Privacy-Enabling CBDC

Presentation to ITU DC3 Conference

Geoff Goodell (University College London)

26 January 2023

g.goodell@ucl.ac.uk

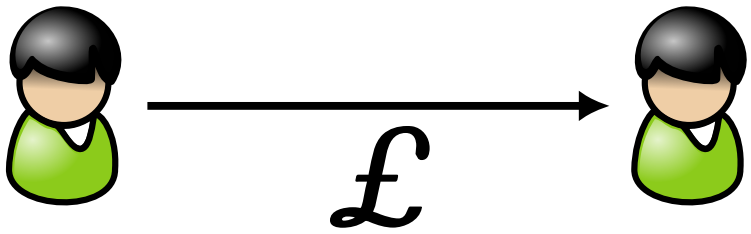
Cash

Image Source: New York Habitat

- issued by a central bank or monetary authority
- mostly held by individuals and businesses as a store of value
- also held by banks to service withdrawals
- has a finite lifespan
- affords users strong privacy and anonymity
- fungible (mutually substitutable and undifferentiated in practice)

Modern retail payments

Cash



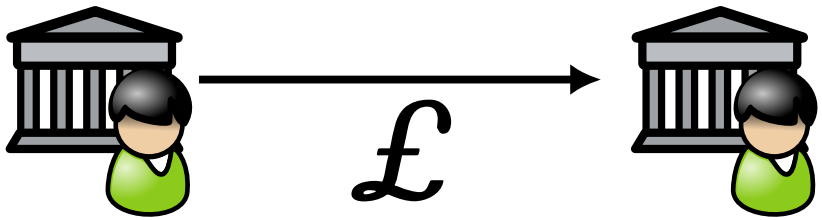
Direct & private interaction between transacting parties.

Currency is possessed and controlled **by owners**.

Fungible tokens provide **assurance** that transactions will succeed.

Everyone's money is **worth the same** as everyone else's.

Retail Banking (cards, EFT, etc)



Interaction is actually between **regulated institutions**.

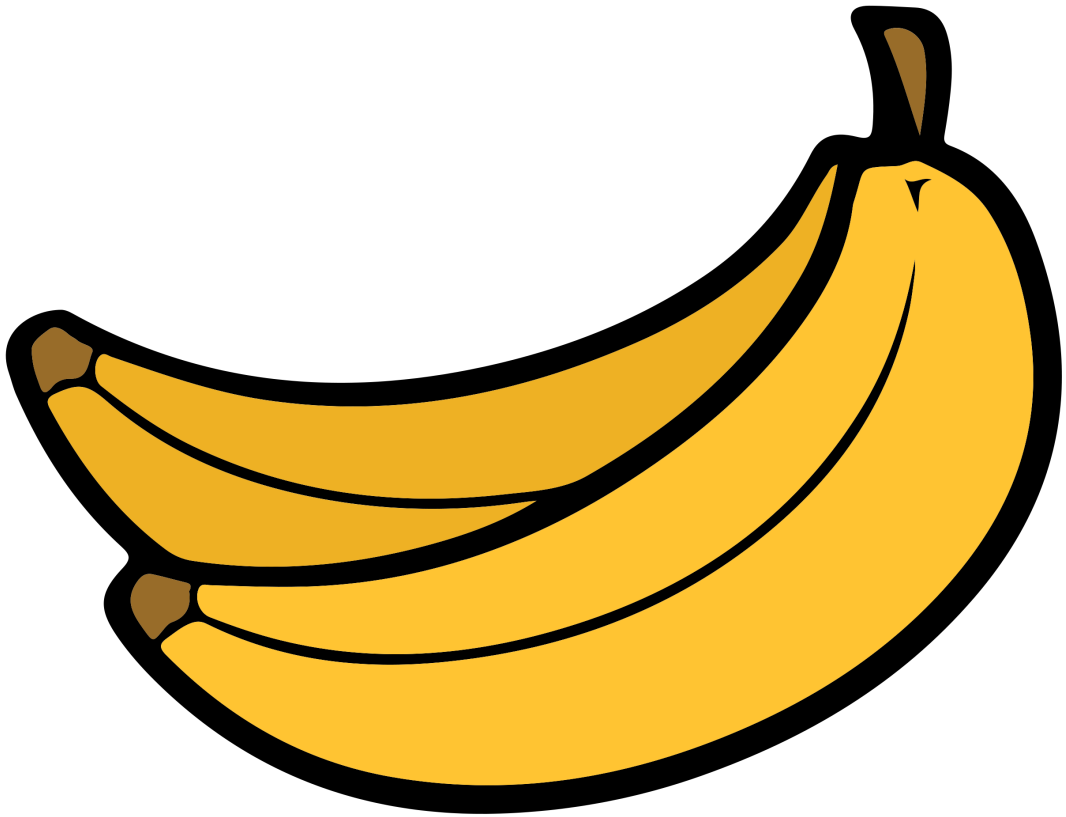
Currency is possessed and controlled **by institutions**.

Transactions may be **intermediated** or **blocked**.

Users might be subject to **discrimination** and **profiling**.

Modern retail payments and private property

Do we intend to **deny** ordinary citizens the **right** to engage with the economy using assets that they **possess** and **control**?



That's bananas!

Digital currency can deliver privacy and control for users

Of course, it depends on the design. A good CBDC design:

(1) Provides a **centrally-issued electronic token**:

- Value can be held outside accounts or relationships.
- Value can be exchanged without account reconciliation.

(2) Allows clearing and settlement by **independent, private actors**.

- Preserves the existing two-tiered payment system.
- **Decentralisation** prevents tampering or unwanted changes to the rules.

(3) Protects consumers from profiling through **privacy by design**.

- withdrawals and deposits are analogous to cash.
- **Payers are anonymous** but recipients may be subject to regulation.

The system must have bearer instruments (tokens)

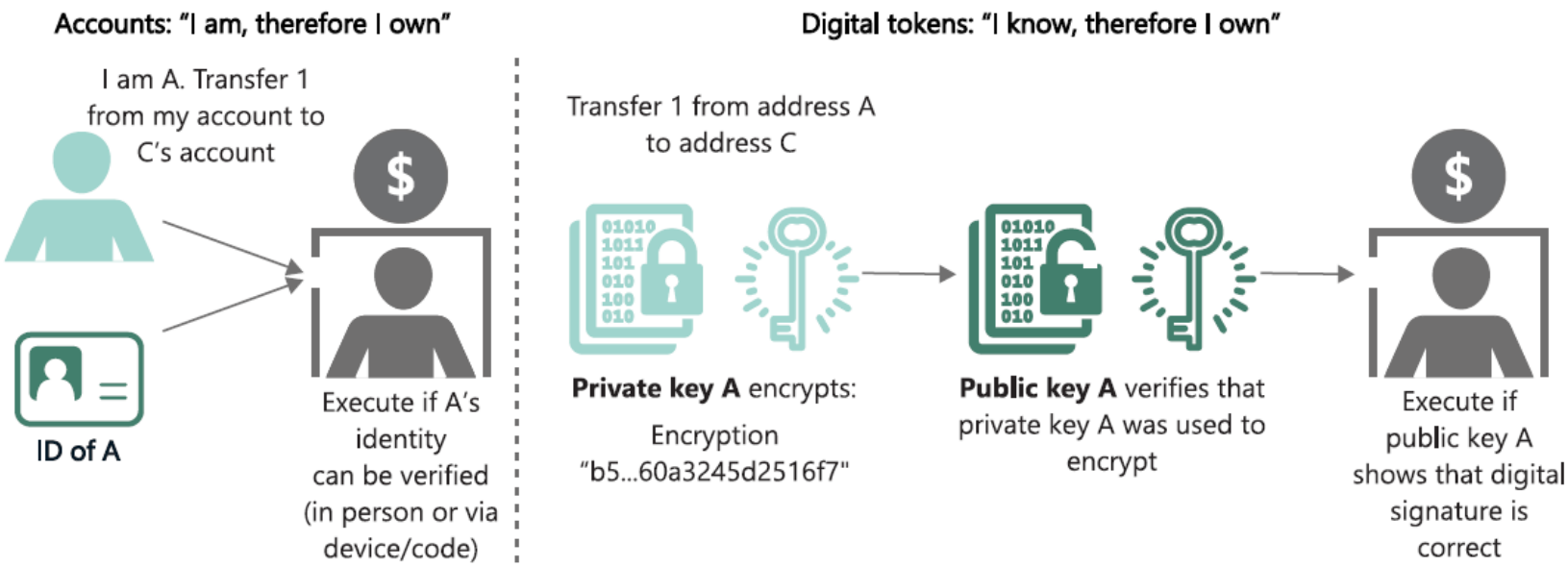


Image Source: Auer & Böhme

It **MUST** be possible to store tokens in **non-custodial wallets**.

Non-custodial wallets **MUST NOT** be **identifiable**.

- Such wallets **MUST NOT** be **issued**.
- Such wallets **MUST NOT** require **registration**.
- Such wallets **MUST NOT** require **trusted computing**.

The system must be private by design for consumers

Risk of **profiling** is **NOT** about knowing who the users of money are.

- OK to require **AML/KYC** for **recipients** of CBDC (for example, accountholders who withdraw tokens or merchants who accept them).
- OK to disallow **peer-to-peer** transactions.

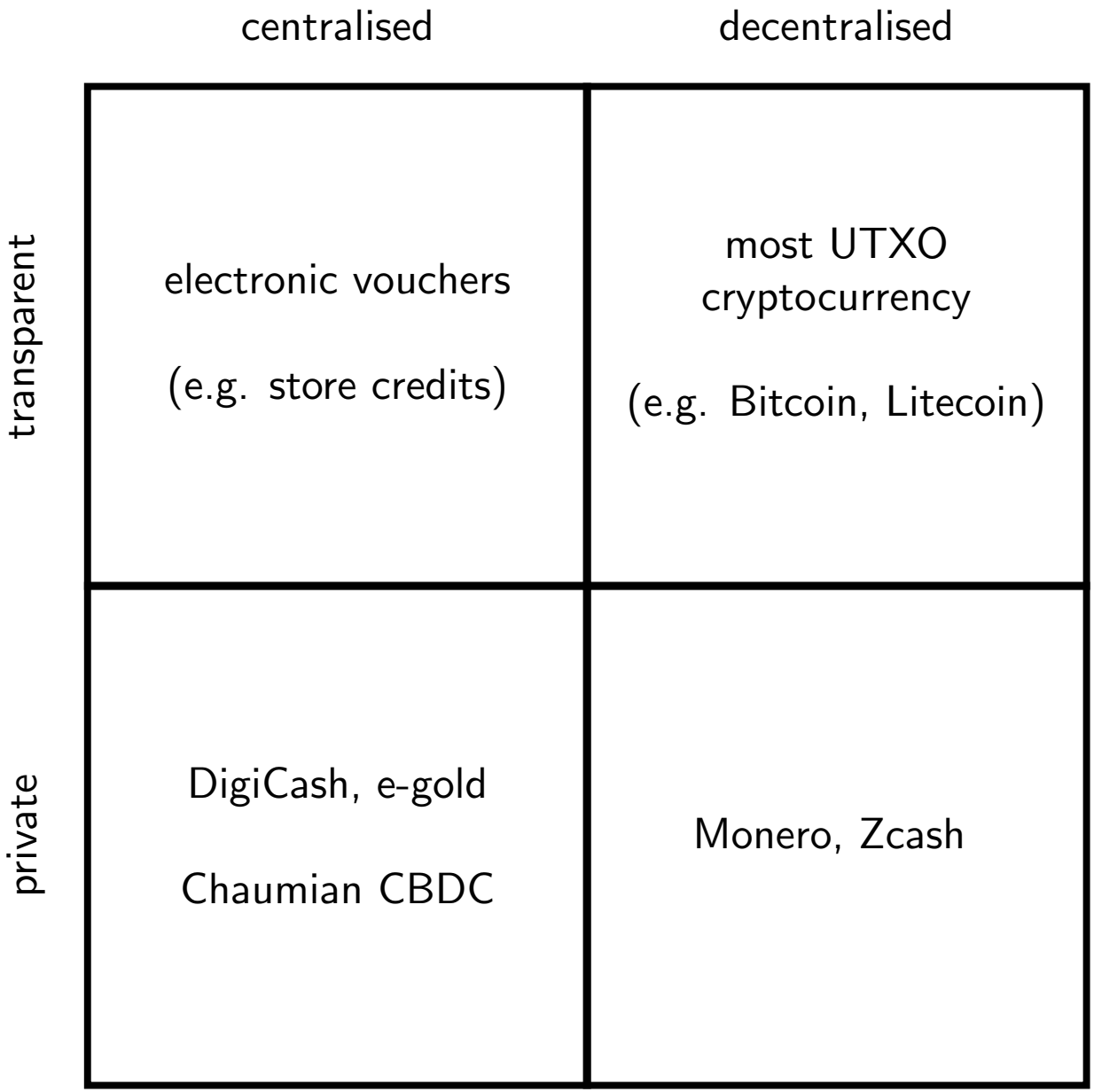
Risk of **profiling** is about knowing how consumers **spend** their money.

- The identity of the sender **MUST NOT** be linked to:
  - the **recipient**
  - the **size**
  - **metadata** such as time, location, service providers, and so on.
- Payments by the same sender **MUST NOT** be linked to **each other**.

Privacy-enhancing technologies (**PETs**) can mitigate these risks.

- **Blind signatures** (viz. Chaum) are sufficient. (ZKP can also work.)

The space of possible system designs



How distributed ledgers support payments

(1) Recording transactions between **accounts**.

- to provide evidence that value has been transferred between externally managed accounts.
- to execute transfers of value between **externally** managed accounts.
- to execute transfers of value between **internally** managed accounts (e.g. Ethereum state updates).

(2) Managing tokens in payment systems with **endogenous** token tracking (e.g. for UTXO systems such as Bitcoin and Monero).

(3) Memorialising commitments in payment systems with **oblivious** token tracking, wherein the assets maintain their own state (USO assets).

A new digital currency architecture: our approach

Three components:

- **Blind signatures**, for privacy by design, with verifiable anonymity
  - Similar to Chaum, Grothoff, Möser
- **Distributed ledgers**, for immutability and institutional trust
  - Nodes are operated by **independent** service providers
  - Assets are stored in **non-custodial wallets**
- **Unforgeable, stateful, oblivious (USO) assets**, for scalability
  - Issuer does not maintain a database of assets (contrast with UTXO approaches)
  - Issuer has no role in the **"hot loop"** of transactions