Designing Partitioned Digital Asset Infrastructure

Presentation to 11th Fintech Conference, Luxembourg

Geoff Goodell (University College London)

8 October 2025

Accounts all the time!

(What if “on**line**” is just another “**line** of credit”?)

Most modern digital payments are custodial...

	custodial	non-custodial
digital	card payments interbank transfers	
physical		cash paper vouchers

...but third-party custody is not a law of nature

	custodial	non-custodial
digital	card payments interbank transfers	opportunity for digital cash
physical		cash paper vouchers

Purely custodial payments are incompatible with privacy

Current efforts by the ECB and other central banks assume that money used for payments **must** only be held by **third-party custodians**.

Purely custodial payments are incompatible with privacy

Current efforts by the ECB and other central banks assume that money used for payments **must** only be held by **third-party custodians**.

- For the transaction to succeed, **custodians must share information**.
- Therefore, if the payer's custodian implements KYC, then the payment is **linkable** to the identity of the payer.
- The **chain of custody** created by successive custodians links all successive payees to the history of transactions.
- There is no privacy with third-party custodial payments.

What about “dual-offline” payments?

Fair exchange requires a **mutually trusted third party**, but it is a mistake to rely on **secure elements** or **secure enclaves** at the system level:

What about “dual-offline” payments?

Fair exchange requires a **mutually trusted third party**, but it is a mistake to rely on **secure elements** or **secure enclaves** at the system level:

- (**1**) **Security risk.** Any sufficiently powerful state actor or organised crime can compromise any hardware device in its possession.
- (**2**) **Treacherous computing.** The device serves a second master that is not the user; can the user really trust it?
- (**3**) **Chilling to innovation.** Users or businesses cannot create their own devices that would work without special, authorised hardware.
- (**4**) **Surplus capture.** Fabrication carries high fixed costs, so the market for trusted device manufacturers will be concentrated.
- (**5**) **Still third-party custody!** The trusted device de facto operates within the security envelope of an asset custodian.

It is better to focus on ways to hold money offline and transact online.

What about using balances and transacting with ZKP?

Zero-knowledge proofs can be used to avoid revealing information about the identity of the payer in a transaction.

For example, proposals such as **Platypus** and **PEReDi** employ open-source wallets that maintain balances and send transactions along with proofs that the payer's balance is greater than zero following the transaction.

What about using balances and transacting with ZKP?

Zero-knowledge proofs can be used to avoid revealing information about the identity of the payer in a transaction.

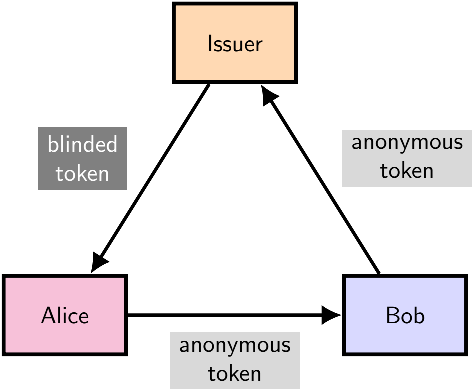
For example, proposals such as **Platypus** and **PEReDi** employ open-source wallets that maintain balances and send transactions along with proofs that the payer's balance is greater than zero following the transaction.

- But: Payers must maintain historical **evidence** to generate the proofs.
- Payers can be blackmailed to provide this evidence on demand.
- Recipients also accumulate **evidence** that can be cross-referenced to information held by the payer.
- Money held in the form of a balance is unsafe for privacy, even if **privacy-enhancing technologies** are used to transact.

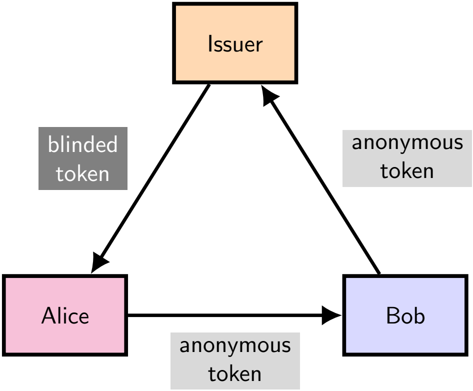
We need **e-cash tokens**, outside accounts

E-cash tokens, outside accounts

Chaum (1981)

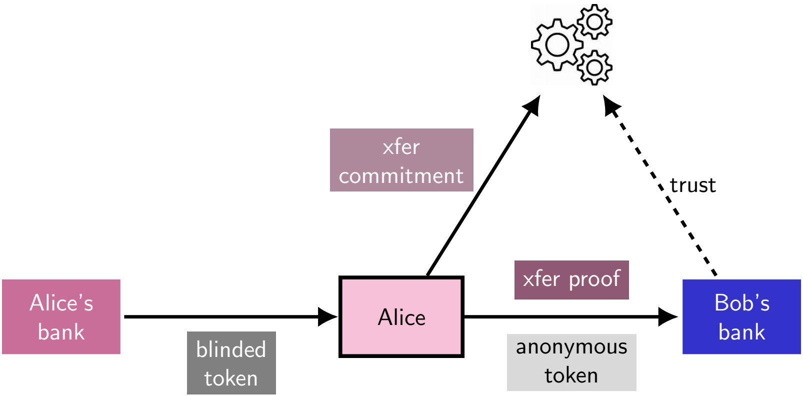

Issuer
blinded token
anonymous token
Alice
Bob
anonymous token

Chaum (1981)



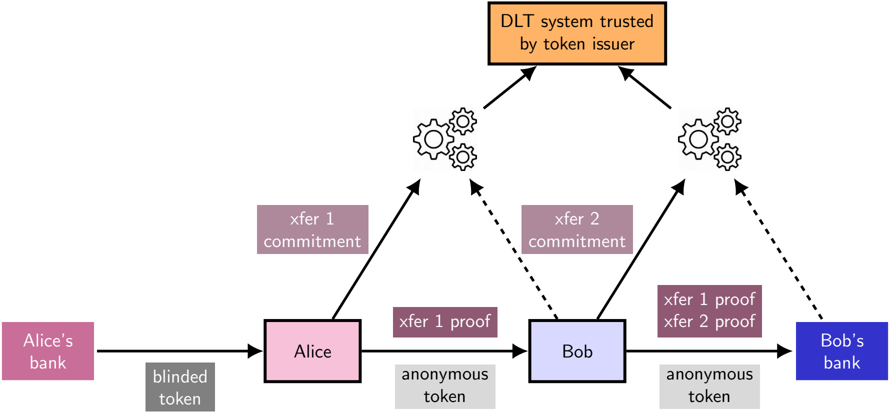
- Issuer is in the **"hot loop"** (race condition & risk for Alice)
- Issuer must maintain a **database** of received tokens (operational risk)
- Issuer can **equivocate** about transactions (security risk)

Goodell, Toliver, Nakib (2022)



- Bob's bank **facilitates** the transaction without knowing who Alice is
- Commitments are oblivious, containing nothing to identify counterparties
- Any entity **mutually trusted** by the counterparties can run a relay
- Users still have **bank accounts**, but payments are **unlinked**

Goodell, Toliver, Nakib (2022)



- Recipients can also use **non-custodial wallets** to hold assets
- Regulators may require transfers to include the identity of the **payee**
- A DLT system may be used to address the risk of relays **equivocating**

Some misconceptions

Misconceptions about digital payments

MYTH 1

"A consumer's balance must always be managed in an account."

Misconceptions about digital payments

MYTH 1

"A consumer's balance must always be managed in an account."

- Accounts imply **accountability** for account holders.
- It is technically possible for consumers to hold **bearer tokens** directly, outside accounts.
- If desired, rules may require that bearer tokens can be transferred only to accounts.

Misconceptions about digital payments

MYTH 2

“Holding limits are necessary to prevent bank runs.”

Misconceptions about digital payments

MYTH 2

"Holding limits are necessary to prevent bank runs."

- Protection against bank runs involving CBDC can be realised with **withdrawal limits** instead (cf Greece 2015).
- Withdrawal limits are **more effective** anyway, since runs comprise withdrawals, not aggregate holdings. What matters are the changes in holdings!

Misconceptions about digital payments

MYTH 3

"The payer must always be identifiable."

Misconceptions about digital payments

MYTH 3

"The payer must always be identifiable."

- **Consumers** have human rights.
- With cash, payers can be **anonymous** and **not discoverable** provided that certain rules are met (e.g. concerning transaction size).
- Ensuring that **payees** are identifiable (and preventing them from becoming payers without authorisation) is sufficient to enforce **tax**, **sanctions**, and **anti-fraud** compliance.
- The FATF "Travel Rule" was created during an era when most retail transactions were done with **cash**, and was fundamentally about preventing **custodians** from misbehaving.

Misconceptions about digital payments

MYTH 4

“To prevent abuse, the issuer must know where all the tokens are.”

Misconceptions about digital payments

MYTH 4

"To prevent abuse, the issuer must know where all the tokens are."

- It is sufficient to ensure that tokens are **unforgeable** and that **rules** for transactions are satisfied.
- Rules for transactions may include requirements that payees have **authorisation** to receive payments, or that such payments must be **reported**.

Misconceptions about digital payments

MYTH 5

"Consumers must always have the option to ask their banks to unwind a transaction."

Misconceptions about digital payments

MYTH 5

"Consumers must always have the option to ask their banks to unwind a transaction."

- Not all consumers want **credit**.
- Vendors generally want transaction **finality**.
- CBDC designs can allow consumer devices to **verify** payees before sending money.
- Additional fraud protections can be implemented outside the payment channel, where consumers can volunteer to provide information about problematic transactions.
- Have **banks** replaced **police** in resolving fraud claims?

Conclusion

Conclusion: Separating payments from banking

What are **banks** really for?

- Traditionally, **taking deposits** and making **risky investments** (banking)
- Increasingly, **payment services**, with revenue from **fees** and **data harvesting** (not banking), not to mention **police functions**
- These functions can (and should) be separated

Payments are largely a **telecommunications** problem

- Banks have a role in payments because of the use of **accounts**
- But digital currency allows for **digital money outside accounts**

Service providers can collect revenues from **facilitating transactions** (even if they are oblivious to what they are facilitating)

- Maybe a first step toward separating payments from the assumption that both parties to a transaction must use **custodial accounts**
- We can put **money for payments** back under the control of asset owners

Thank You

Contribute to a better payments landscape!

The UCL **Future of Money** Initiative

`https://fmi.cs.ucl.ac.uk/`

Collaboration and partnership opportunities

`g.goodell@ucl.ac.uk`

Further reading

G Goodell, H Nakib, and T Aste. **'Retail Central Bank Digital Currency: Motivations, Opportunities, and Mistakes.'** March 2024. To appear, *International Journal of Political Economy* (2025). https://doi.org/10.2139/ssrn.4769226

G Goodell, D Toliver, and H Nakib. **'A Scalable Architecture for Electronic Payments.'** Presented at WTSC, Grenada, May 2022. In: S Matsuo et al., Financial Cryptography and Data Security. FC 2022 International Workshops. *Lecture Notes in Computer Science*, volume 13412, 2023. Springer, Cham. https://doi.org/10.1007/978-3-031-32415-4_38

D Friolo, G Goodell, D Toliver, and H Nakib. **'Private Electronic Payments with Self-Custody and Zero-Knowledge Verified Reissuance.'** Presented at CoDecFin, Miyakojima, April 2025. To appear, *Lecture Notes in Computer Science*. https://doi.org/10.48550/arXiv.2409.01958

G Goodell. **'Token-Based Payment Systems.'** July 2021. To appear, *Elgar Encyclopedia of Cryptocurrencies, Blockchain, and DLT*. https://doi.org/10.48550/arXiv.2207.07530

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