Blockchain and Cryptocurrency Conference (B2C'2023),
18 - 20 October 2023, Corfu, Greece

SECURING PRIVACY IN OFFLINE PAYMENT FOR RETAIL CENTRAL BANK DIGITAL CURRENCY : A COMPREHENSIVE FRAMEWORK

Olivier ATANGANA[1,2], Morgan BARBIER[1], Lyes KHOUKHI[1], Willy ROYER[2]

1 Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
2 FIME EMEA, 14000 Caen, France

Thomas-Olivier.atangana@unicaen.fr; morgan.barbier@unicaen.fr;
lyes.khoukhi@ensicaen.fr; willy.royer@fime.com

GREYC
Electronics and Computer Science Laboratory

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

fime

OUTLINE

01 INTRODUCTION

02 PROTOCOL OVERVIEW AND SYSTEM OPERATION

03 FUTURE INTEGRATION AND EXPANSION

04 CONCLUSIONS

INTRODUCTION

Emerging Context of Central Bank Digital Currency

01

01 INTRODUCTION

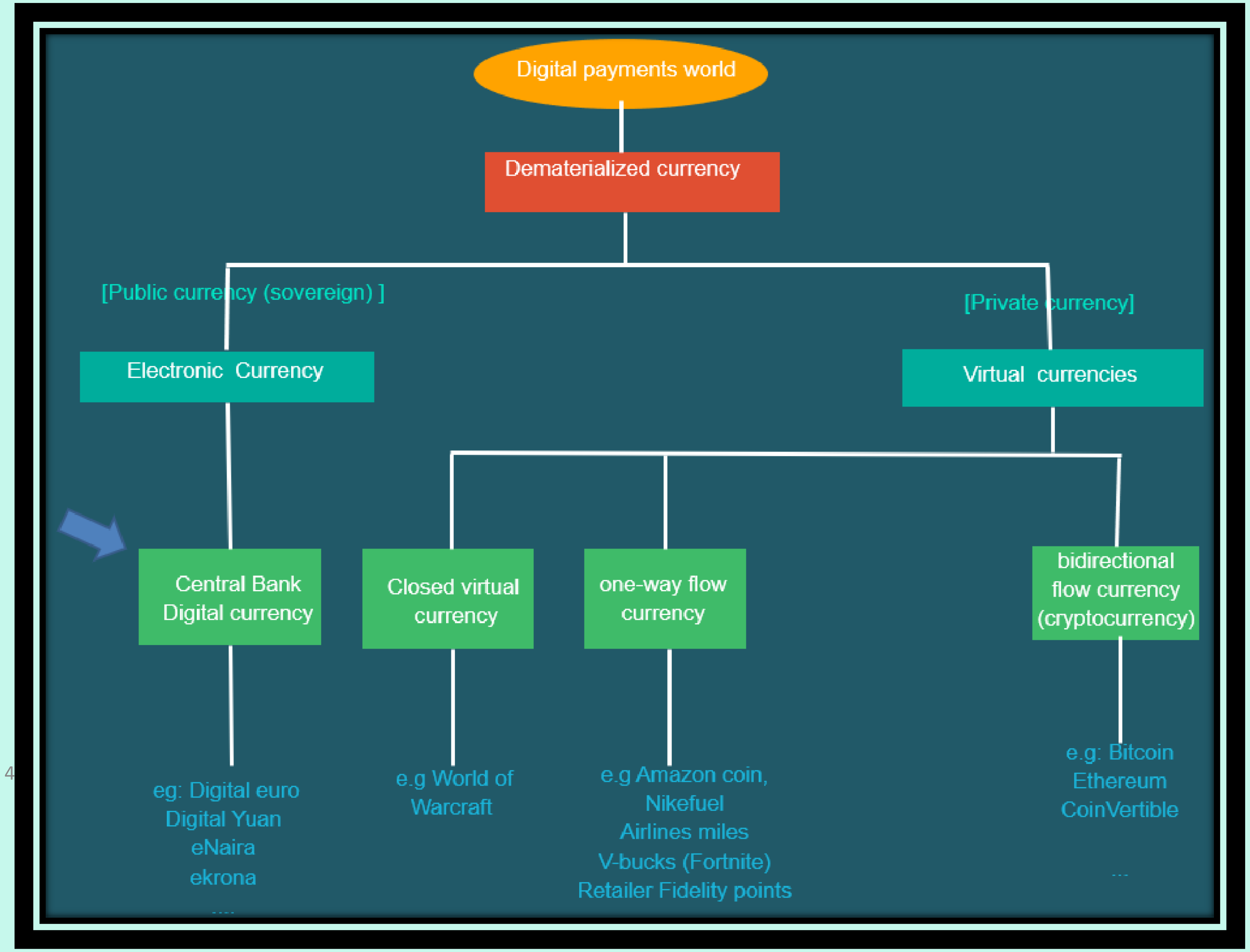
-What's Central Bank Digital currency(CBDC)?

Digitalization of fiat money backed by Central Bank Digital Currency

2 kind of CBDC : Wholesale CBDC, Retail CBDC, Hybrid CBDC

-Emerging Context

Rise of Cryptocurrencies Post-2008 financial crisis



Digital payments world

Dematerialized currency

[Public currency (sovereign)]

[Private currency]

Electronic Currency

Virtual currencies

Central Bank Digital currency

Closed virtual currency

one-way flow currency

bidirectional flow currency (cryptocurrency)

eg: Digital euro
Digital Yuan
eNaira
ekrona
....

e.g World of Warcraft

e.g Amazon coin,
Nikefuel
Airlines miles
V-bucks (Fortnite)
Retailer Fidelity points

e.g: Bitcoin
Ethereum
CoinVertible
...

Fig.1. Dematerialized currencies world

01 INTRODUCTION

- rCBDC'S Challenges

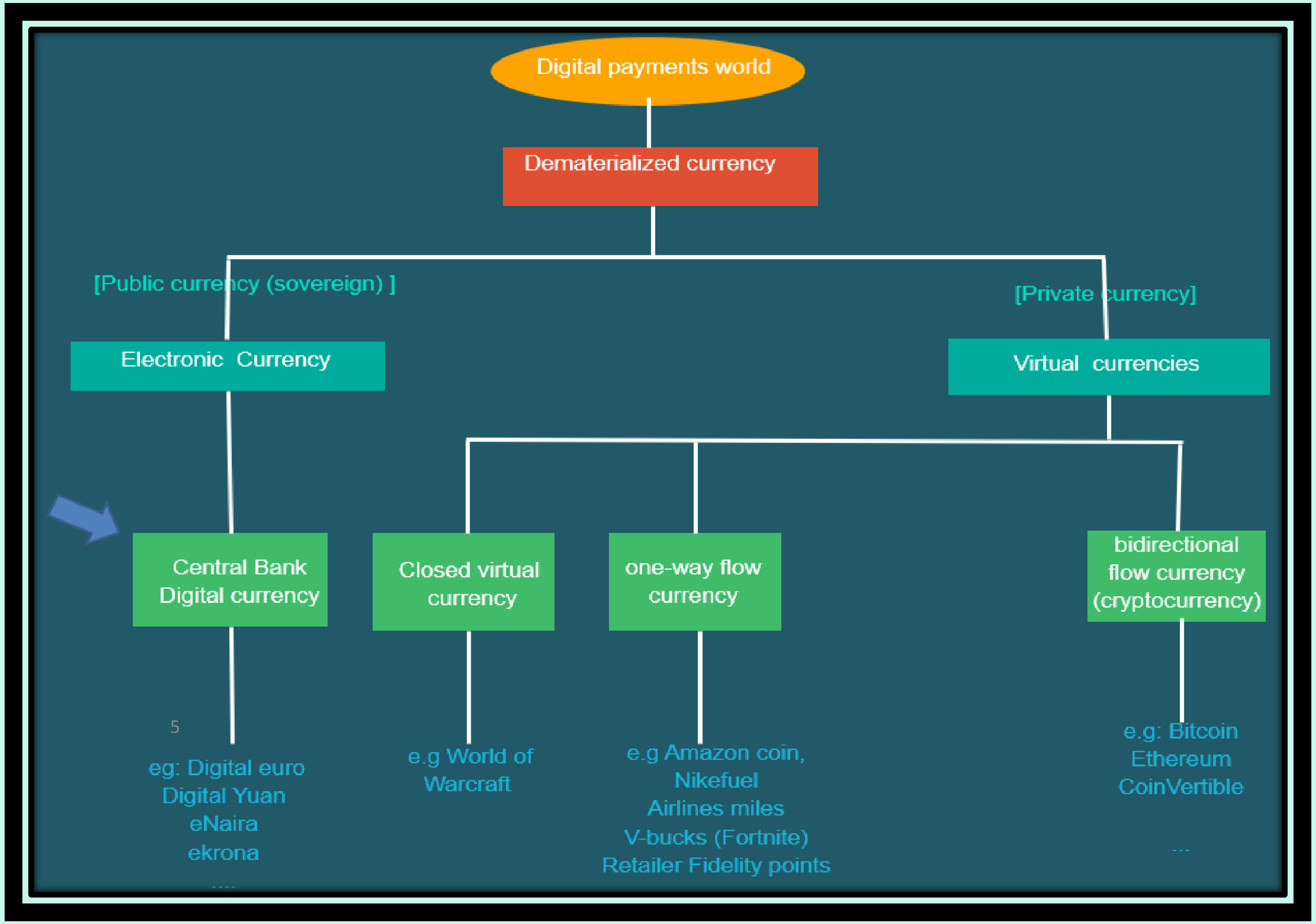
Security

Privacy

Offline payment function

Interoperability

...



Digital payments world

Dematerialized currency

[Public currency (sovereign)]

[Private currency]

Electronic Currency

Virtual currencies

Central Bank Digital currency

Closed virtual currency

one-way flow currency

bidirectional flow currency (cryptocurrency)

5

eg: Digital euro
Digital Yuan
eNaira
ekrona
....

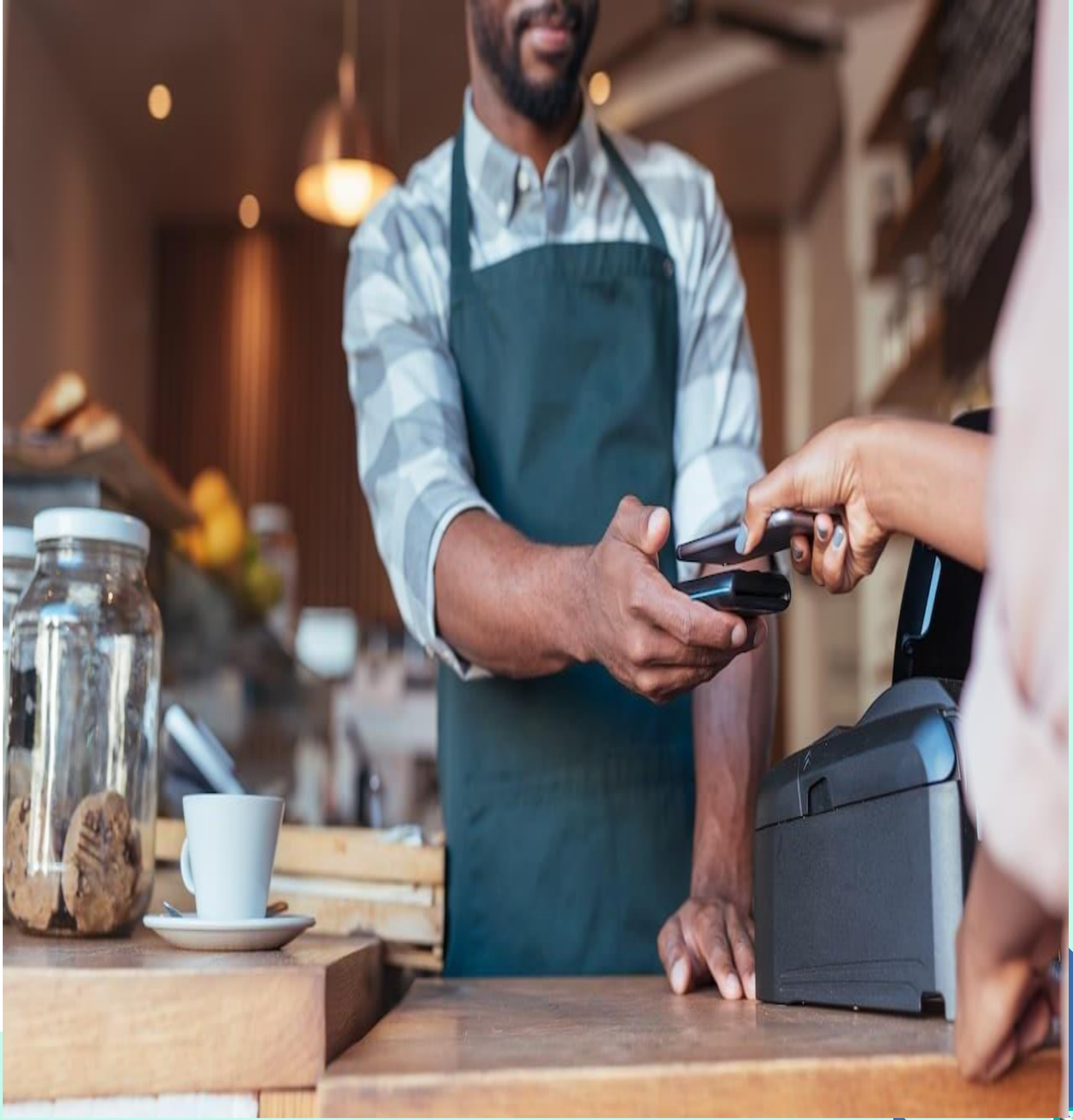
e.g World of Warcraft

e.g Amazon coin,
Nikefuel
Airlines miles
V-bucks (Fortnite)
Retailer Fidelity points

e.g: Bitcoin
Ethereum
CoinVertible
...

Fig.1. Dematerialized currencies world

Problematic: How can security be ensured in an offline payment, cash-like CBDC payment system without sacrificing privacy protection?



Blockchain and cryptocurrency conference (B2C'2023),

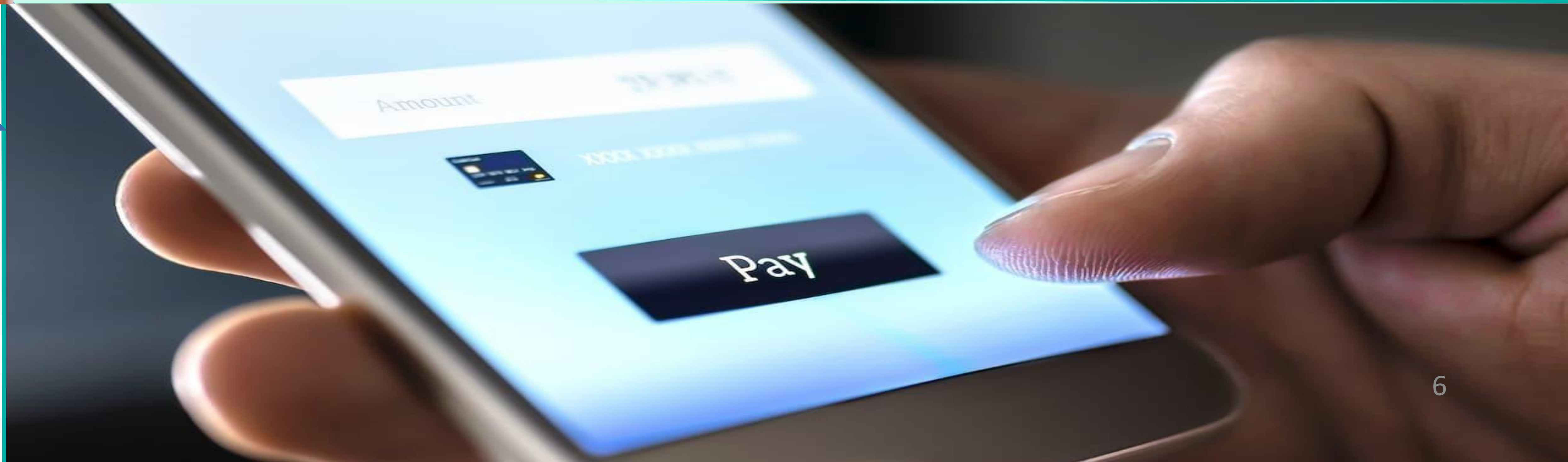
18-20 October 2023,

Corfu, Greece

OFFLINE PROTOCOL OVERVIEW AND SYSTEM OPERATION

Diving into the Mechanics: How Offline Transactions Work

02



02 OFFLINE PROTOCOL OVERVIEW

- OFFLINE FUNCTION

  No internet connection
  No ledger system connection
  No telecom connectivity

- DIGITAL COINS

  CBDC Unit corresponds to a public/private hey pair provided par Central Bank

- KEY BUILDING BLOCKS

Chaum's blind signature Protocol

ZK-SNARK (Zero-knowledge Succint Non interactive Argument of Knowledge)

TEE (Trusted Execution Environment)

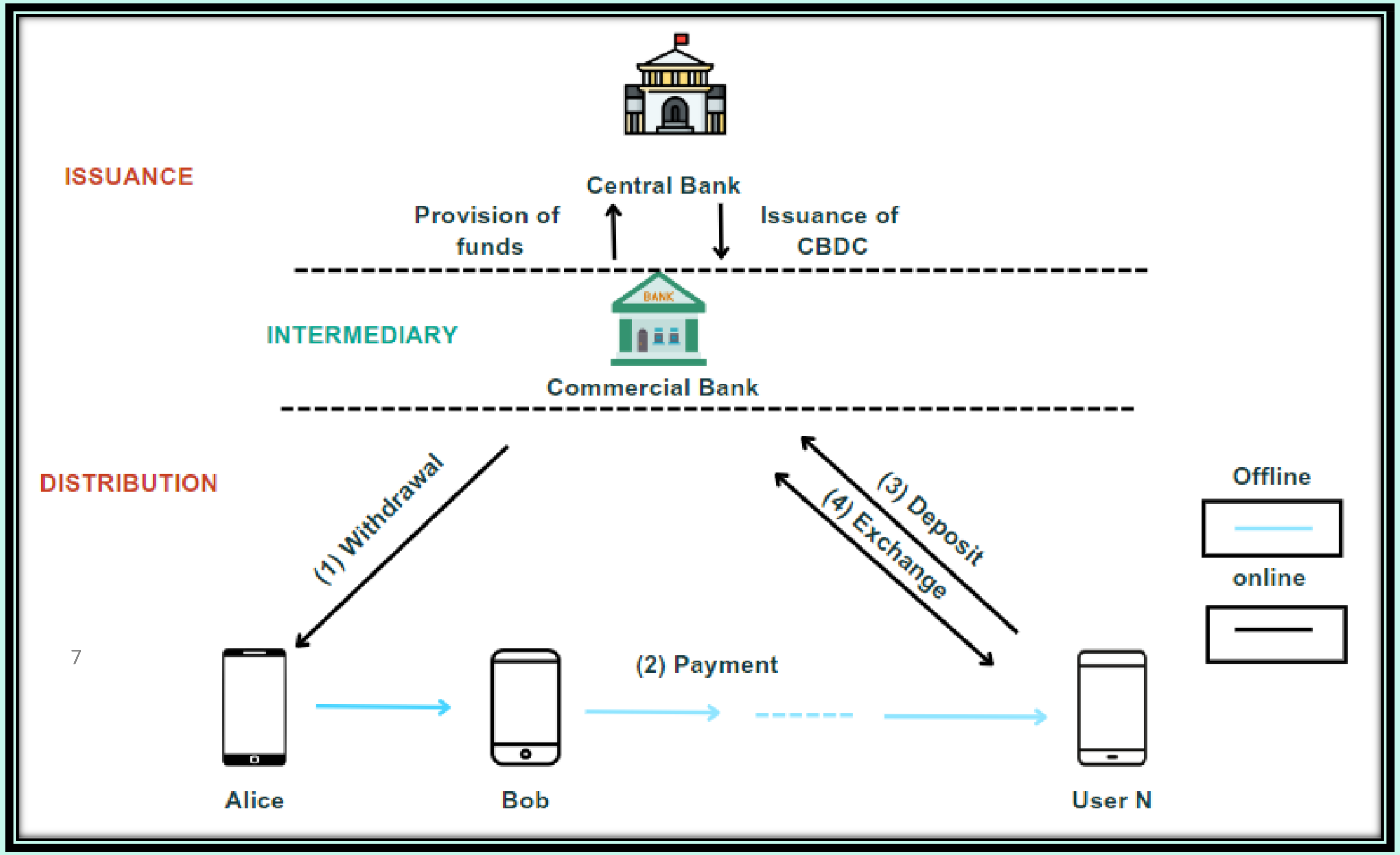


Fig.2. Our Retail CBDC ARCHITECTURE

02 SYSTEM OPERATION

➢ CORE FUNCTIONS

Withdrawal
Payment
Deposit
Exchange

➢ STAGES'PROCESS

STAGE 1: coin's withdrawing (Online)

Actors:

Alice (Emitter's transaction)

Commercial Bank

Central Bank

Purpose: Alice wants to transfer privately some coins from her online account to her personal wallet

Cryptographic method: Blind signature

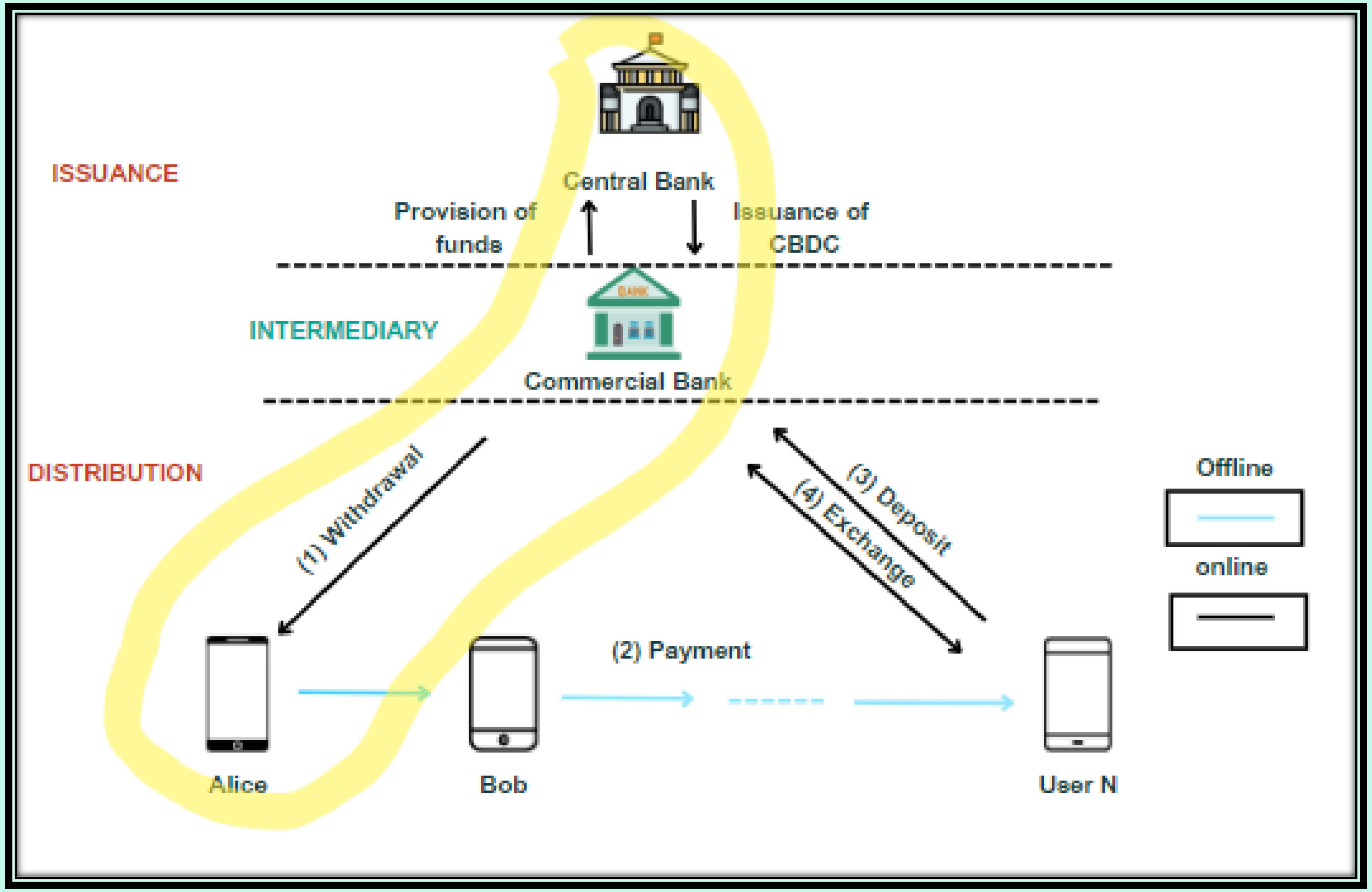
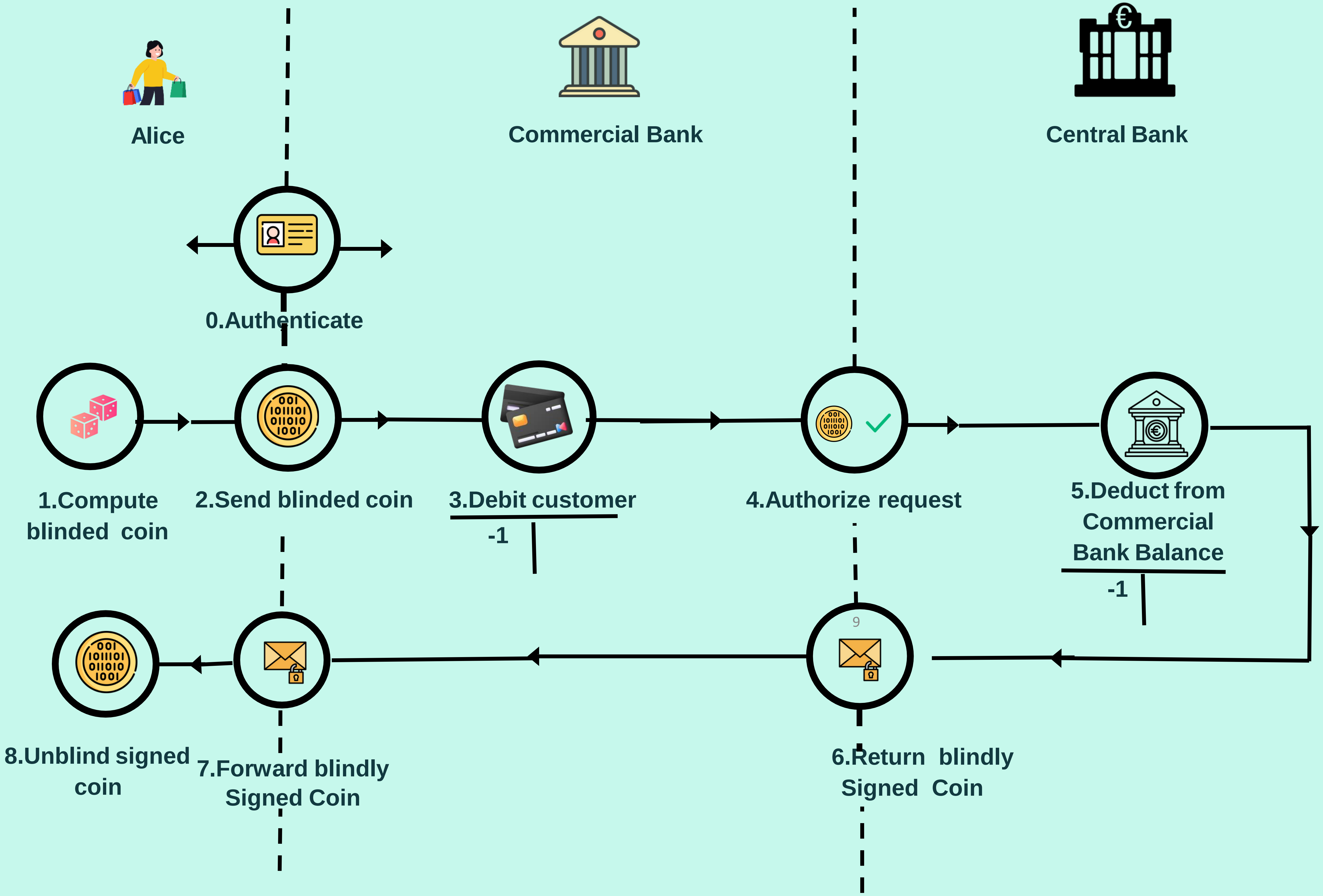


Fig.3. Withdrawal step



Alice

Commercial Bank

Central Bank

0.Authenticate

1.Compute blinded coin

2.Send blinded coin

3.Debit customer

-1

4.Authorize request

5.Deduct from Commercial Bank Balance

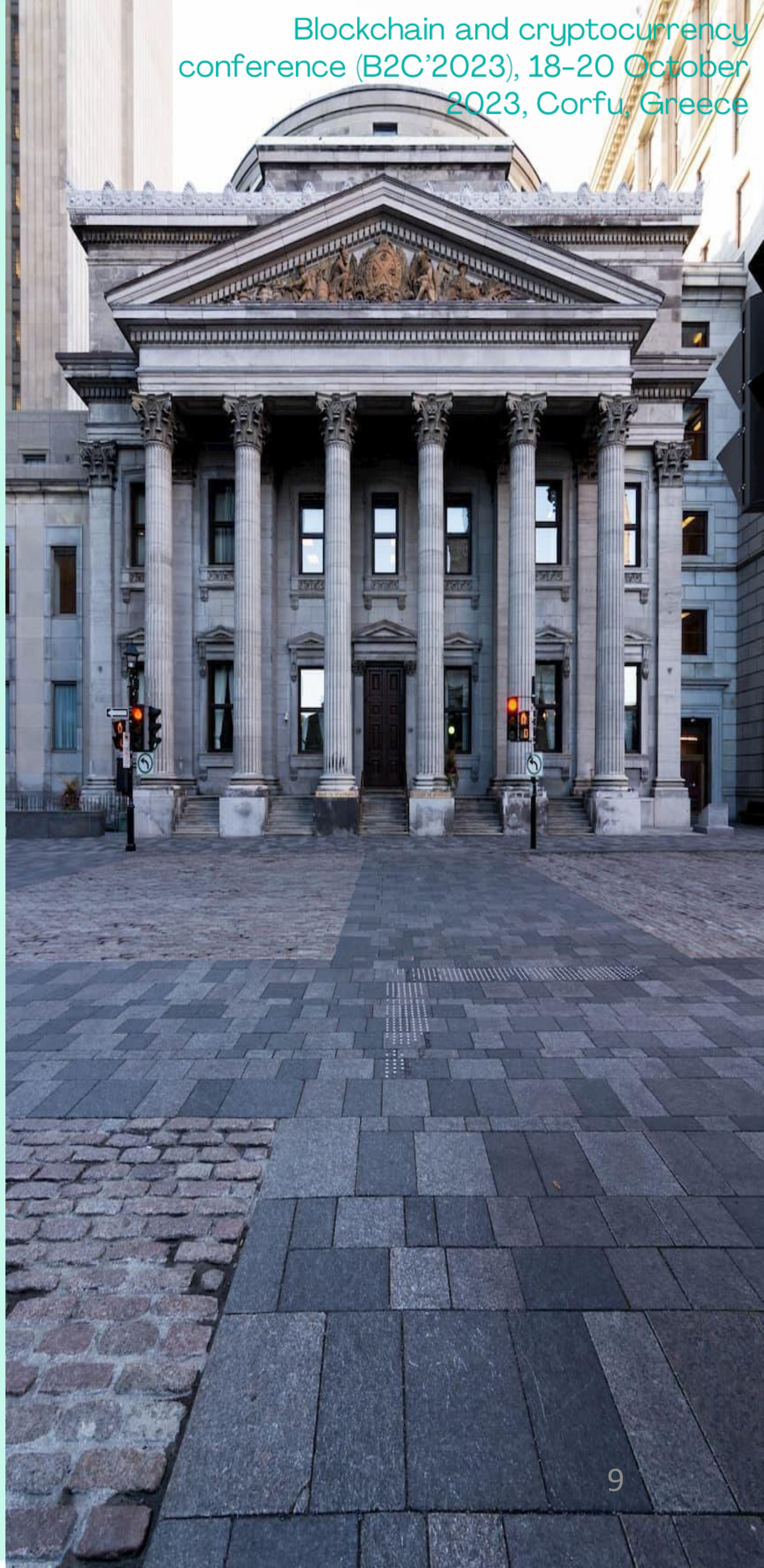
-1

6.Return blindly Signed Coin

7.Forward blindly Signed Coin

8.Unblind signed coin

Fig.4. detailed Widthdrawal step



02 SYSTEM OPERATION

➢ CORE FUNCTIONS

Widrawal
Offline Payment
Deposit
Exchange

➢ STAGES'PROCESS

STAGE 2: Offline sealed transaction

Actors:

Alice (Emitter's transaction)
Bob: (Recepient's transaction)

Purpose: Alice wants to transfer securely CBDC's coin from her offline wallet to Bob's wallet

Cryptographic methods: ZK-SNARK Protocol & digital certificate

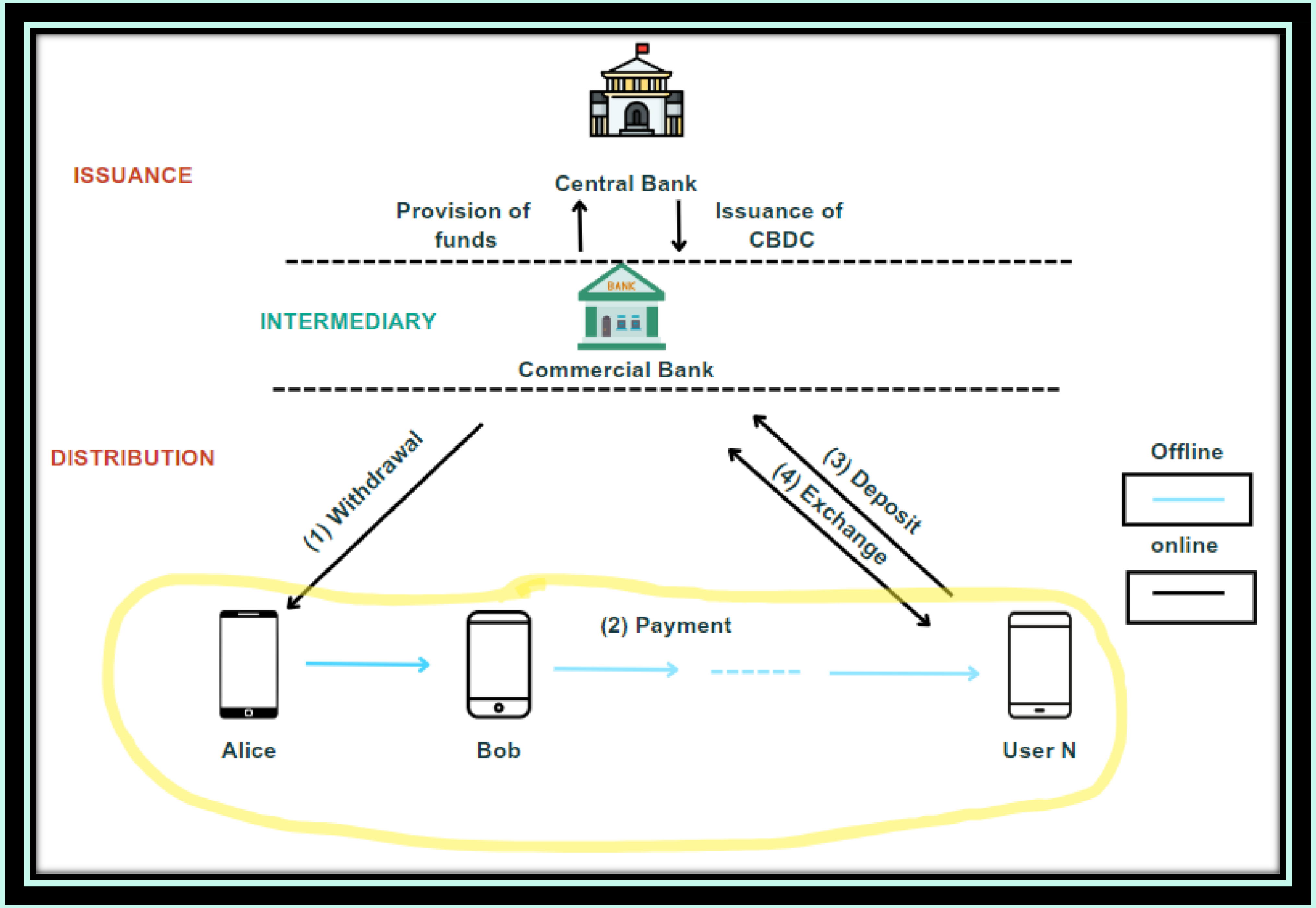
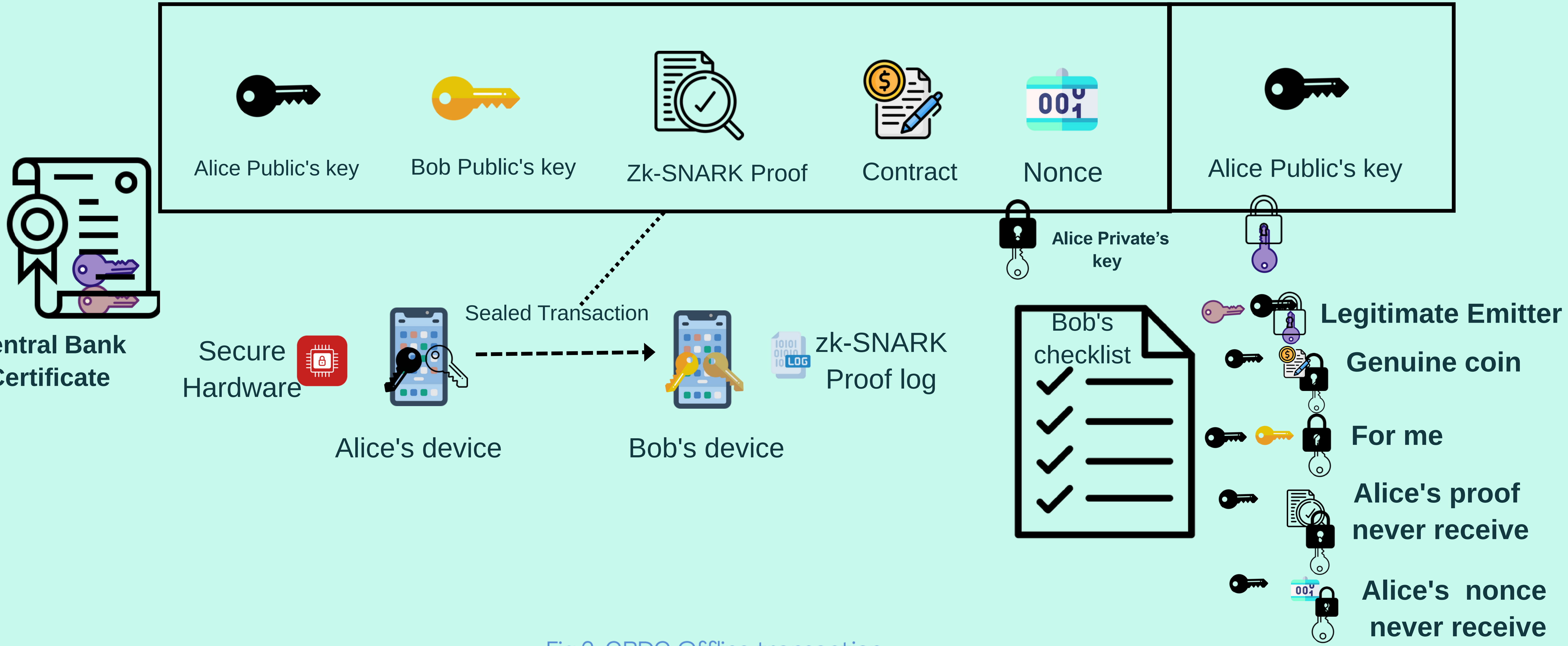


Fig.5. CBDC Offline Payment Step

02 SYSTEM OPERATION

OFFLINE



Alice Public's key

Bob Public's key

Zk-SNARK Proof

Contract

Nonce

Alice Public's key

Alice Private's key

Central Bank Certificate

Secure Hardware

Sealed Transaction

Alice's device

Bob's device

zk-SNARK Proof log

Bob's checklist

Legitimate Emitter

Genuine coin

For me

Alice's proof never receive

Alice's nonce never receive

Fig.6. CBDC Offline transaction

02 SYSTEM OPERATION

➢ CORE FUNCTIONS

Widrawal
Offline Payment
Deposit
Exchange

➢ STAGES'PROCESS

STAGE 2: Deposit (Online)

Actors:
Bob (Emitter's transaction)
Commercial bank: (Recepient's transaction)

Purpose: Bob wants to transfer privately CBDC's coin from his offline wallet to his online account Bob's.

Secure element: TEE

Cryptographic methods: ZK-SNARK Protocol & digital certificate

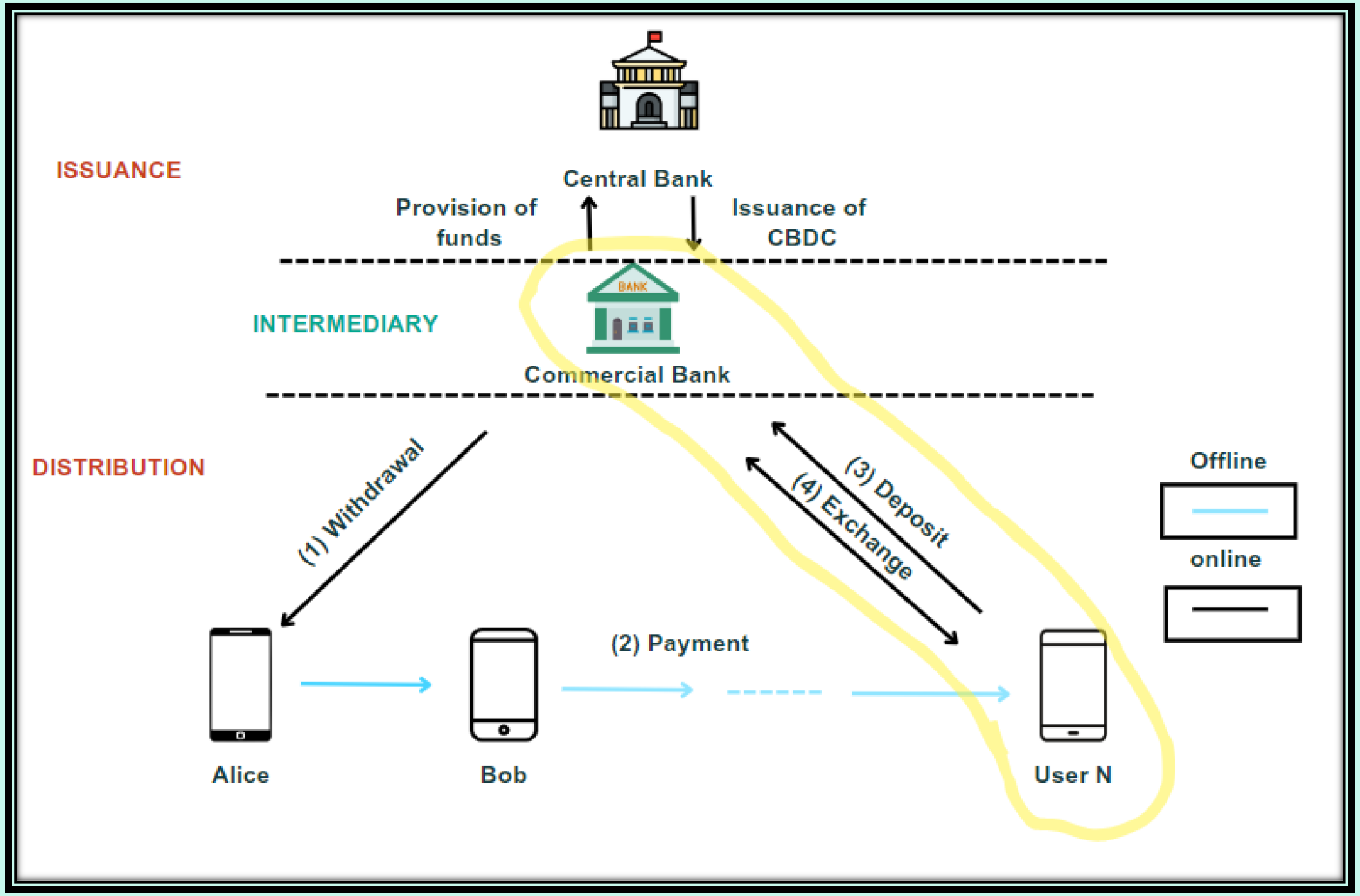
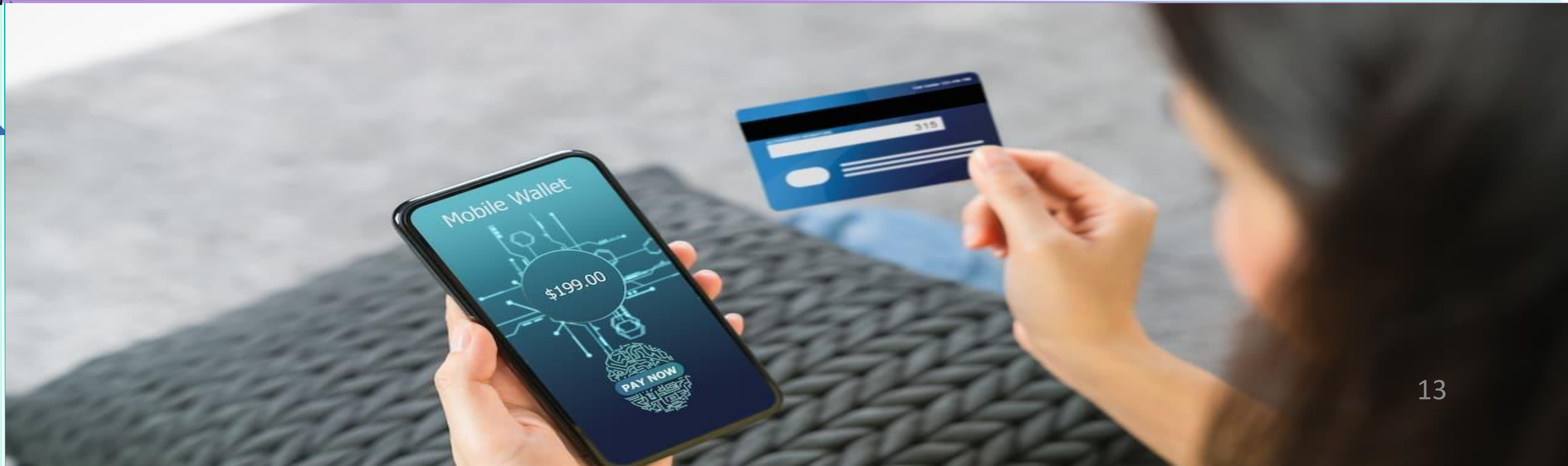


Fig.7. Deposit and Exchange step

FUTURE INTEGRATION AND EXPANSION

Paving the Way: Next Steps for our CBDC Solution

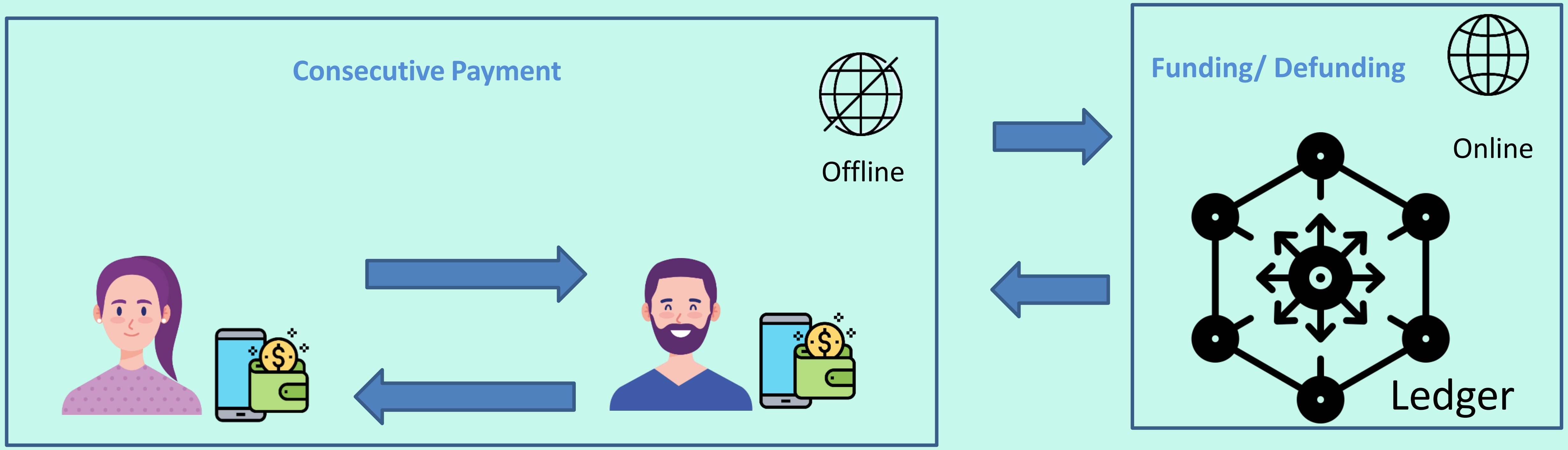
03



02 FUTURE INTEGRATION AND EXPANSION

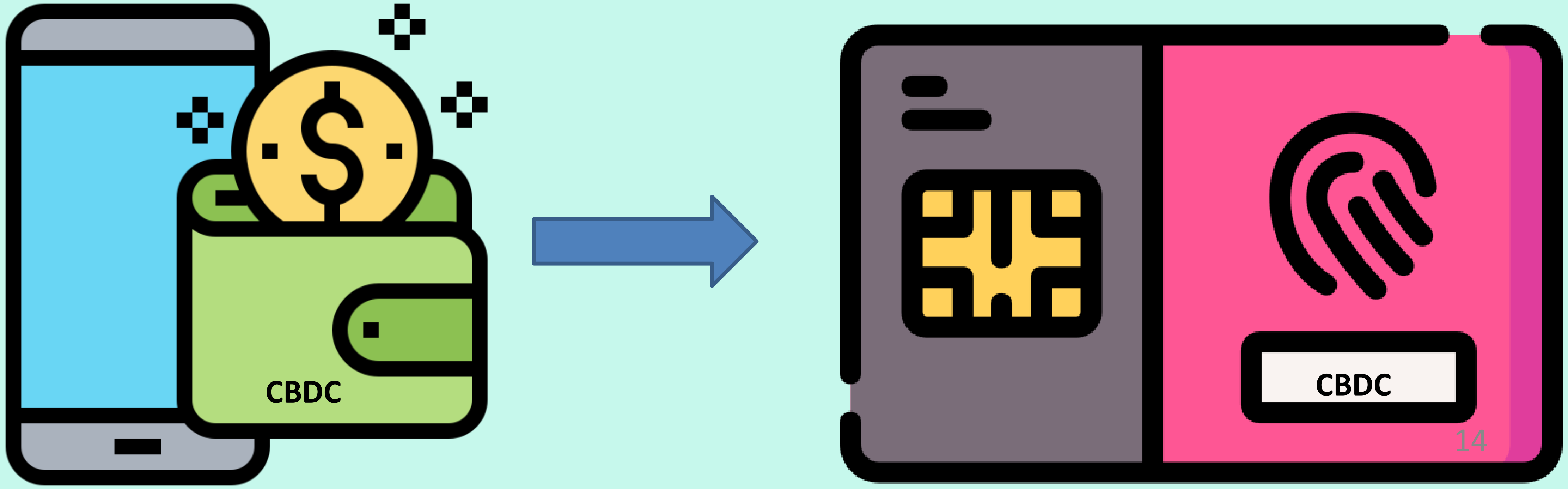
➢ BLOCKCHAIN INTEGRATION

By using a ZK-SNARK proof our solution can be seamless integrated in blockchain infrastructure



➢ EXTENDING TO SMART CARDS

Smart Card would provide users another tangible, secure, and convenient method to make offline payments.



CONCLUSIONS

Reflecting on Achievements and Envisioning the Road Ahead

04

04 CONCLUSIONS

Key benefits of our innovative solution:

1-Enhancing Privacy

-The recipient holds only payment proof (no transaction metadata)

- Quantum resistant Privacy

2-Guarantees security

- No double spending issues

-No counterfeits

3-Ensuring Compliance

- Know Your Customer (KYC)

-Commercial Banks monitore fund movements to prevent financial instability

Adressing Framework Limitations:

Switching from zk-SNARK to zk-STARK for enhanced security.

zk-STARK Advantages:

No initial setup phase

Quantum-resistant

Faster proof generation

Considerations:

Newer technology; requires thorough evaluation

Larger proof size compared to zk-SNARKs

CREDITS

Greyc Lab/Ensicaen Engineering School:

Thanks to their team for their feedback and commitment to this study

GREYC
Electronics and Computer Science Laboratory

Fime:

Grateful for their invaluable insights and support throughout this research.

fime

Images: Flaticon.com

GREYC Digital Sciences Research Unit
ADVANCING NETWORK SECURITY, CRYPTOGRAPHY, INFORMATION PROTECTION, AND SOFTWARE SECURITY

Secure and Efficient CBDC Adoption with FIME
HELPING DIFFERENT SEGMENTS EMBRACE DIGITAL CURRENCIES

Thank you