Scalable Digital Currency for Central Banks

Monero Konferenco 2022, Lisbon

Geoff Goodell (University College London)

18 June 2022

Cash

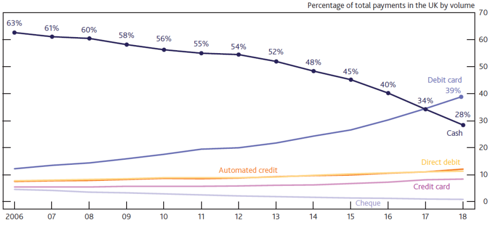
Image Source: New York Habitat

- 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)

Cash usage is in decline

- Cash infrastructure has high fixed costs.
- Digital payments are cheap and popular.
- The coronavirus has bolstered internet and contactless payments.

- May undermine **monetary sovereignty**.
- Transforms custodians into **gatekeepers**.



Source: UK Finance 2019.

Source: UK Finance 2019

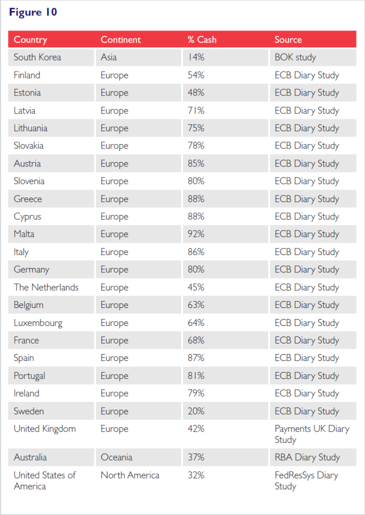
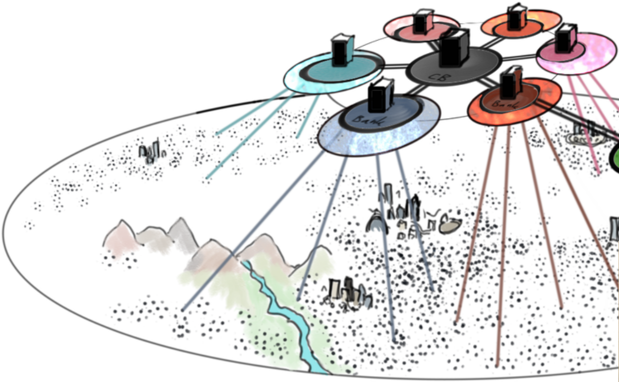


Figure 10

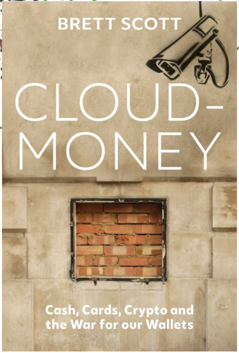
Country	Continent	% Cash	Source
South Korea	Asia	14%	BOK study
Finland	Europe	54%	ECB Diary Study
Estonia	Europe	48%	ECB Diary Study
Latvia	Europe	71%	ECB Diary Study
Lithuania	Europe	75%	ECB Diary Study
Slovakia	Europe	78%	ECB Diary Study
Austria	Europe	85%	ECB Diary Study
Slovenia	Europe	80%	ECB Diary Study
Greece	Europe	88%	ECB Diary Study
Cyprus	Europe	88%	ECB Diary Study
Malta	Europe	92%	ECB Diary Study
Italy	Europe	86%	ECB Diary Study
Germany	Europe	80%	ECB Diary Study
The Netherlands	Europe	45%	ECB Diary Study
Belgium	Europe	63%	ECB Diary Study
Luxembourg	Europe	64%	ECB Diary Study
France	Europe	68%	ECB Diary Study
Spain	Europe	87%	ECB Diary Study
Portugal	Europe	81%	ECB Diary Study
Ireland	Europe	79%	ECB Diary Study
Sweden	Europe	20%	ECB Diary Study
United Kingdom	Europe	42%	Payments UK Diary Study
Australia	Oceania	37%	RBA Diary Study
United States of America	North America	32%	FedResSys Diary Study

Source: World Cash Report 2018

Payments are a modern panopticon



"If you wanted to build an unobtrusive system for surveillance, you couldn't do much better than an EFTS [electronic funds transfer system]"
— Paul Armer, Rand Corporation, 1975


BRETT SCOTT

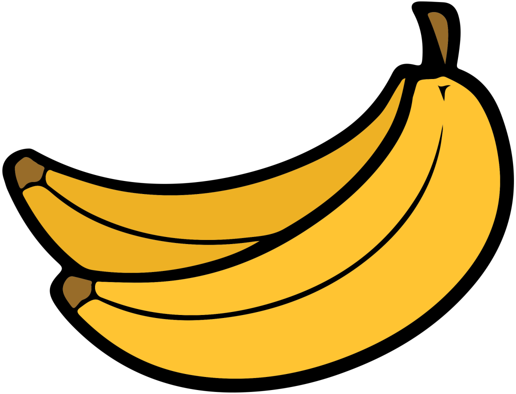
CLOUD-MONEY

Cash, Cards, Crypto and the War for our Wallets

Image Credits: Brett Scott

Modern retail payments and private property

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



That's bananas!

Central bank digital currency (CBDC) can deliver privacy

Of course, it depends on the design. Our proposal:

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

- can hold value outside accounts.
- can exchange value 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** and recipients are not.

The system must have bearer instruments (tokens)

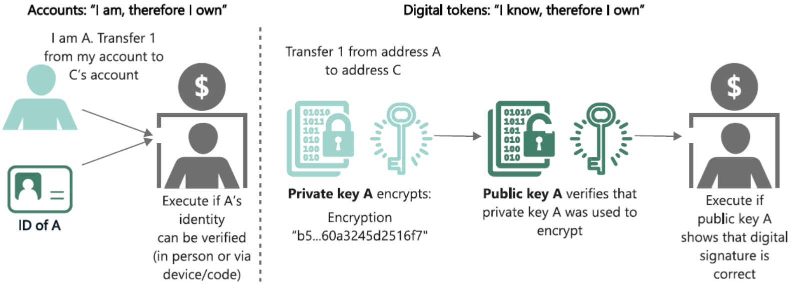

Accounts: "I am, therefore I own"
I am A. Transfer 1 from my account to C's account
ID of A
Execute if A's identity can be verified (in person or via device/code)
Digital tokens: "I know, therefore I own"
Transfer 1 from address A to address C
01010 1011 101 010 100 010
Private key A encrypts:
Encryption "b5...60a3245d2516f7"
Public key A verifies that private key A was used to encrypt
Execute if public key A shows that digital signature is correct

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.

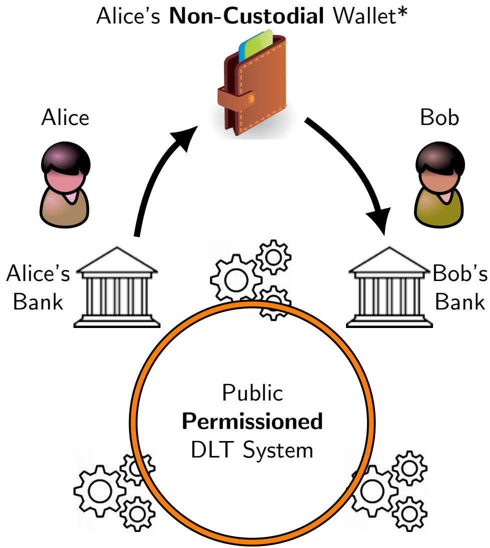
- **Blind signatures** (viz. Chaum) are sufficient. (ZKP can also work.)

A novel digital currency architecture: Approach

Our system combines:

- **Blind signatures**, for privacy by design, with verifiable anonymity
  - Similar to Chaum, Grothoff, Möser
- **Distributed ledgers**, for decentralised transaction processing
  - Nodes are operated by **independent** payment service providers
  - Assets are stored in **non-custodial wallets**
- **Unforgeable, stateful, oblivious** (**USO**) **assets**, to avoid requiring issuers or service providers to maintain asset state
  - Issuer does not maintain a database of assets (contrast with UTXO approaches)
  - Issuer has no role in the **“hot loop”** of transactions

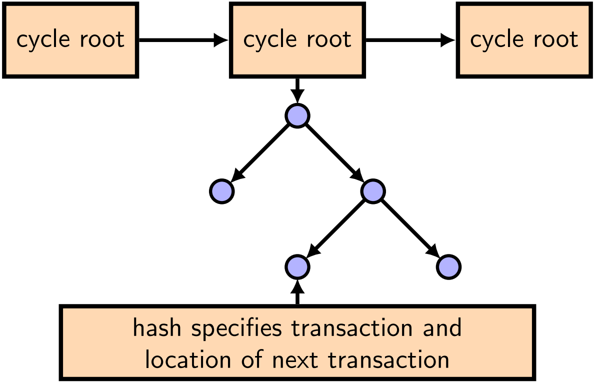
Overview: Non-custodial wallets and DLT



Alice's **Non-Custodial** Wallet*
Alice
Bob
Alice's Bank
Bob's Bank
Public **Permissioned** DLT System

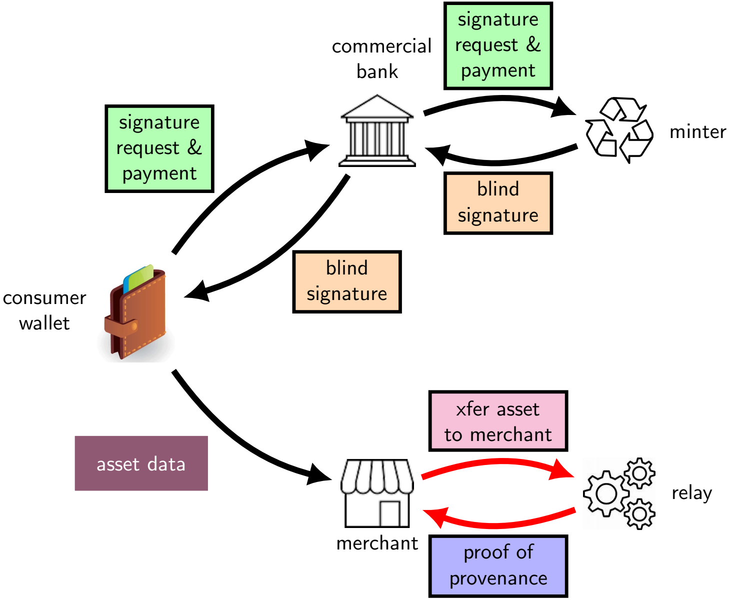
The value of DLT lies in externalising commitments

Separate consensus and token issuance:
We don't need **"gas"**!



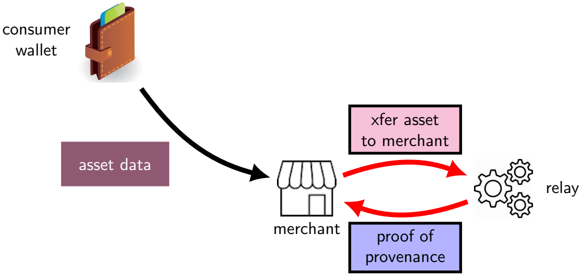
- The history of an asset can be verified via **proofs of provenance**.
- The Merkle trie structure ensures **integrity** and **uniqueness**.

The consumer journey



Spending CBDC

Alice can give Bob control & possession at the same time:



consumer wallet

asset data

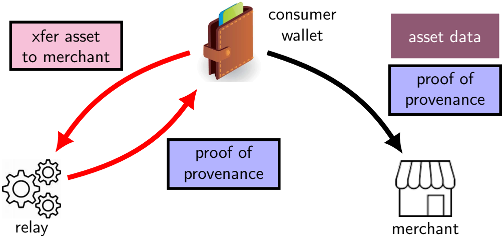
xfer asset to merchant

merchant

relay

proof of provenance

Or, Alice can give Bob control first & possession later (semi-offline):



xfer asset to merchant

consumer wallet

asset data

proof of provenance

proof of provenance

relay

merchant

Further reading

G Goodell, D Toliver, and H Nakib. **'A Scalable Architecture for Electronic Payments.'** November 2021. http://dx.doi.org/10.2139/ssrn.3951988

G Goodell and H Nakib. **'The Development of Central Bank Digital Currency in China: An Analysis.'** LSE Systemic Risk Centre, November 2021. https://www.systemicrisk.ac.uk/sites/default/files/2021-12/2108.05946.pdf

G Goodell, H Nakib, and P Tasca. **'A Digital Currency Architecture for Privacy and Owner-Custodianship.'** *Future Internet* 2021, 13(5), May 2021. https://doi.org/10.3390/fi13050130

G Goodell, H Nakib, and P Tasca. **'Digital Currency and Economic Crises: Helping States Respond.'** LSE Systemic Risk Centre Special Papers SP 20, September 2020, presented at 6th Annual Peer-to-Peer Financial Systems Workshop (P2PFISY 2020). https://systemicrisk.ac.uk/sites/default/files/2020-09/SP-20_0.pdf

G Goodell and T Aste. **'Can Cryptocurrencies Preserve Privacy and Comply with Regulations?'** *Frontiers in Blockchain*, May 2019. https://doi.org/10.3389/fbloc.2019.00004

G Goodell. **'Privacy by Design in Value-Exchange Systems.'** Discussion Paper, June 2020. https://arxiv.org/abs/2006.05892

Designing a better cashless payment infrastructure

"Future Infrastructure for Retail Remittances"

How can we create a cashless payment infrastructure that works for everyone?

WE'RE HIRING

UCL is seeking a new Research Fellow in Computational Finance to work on CBDC

Enquiries:

`g.goodell@ucl.ac.uk`