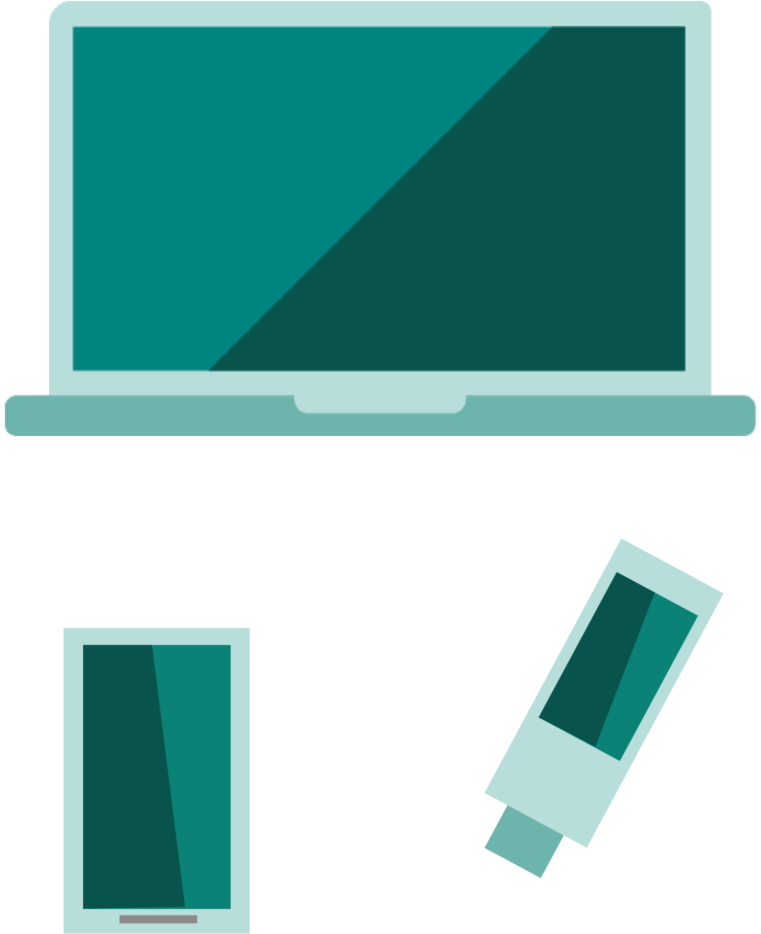
Crypto Assets	Stablecoins	CBDC
Example: Bitcoin, Ethereum	**Example: Tether (USDT)**	**Example: Digital Euro, Yuan etc.**
› Blockchain Technology	› Smart contracts based on blockchain	› Various digital ledger technologies
› Decentralized mining & transactions	› Can be M2M secure endpoints	› Central Bank driven (regional)
› Hardware (Cold) Wallets	› Embedded Secure Elements (SE)	› Card, Smartphone



Crypto Asset Examples

+ M2M

Crypto Assets – USB sticks or companion devices



- Cold storage for digital crypto wallets
  → storing cryptocurrency keys offline
  → prevent access from attackers

- Hot storage digital wallets are connected to the internet
  → vulnerable to cyber fraud, lost value and impersonation

- **„NOT YOUR KEYS, NOT YOUR COINS“**

- Keys are stored ideally in a certified security chip or alternatively in a Secure Execution Environment (SEE) on a separate device

- Device connects to your laptop or smartphone via USB or bluetooth

- App for desktop or mobile manages your offline coins

Examples

LEDGER | TREZOR | ELLIPAL

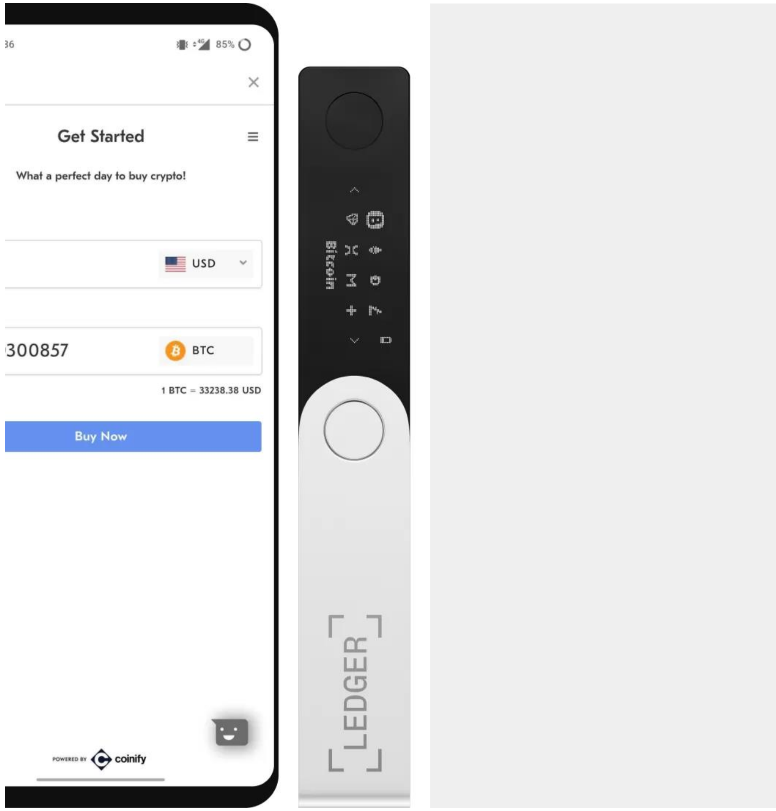


Photo: www.legder.com

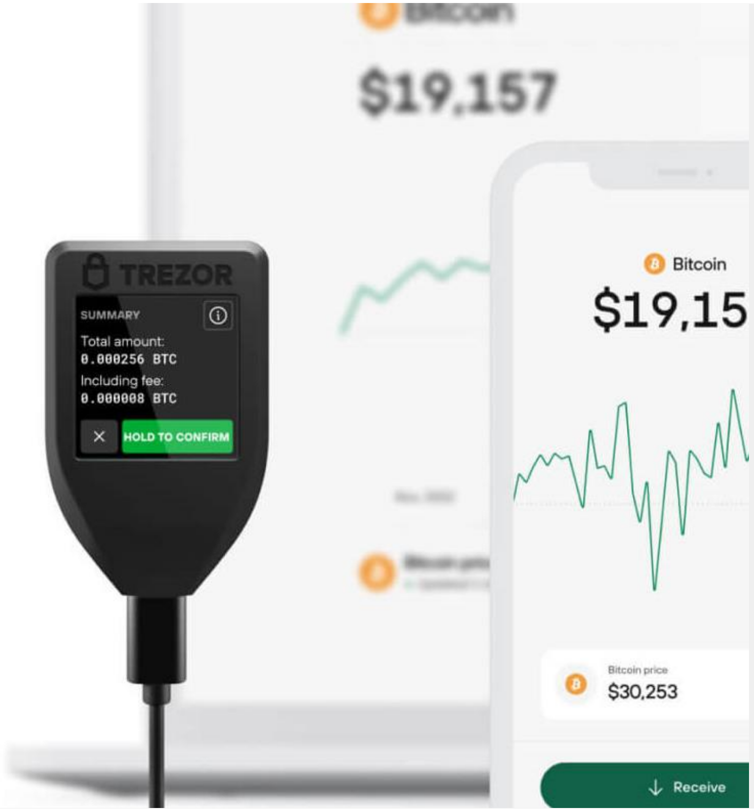


Photo: www.trezor.io

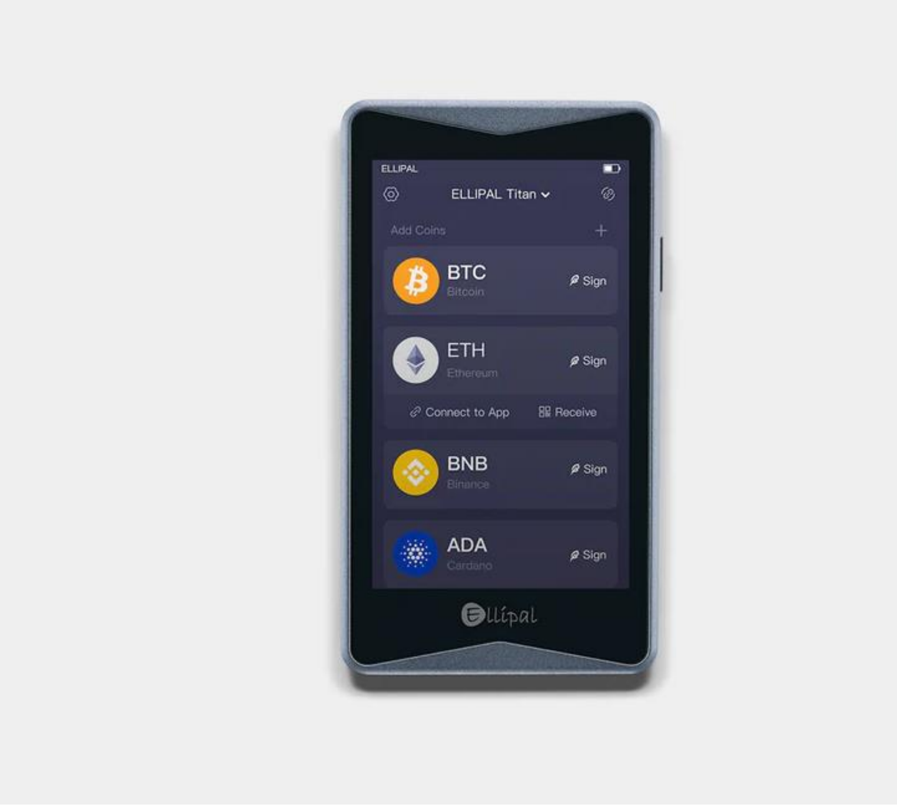


Photo: www.ellipal.com

Please note that the products displayed are for illustrative purposes only and serve as real-life examples of the use case discussed. This does not imply any partnership with Infineon nor does it exclude this. Moreover, there may be other products that serve the same use case and are not displayed.

Crypto Assets - Card

- Key creation, management and digital signature for crypto transactions on a certified security chip in a smart card
- Digital Wallet App to manage your digital currencies
- „Air Gap“ by tapping the card to the mobile wallet only during key generation or transaction
- Can be used for other use cases as well:
  - FIDO second-factor authentication
  - Traditional EMV card payment transactions

Examples

AMMER CARD

Photo: www.ammer.cards

ARCULUS

Photo: www.getarculus.com

SATOCHIP

Photo: www.satochip.io

Please note that the products displayed are for illustrative purposes only and serve as real-life examples of the use case discussed. This does not imply any partnership with Infineon nor does it exclude this. Moreover, there may be other products that serve the same use case and are not displayed.

Stablecoin – M2M use case

Photo: https://cash-on-ledger.com/fully-automatic/ & Lindner Traktoren

CashOnLedger

Use case:

- Pay-per-use rental model based on blockchain
- Automated rental and billing process using smart contracts stored on the blockchain
- The solution maximizes the efficiency of transactions between the parties
- It is used to gather data for inventory optimization
- Authentication of machines

Please note that the products displayed are for illustrative purposes only and serve as real-life examples of the use case discussed. This does not imply any partnership with Infineon nor does it exclude this. Moreover, there may be other products that serve the same use case and are not displayed.

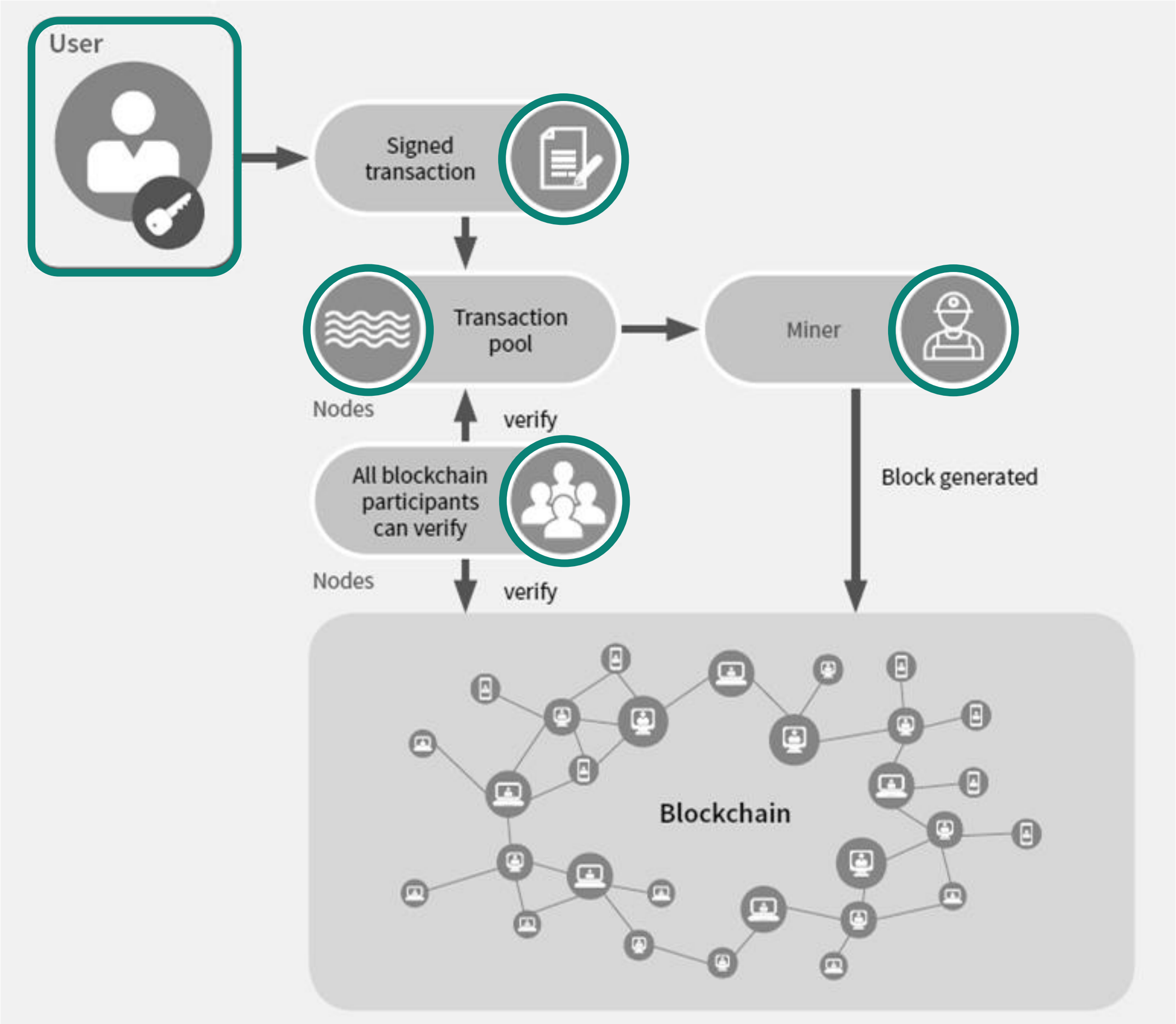
Offline CBDC transactions

1. Resilience
2. Cash resemblance
3. Inclusion
4. Lack of developed communication infrastructure
5. Privacy
6. Lower transaction costs
7. Performance and scalability support
8. Universal access
9. Civil contingency
10. Trust
11. Making digital peer-to-peer (P2P) and person-to-business (P2B) payments

Source: BIS – Project Polaris - https://www.bis.org/publ/othp64.htm

Java Card support for digital currency cryptography

Blockchain Security

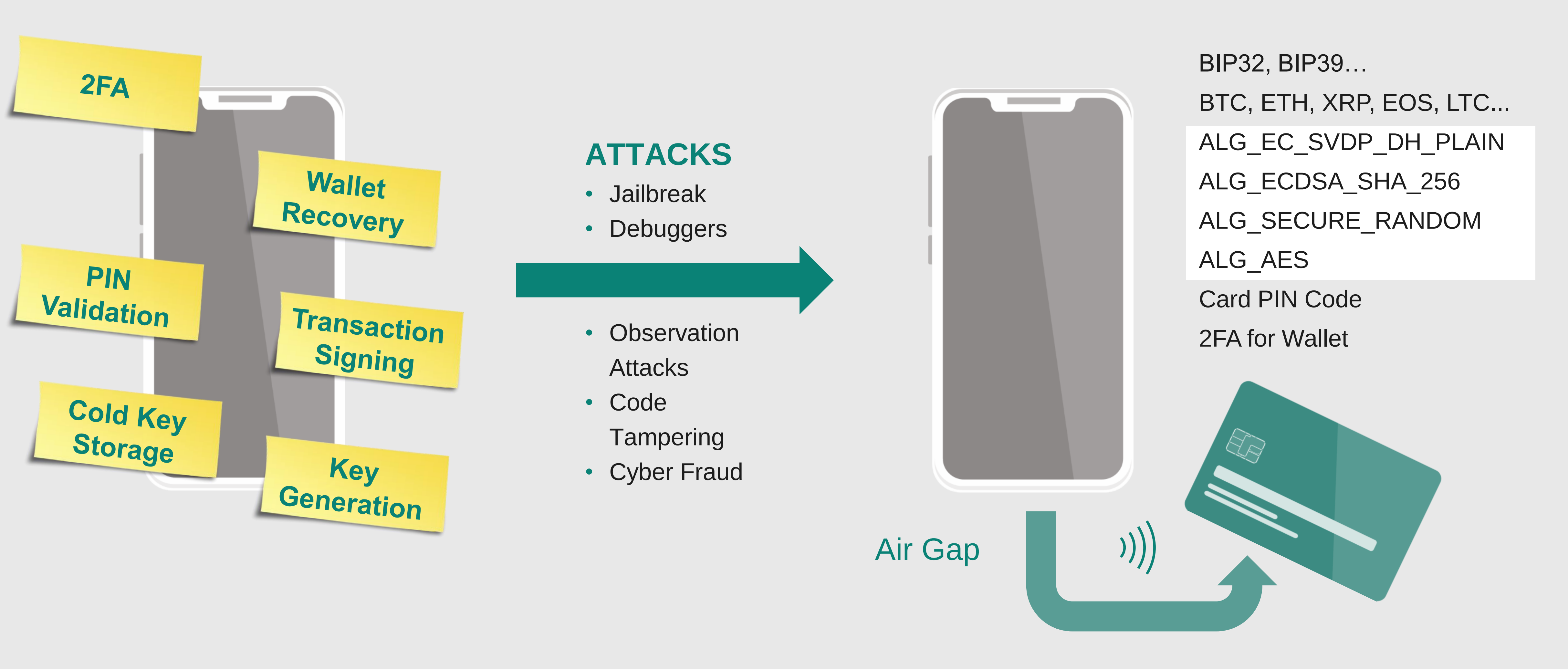


- **Blockchain infrastructure** provides **inherent security**

- **Private key**, identity and **security credential**, enables **interaction with blockchain**

- **Secured storage** of the **private key** is **essential**

From „Hot Wallets“ to Cold Wallets



ATTACKS

- Jailbreak
- Debuggers

- Observation Attacks
- Code Tampering
- Cyber Fraud

BIP32, BIP39…

BTC, ETH, XRP, EOS, LTC...

ALG_EC_SVDP_DH_PLAIN

ALG_ECDSA_SHA_256

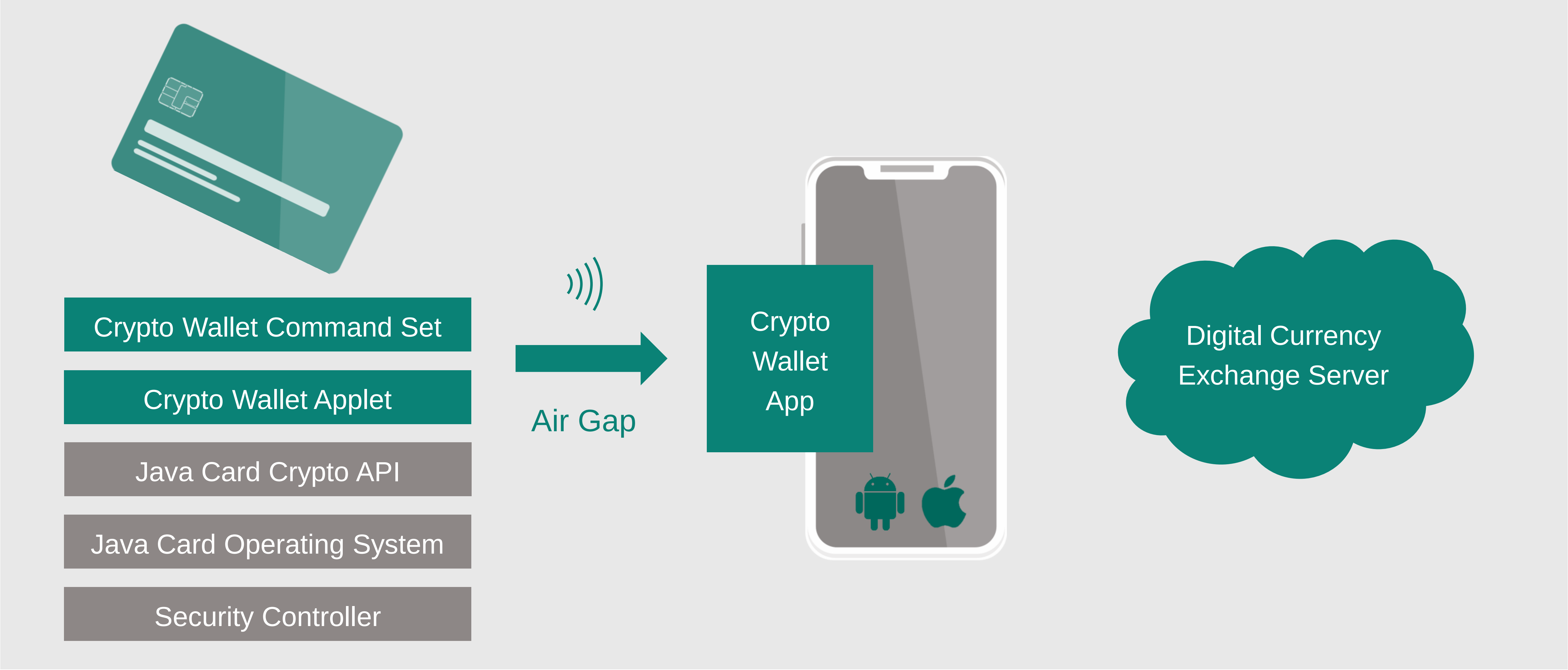
ALG_SECURE_RANDOM

ALG_AES

Card PIN Code

2FA for Wallet

Cold Wallet Architecture on Java Card



Crypto Wallet Command Set

Crypto Wallet Applet

Java Card Crypto API

Java Card Operating System

Security Controller

Air Gap

Crypto Wallet App

Digital Currency Exchange Server

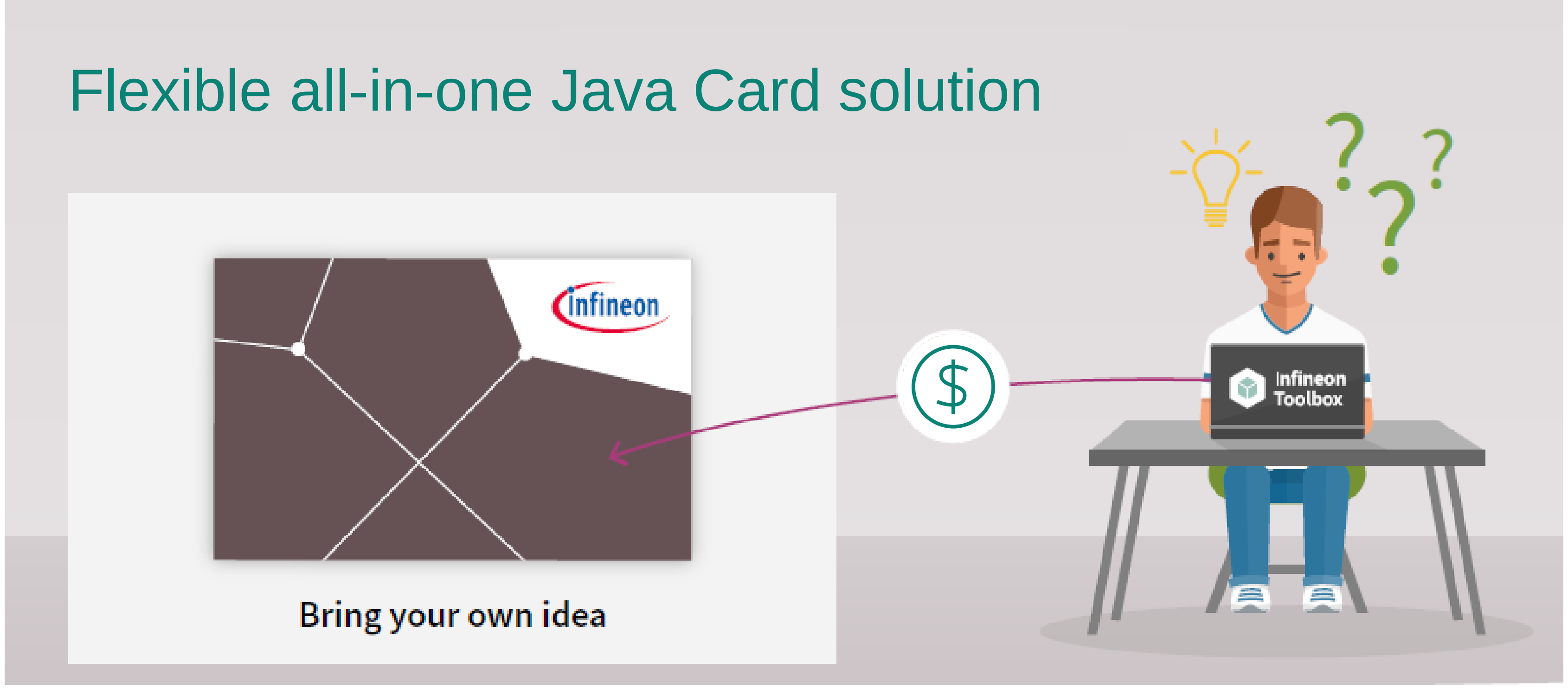
Java Card cryptography for Cold Wallets

- Secured key **generation and derivation**
  - non-deterministic:
    - on chip key pair generation (RNG)
  - deterministic:
    - seed from mnemonic words (HMAC_SHA512 in PBKDF2 based on BIP39)
    - master node and child node key derivation (HMAC_SHA512, RIPEMD160 based on BIP32, modular addition)

- Secured Elliptic Curve based **signature and transaction**
  - Koblitz SECP256K1 – typical (Bitcoin/Etherium...)
  - NIST SECP256R1 – (SLIP10) rather used in IoT
  - Edward Ed25519 – (SLIP10) future

- Secured **backup and key restorage**
  - User centric key recovery based on BIP39 and seed import

SECORA^{TM} ID



Flexible all-in-one Java Card solution

Bring your own idea

- Maximum customization
- Real open platform
- Eclipse based development tools
- Development trainings and support
- Composite certification enabled

More information: https://www.infineon.com/cms/en/product/promopages/secora-id

Webinar

Java Card Forum

Secured hardware
for digital currencies

in www.linkedin.com/in/lisk