Privacy and CBDC

Designing a CBDC with Support for Cash-Like Privacy

University of Bayreuth

Matthias Babel
Dr. Jonas Gross
Benjamin Schellinger
Johannes Sedlmeir

University of St. Gallen

Dr. Alexander Bechtel

October 2022

Projektgruppe
Wirtschaftsinformatik

Kernkompetenzzentrum
Finanz- & Informationsmanagement

Introduction of the Speaker

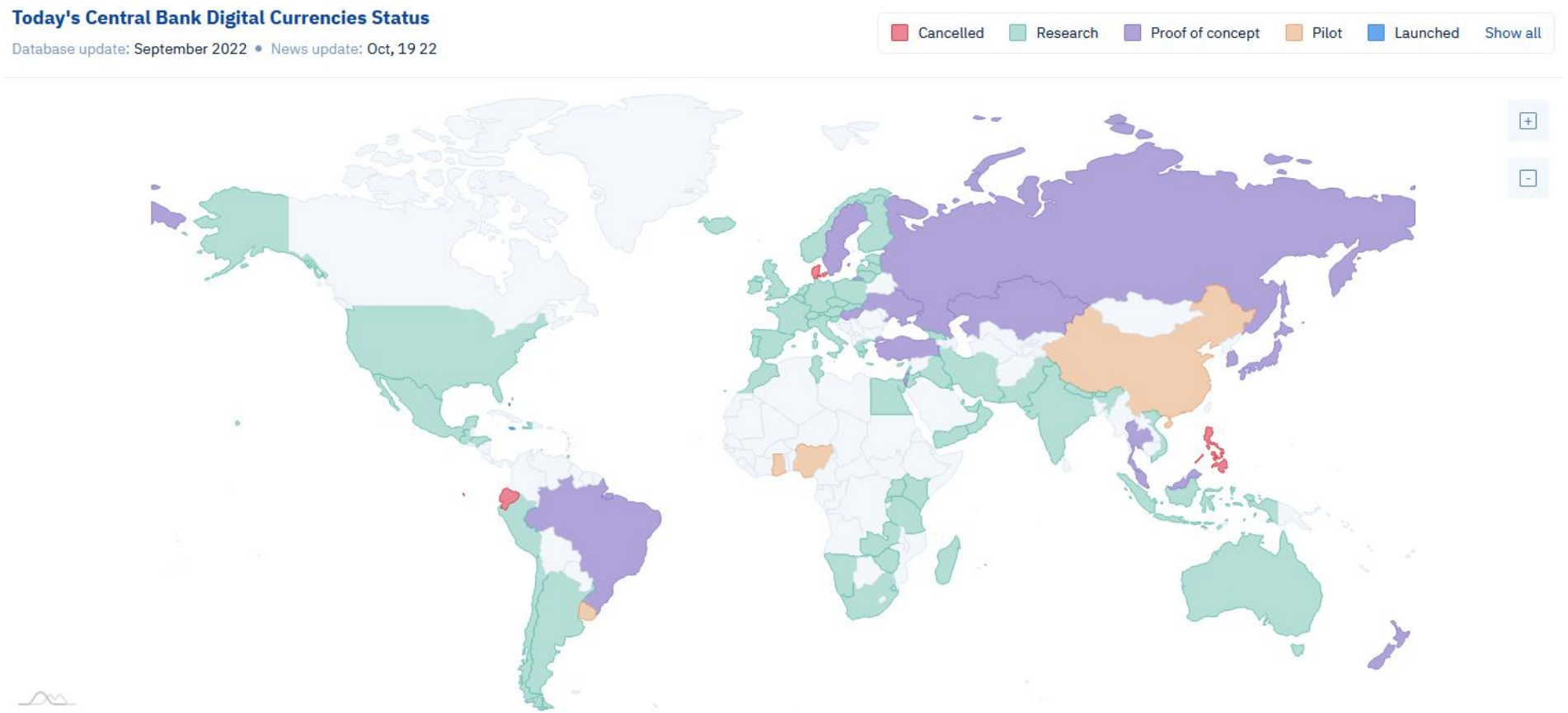
Dr. Jonas Gross

- PhD in Economics (on digital currencies and monetary policy) at University of Bayreuth, Germany
- Chairman at the Digital Euro Association
- Head of Digital Assets and Currencies at etonec

Outline

1) **Motivation for privacy and CBDC**
2) Our Proposal in a Nutshell
3) Our Proposal in Depth
4) Discussion

The Status Quo of CBDCs Worldwide



Source: CBDC Tracker (2022).

Why Cash-like Privacy for Payments Matters

Privacy is secured by civil rights, such as freedom of expression and freedom of association

Cash-like privacy prevents government scrutiny and surveillance abuses

Cash-like privacy prevents authorities to restrict specific transactions by individuals

Cash-like privacy protects users from data exploitation

As financial transaction data is particular confidential, privacy plays an essential role for payments (and also for CBDC, especially in a world where the use of cash declines)

Privacy and Regulatory Compliance of Payments

- There are different **degrees of data privacy** of transaction data: Transaction data can be stored transparently (e.g., bank transfers), pseudonymously (e.g., Bitcoin), or anonymously (e.g., Zcash), or not at all (physical cash).

- The degree of data privacy has strong implications for **anti-money laundering (AML), and counter-terrorist financing (CFT) regulation** as anonymous transactions cannot be assigned to a specific person, thereby enabling using money for illicit activities.

To restrict the large-scale financing of illicit activities, regulators enforce **per-transaction, turnover, and/or balance limits for anonymous payments**.

Per-transaction limits for **fully private cash payments** (e.g., Greece (500 EUR), France and Portugal (1,000 EUR), Italy (2,000 EUR), Spain (2,500 EUR), Belgium (3,000 EUR), and Slovakia (15,000 EUR)

For **anonymous e-money transactions**, the *5th AML Directive* defines a monthly **turnover** and **balance limit** of 150 EUR.

Our Solution

Our CBDC framework supports cash-like privacy in a regulatory compliant way. It allows cash-like private transactions up to a pre-defined limits and thereby complies with AML and CFT regulation.

Summary of our CBDC proposal

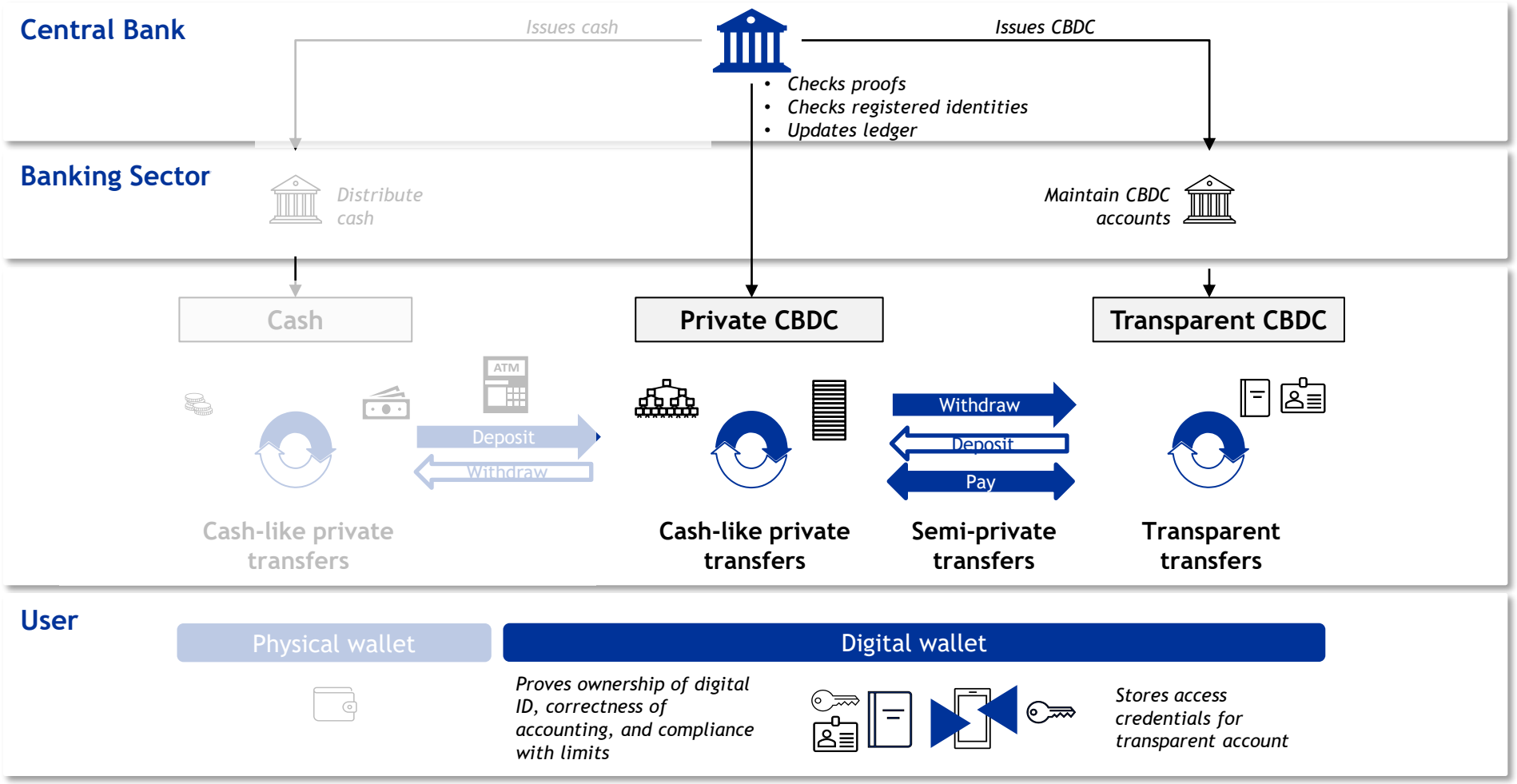
Goal 	Ensure **cash-like data privacy** for CBDC **up to specific limits** so that banks, central banks, and regulatory authorities cannot access transaction details.
Approach 	Cash-like privacy ensured by **cryptography** without trusting third parties (=trustless privacy)
User-centric compliance 	Absent third parties that can conduct compliance checks, users must provide **compliance checks on their own:** ▪ Prove specific requirements for payments are met. ▪ Compliance checks need to be provided by design/default. ▪ Zero-Knowledge Proofs (ZKPs) to prove integrity without revealing confidential information.

CBDC system that provides cash-like privacy and compliance by design

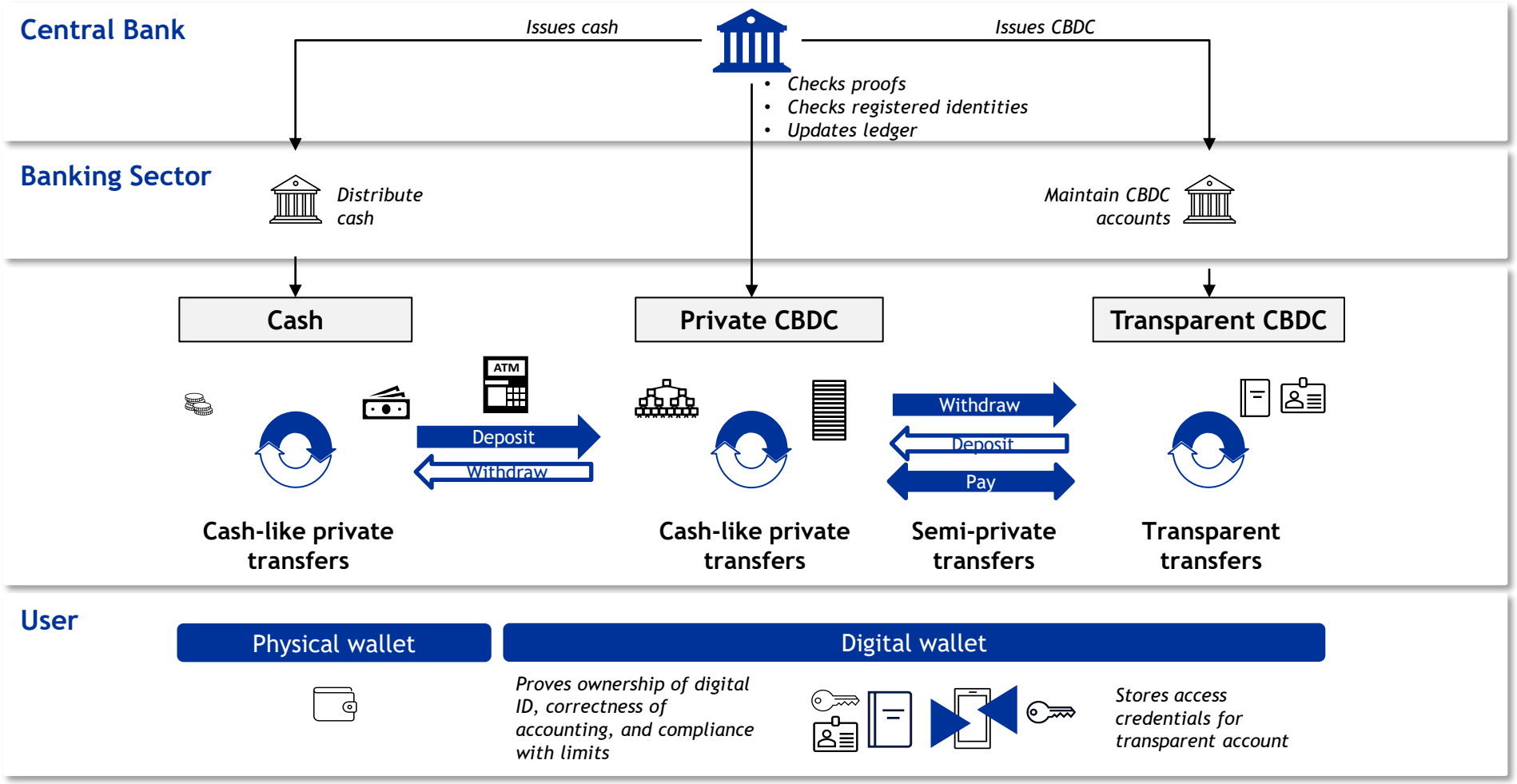
Outline

1) Motivation for privacy and CBDC
2) **Our Proposal in a Nutshell**
3) Our Proposal in Depth
4) Discussion

Our CBDC Proposal in a Nutshell



Our CBDC Proposal in a Nutshell

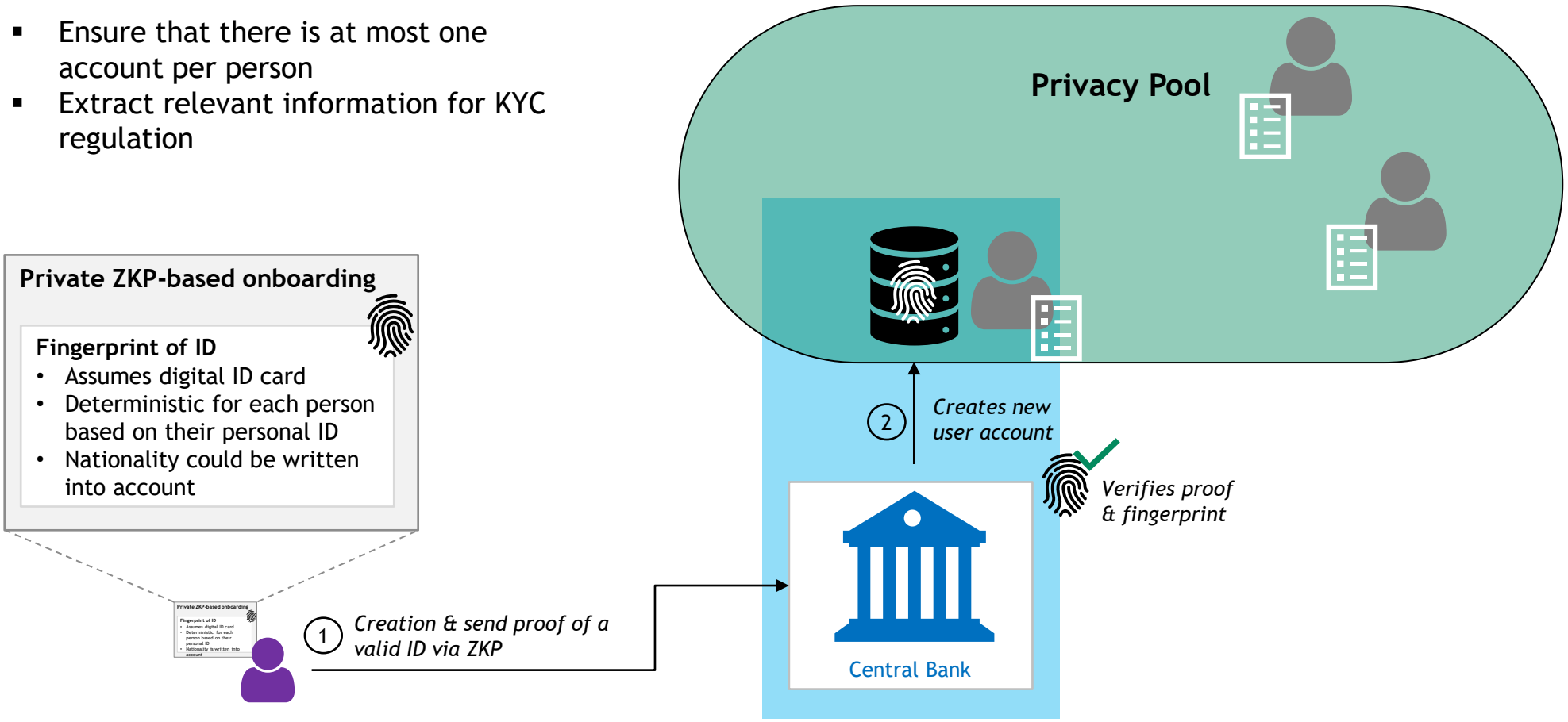


Outline

1) Motivation for privacy and CBDC
2) Our Proposal in a Nutshell
3) **Our Proposal in Depth**
4) Discussion

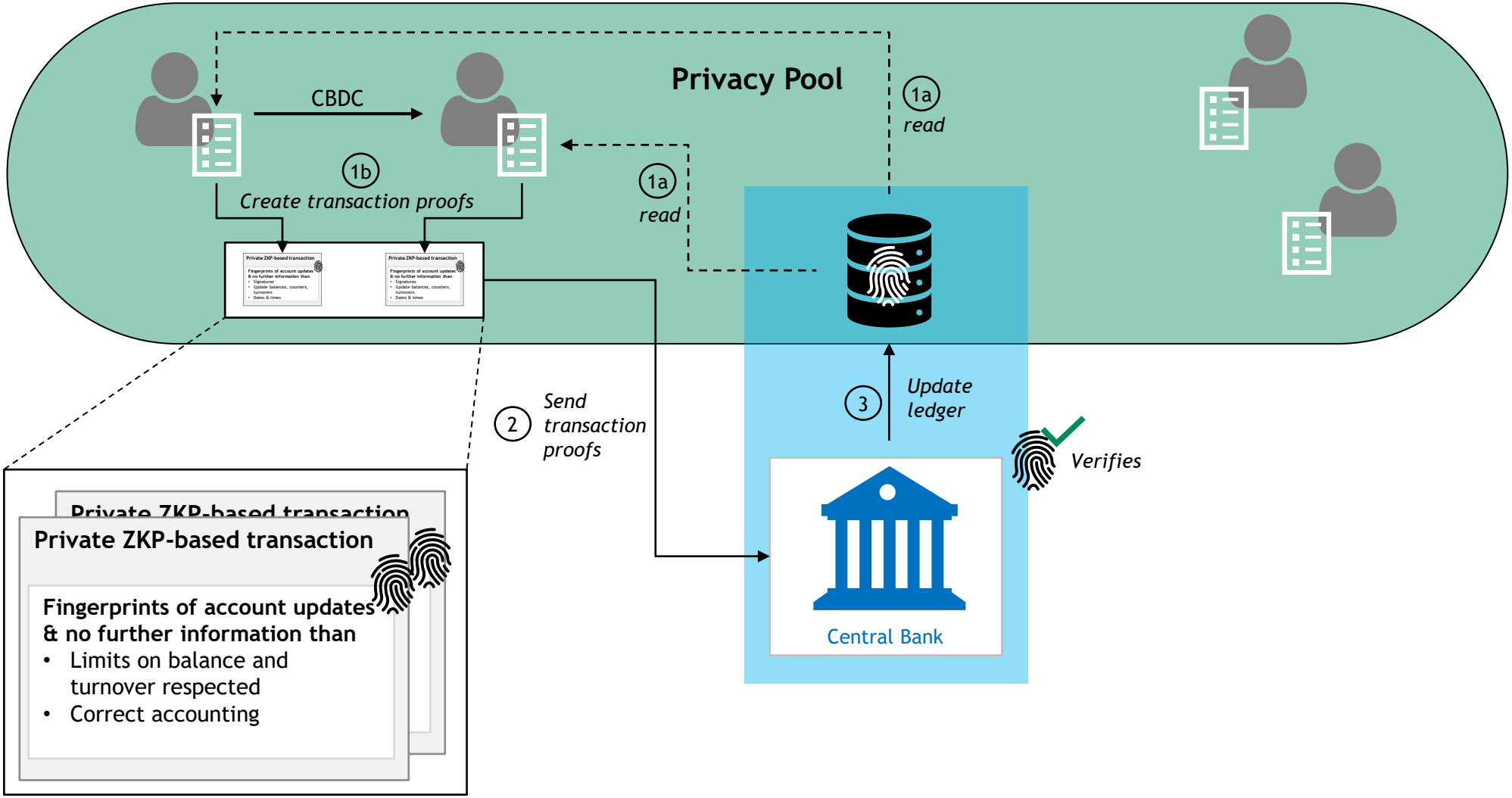
Onboarding to the Privacy Pool

- Ensure that there is at most one account per person
- Extract relevant information for KYC regulation

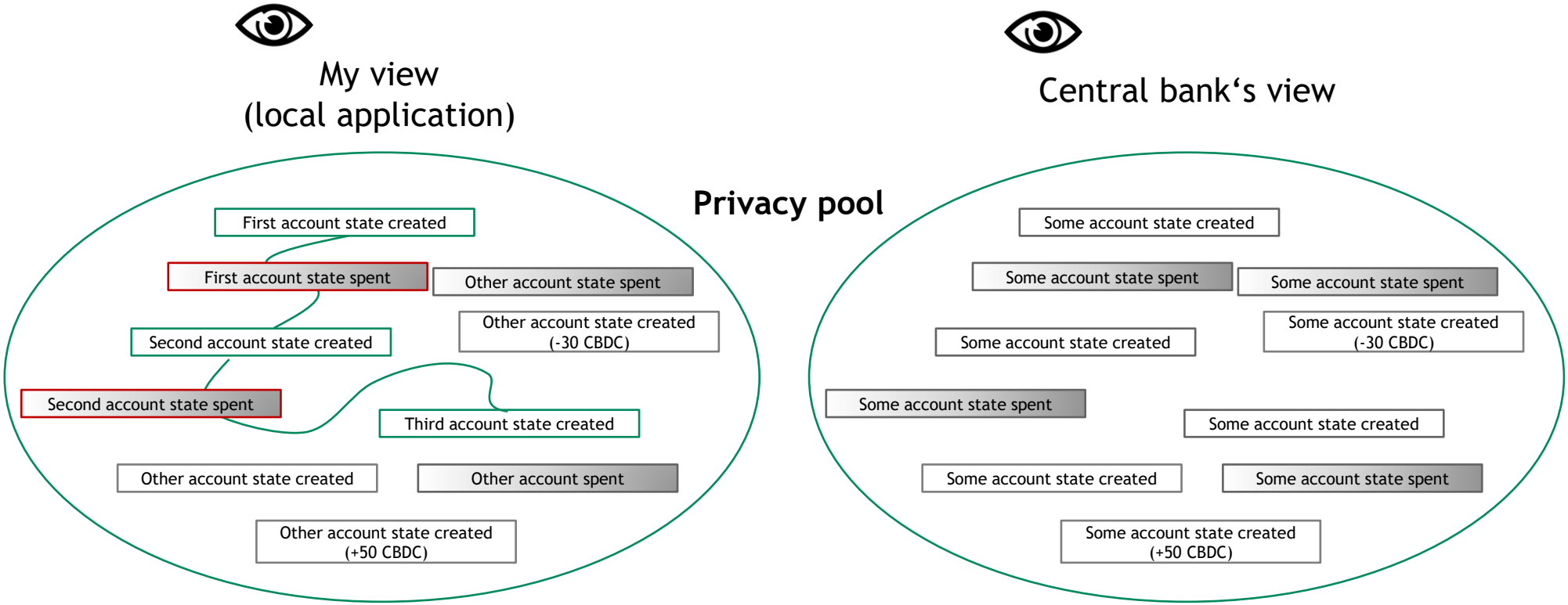


Zero-Knowledge Proof (ZKP)
- Cryptographic protocols in which an account holder can convince the central bank that a computation was performed correctly.
- Account holder knows an input to a function that results in a specific output without revealing the input itself.

Architecture of Fully Private Transactions



High Level Perspective



Thanks for your time!

Outline

1) Motivation for privacy and CBDC
2) Our Proposal in a Nutshell
3) Our Prototype in Depth
4) **Discussion**