Privacy-Enabling Electronic Value Exchange

University College London

Geoff Goodell

16 November 2018

g.goodell@ucl.ac.uk

Agenda

Background

- Modern Retail Payments
- Cryptocurrencies

Proposals for a Privacy-Enabling Electronic Value Exchange

- (1) Institutionally Supported Privacy-Enabling Cryptocurrency
- (2) Institutionally Mediated Private Value Exchange

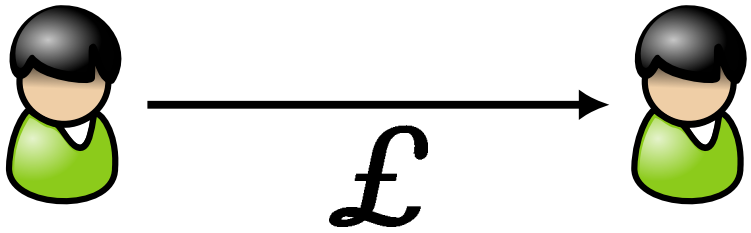
Discussion

Desiderata for Payment Methods

- Robust to cyberattacks
- Usable without registration
- Unlinkable transactions
- Electronic transactions
- Fungible
- Suitable for taxation
- Can block some illicit uses
- Supports monetary policy

Modern Retail Payments

Cash



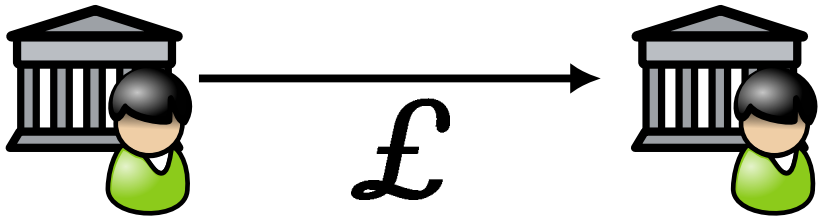
Direct interaction between transacting parties.

Currency is held **locally**.

Transactions cannot be **intermediated** or **blocked**.

Unlimited **choice** of currency.

Retail Banking (cards, EFT, etc)



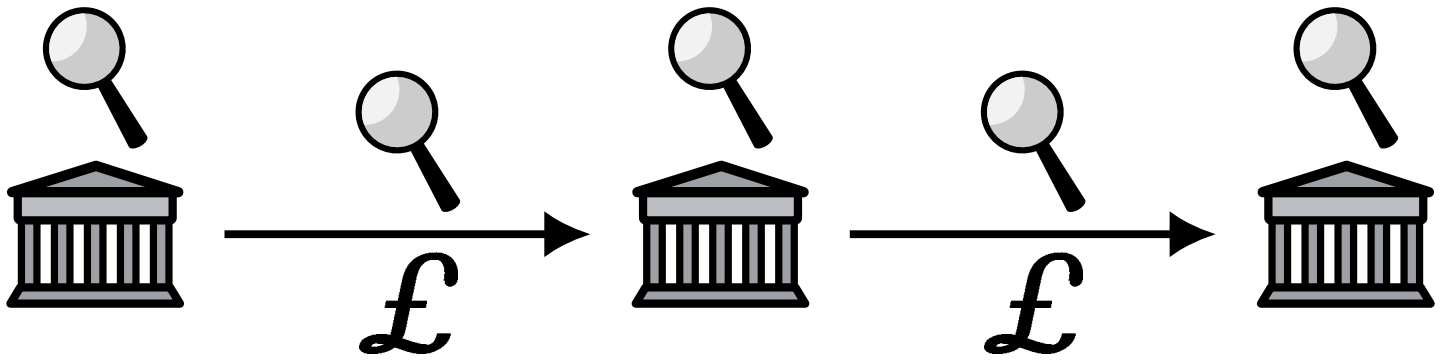
Interaction is actually between **regulated institutions**.

Currency is held **by institutions**.

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

Choice of currency may be limited by **regulations**.

Modern Retail Payments

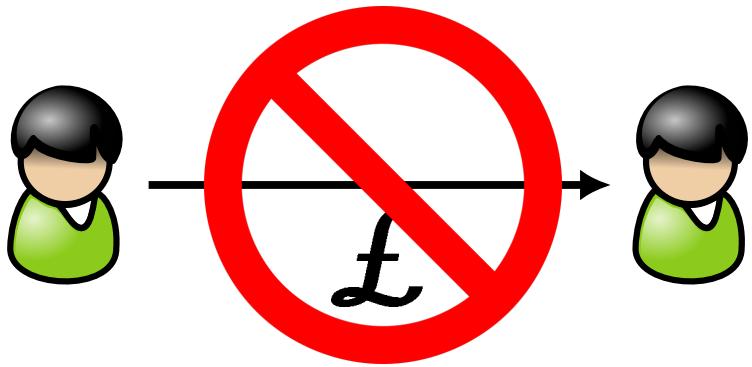


Institutional **accounts** and **transfers** between institutions may be monitored by a variety of observers.

Observers may include:

- regulators
- credit bureaus, lenders, insurers, and other data consumers
- other government authorities (cf Snowden disclosure)
- unscrupulous insiders
- hackers (state-sponsored?) (foreign governments?)

Modern Retail Payments: Toward a Cashless Society?



Widely seen as inevitable

- Some central banks (including UK, US, CH) promise to keep cash (for now)
- But research shows increasing popularity of electronic payments

Advantages of cashlessness may include reduced **tax evasion** and **crime**

- See arguments by Kenneth Rogoff, Narendra Modi

But cashlessness comes at the cost of **privacy**:

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

Institutional Posture on Payments

Anti-Money Laundering (**AML**) and "Know Your Customer" (**KYC**) reguations around the world:

- Financial institutions must **collect identification data** on all clients
- Financial institutions must monitor their clients and **report suspicious activity**

Financial Action Task Force (**FATF**)

- A framework for **blacklisting** non-compliant governments and punishing businesses in their countries

Main idea:

- All electronic financial transactions must take place between accounts held by **regulated institutions**.
- Each account must be associated with the **unitary identity** of its owner.

The Challenge

Christine Lagarde
Managing Director
International Monetary Fund
(at Singapore Fintech
Festival on Wednesday)

"Imagine that people purchasing beer and frozen pizza have higher mortgage defaults than citizens purchasing organic broccoli and spring water. What can you do if you have a craving for beer and pizza but do not want your credit score to drop? Today, you pull out cash. And tomorrow? Would a privately-owned payment system push you to the broccoli aisle?

"Would central banks jump to the rescue and offer a fully anonymous digital currency? Certainly not. Doing so would be a bonanza for criminals."

`https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency`

Cryptocurrencies are Really about Privacy

A "Pre-History" of Modern Cryptocurrencies

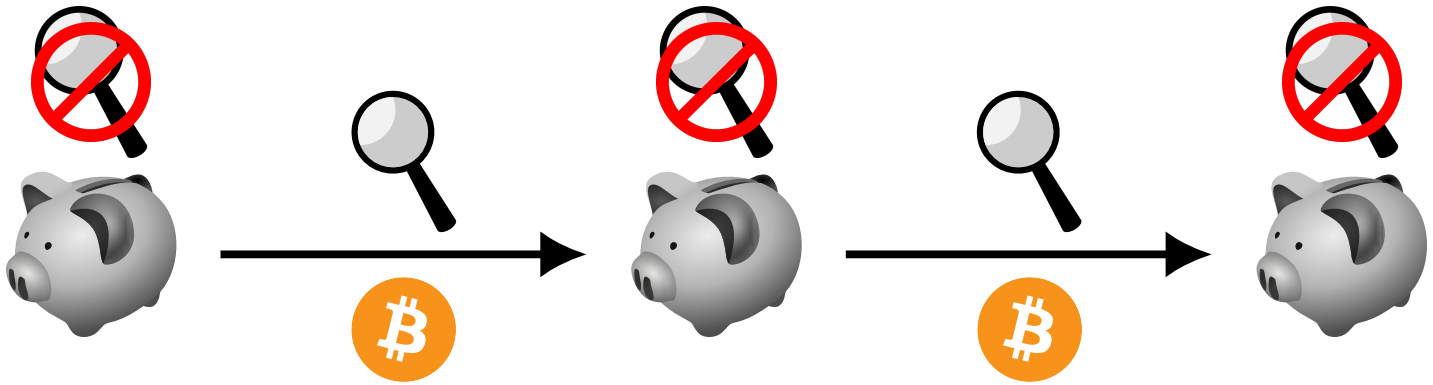
- **1982**: David Chaum, "Blind Signatures for Untraceable Payments."
- **1989**: DigiCash (Ecash) started by David Chaum
- **1996**: E-gold
- **2006**: Liberty Reserve

When Bitcoin launched in **2009**, the **financial crisis** offered an alternative justification (avoiding currency devaluation).

Privacy-oriented **enhancements** and **alternatives** continued to evolve:

- **2014**: Monero
- **2016**: Mimblewimble

"Basic" Cryptocurrency (e.g. Bitcoin)



Users can transact **without accounts**, avoiding AML/KYC

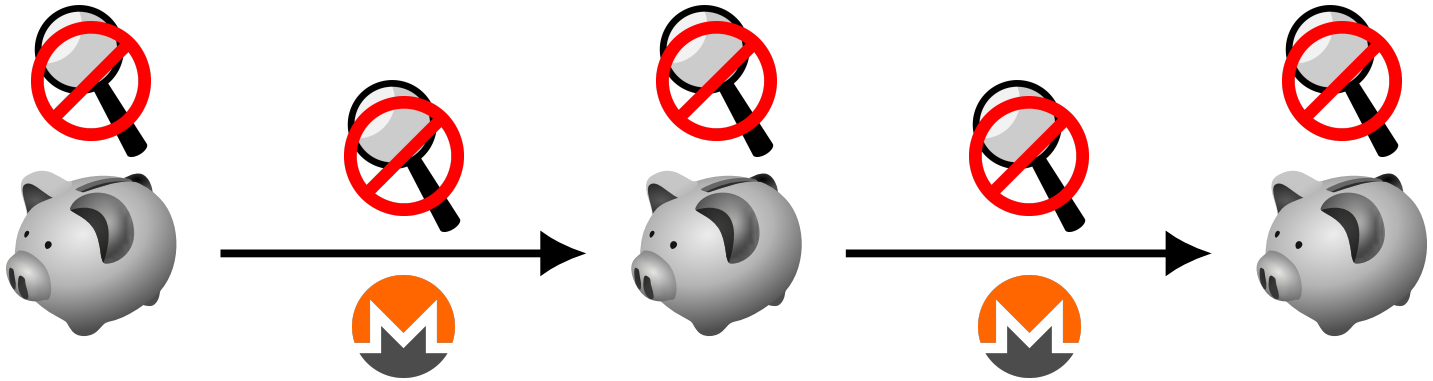
But most users use **wallet services**, e.g. *blockchain.info*, *myetherwallet*

Without wallet services: coin stores may be private; **transactions** are not:

- Transactions may be **linked** to each other, forming a chain
- In some ways, more traceable than institutional transfers

Not fungible: "clean" versus "dirty" tokens

"Privacy-Enabling" Cryptocurrency (e.g. Monero)



Second-Generation cryptocurrencies such as *Monero* and *Zcash* are explicitly designed to address traceability concerns.

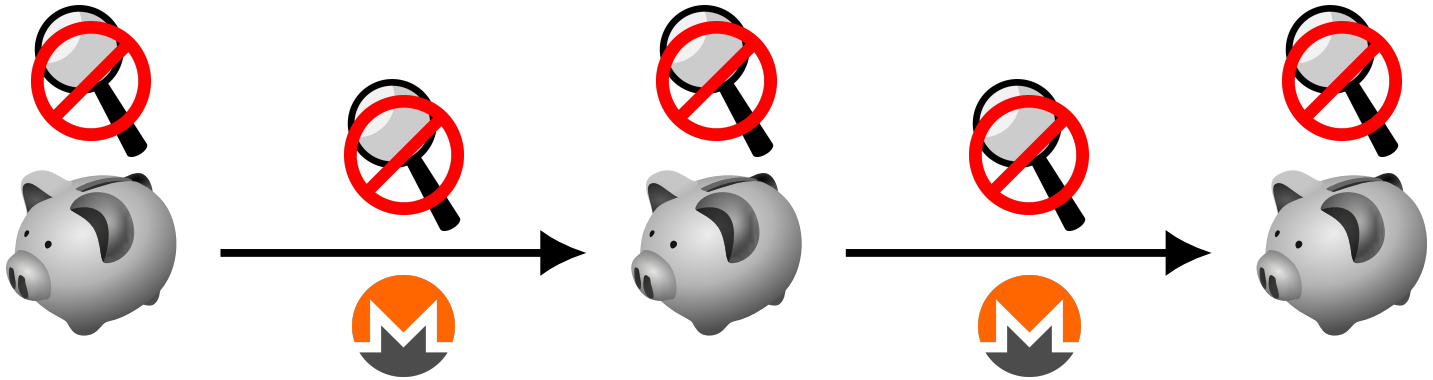
Technologies include:

Ring signatures, which allow signed messages to be attributable to "a set of possible signers without revealing which member actually produced the signature" [Rivest et al, 2001]

Stealth addresses, in which public keys can be derived separately from private keys for the purpose of obscuring the public keys [Courtois 2017]

Confidential transactions, which use Pedersen commitment schemes [Pedersen 1991] to restrict disclosing the amounts transacted to anyone other than the transacting parties [van Wirdum 2016]

"Privacy-Enabling" Cryptocurrency (e.g. Monero)



Second-Generation cryptocurrencies such as *Monero* and *Zcash* are explicitly designed to address traceability concerns.

Weaknesses

Privacy-enabling cryptocurrencies still have serious **technical shortcomings**. "Privacy isn't a thing you achieve, it's a constant cat-and-mouse battle" — Ricardo Spagni, Monero, 2018

Not enough users are taking advantage of anonymity features (e.g., of Zcash) for them to be effective.

So-called "privacy coins" have been **banned** by government agencies such as Japanese Financial Security Agency and US Secret Service.

Comparison of Various Payment Methods

	cash	modern retail banking	traditional cryptocurrency (e.g. Bitcoin)	privacy-enabling cryptocurrency (e.g. Monero)
Robust to cyberattacks	●	○	○	○
Usable without registration	●	○	●	●
Unlinkable* transactions	◑	○	○	●
Electronic transactions	○	●	●	●
Fungible	●	●	○	●
Suitable for taxation	◑	●	○	○
Can block some illicit uses	○	●	○	○
Supports monetary policy	●	●	○	○

Proposed Compromise Approaches

How to bridge the divide between **policymakers** and **cyberlibertarians**?

Two ideas for **compromise**:

(1) Institutionally Supported Privacy-Enabling Cryptocurrency

i.e., policymakers accept cryptocurrency

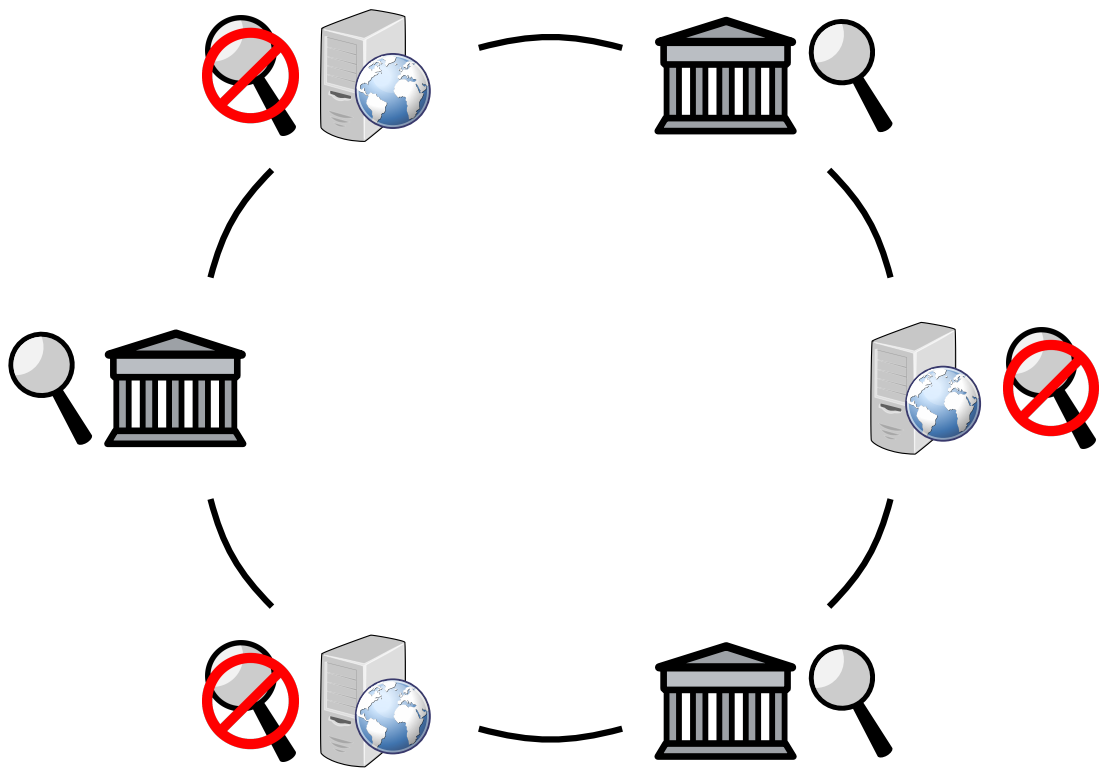
(they may have no other choice if they want to stay relevant)

(2) Institutionally Mediated Private Value Exchange

i.e., cyberlibertarians accept institutions

(they may have no other choice if they want to continue operating)

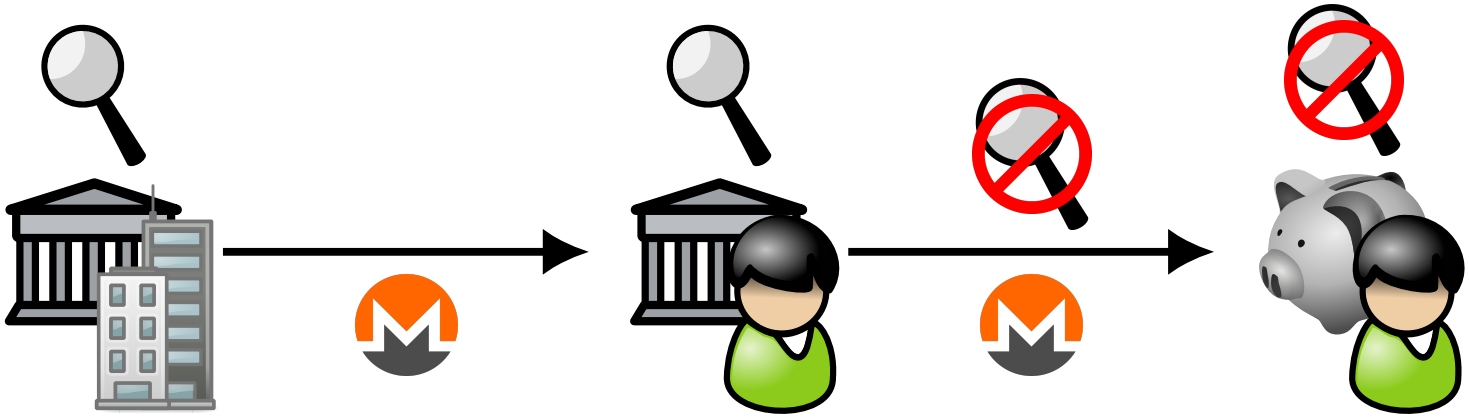
Institutionally Supported Privacy-Enabling Cryptocurrency



Institutions would join global networks of servers operating as nodes in existing cryptocurrency networks.

Not all participants in these networks are regulated institutions.

Institutionally Supported Privacy-Enabling Cryptocurrency



(Monero symbol used without loss of generality.)

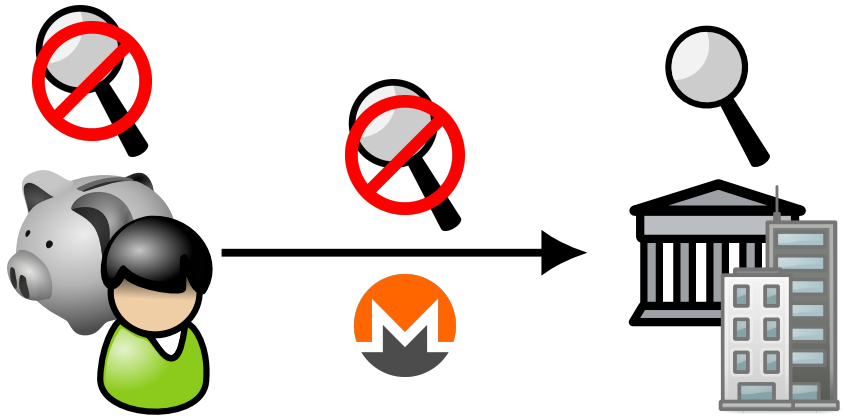
Corporations and registered businesses maintain **accounts** held by **regulated financial insitutions** (leftmost icon).

Such **accounts** would be subject to **monitoring** and may only remit cryptocurrency payments to other **accounts** held by regulated financial institutions.

Individuals and non-business partnerships (centre icon) may transfer cryptocurrency from accounts to **unmonitored, private storage** (rightmost icon).

Compare Zcash "T" (Transparent) and "Z" (Shielded) addresses.

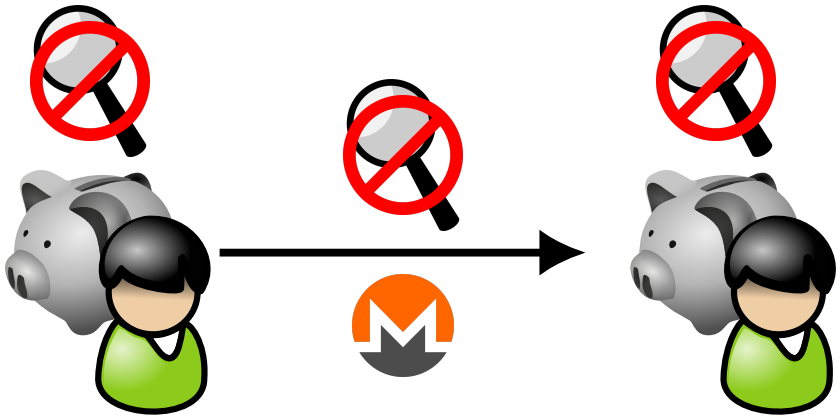
Institutionally Supported Privacy-Enabling Cryptocurrency



An individual (left) with a private store of cryptocurrency may remit payments without revealing her identity to a business with an account held by a regulated institution (right).

The business may or may not require authentication.

Institutionally Supported Privacy-Enabling Cryptocurrency

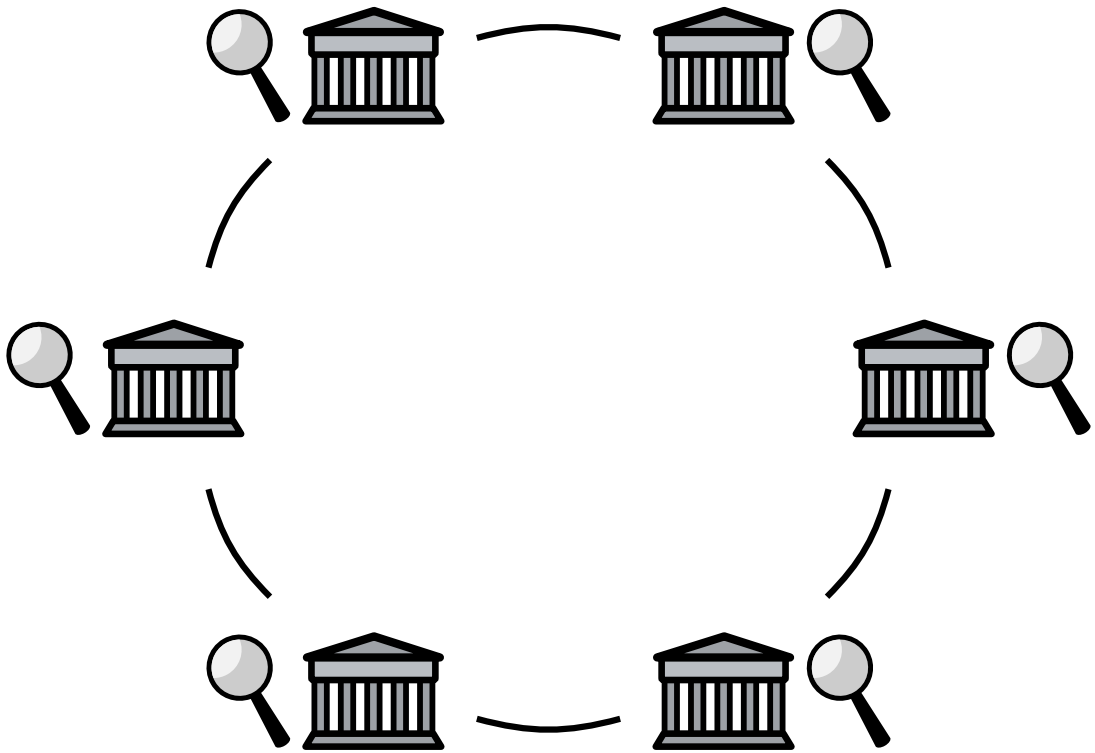


Individuals with private stores of privacy-enabling cryptocurrency may transact **directly** and **without revealing their identities**.

This ensures that money from institutions can be converted to **true cryptocurrency** and vice-versa.

This may pose a problem for governments wishing to implement **blacklists** and **economic sanctions**.

Institutionally Mediated Private Value Exchange



The distributed ledger is operated by a **federation of regulated institutions**.

Since the distributed ledger is private, it may use an energy-efficient **BFT consensus algorithm**.

Institutionally Mediated Private Value Exchange

About **self-regulation**:

Regulators make the rules; **regulated institutions** develop the technology.

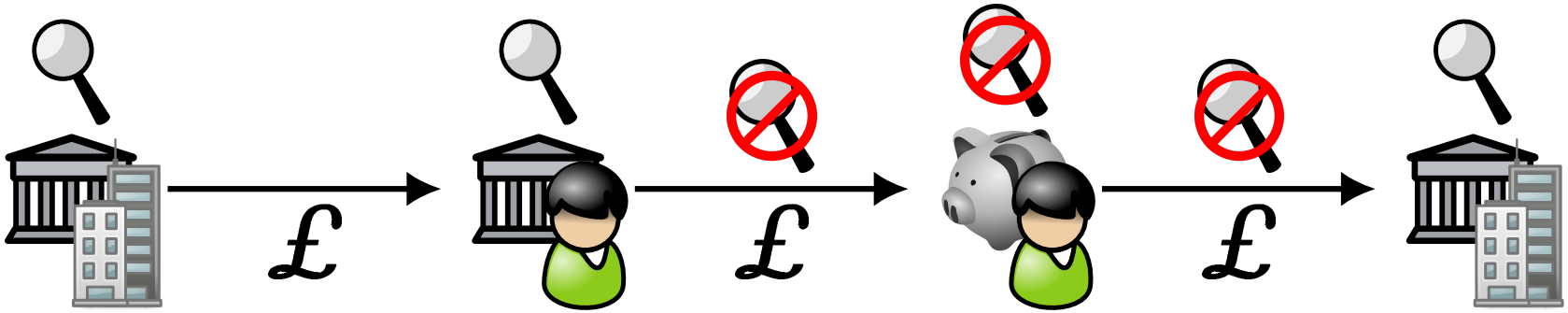
Regulation may **promote** rather than **inhibit** innovation.

Consider the example of the National Market System for exchanges that list US equities.[1]

- Exchanges were forced to participate in a real-time feed.
- A new market for smart order routers emerged.
- The New York Stock Exchange monopoly was broken.
- High-frequency traders benefited in the short term.
- Small-size traders benefited in the long term.

[1] `http://www.sechistorical.org/museum/timeline/2000-timeline.php`

Institutionally Mediated Private Value Exchange

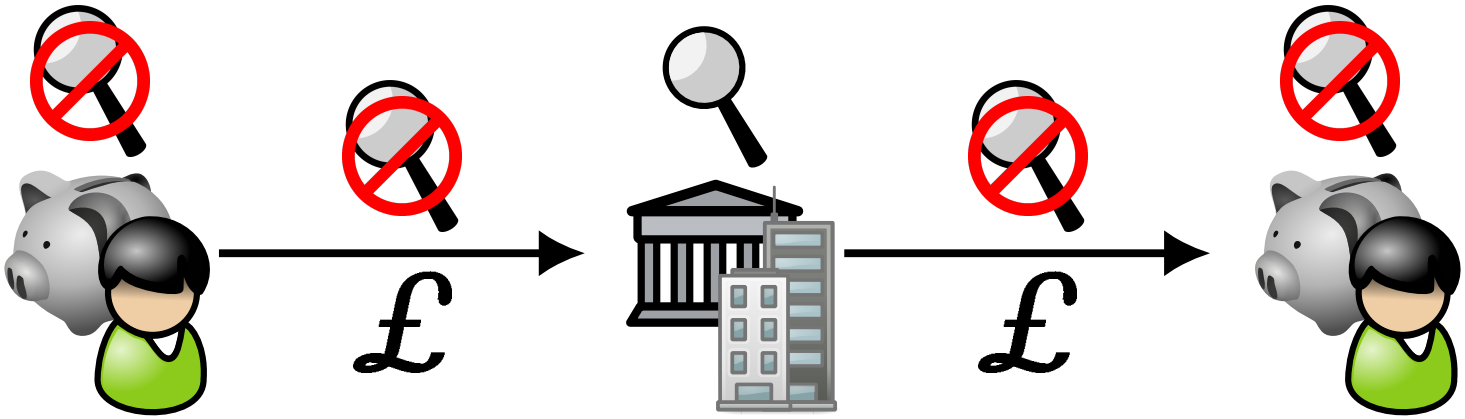


An individual receives funds into her **institutional account** (second icon from left) and transfers them to her **private store** (second icon from right).

The funds may be **state-issued currency** (as indicated by the Pound Sterling symbols) rather than cryptocurrency.

When she wants to make a payment, she must remit it from her private store to an account held by a **regulated institution** (rightmost icon).

Institutionally Mediated Private Value Exchange



Individuals (outer icons) wishing to transact with each other via their private stores rather than accounts with regulated institutions must transact via a **regulated intermediary** (centre icon).

The intermediary could charge a **fee** for its service.

The intermediary may require a less-stringent form of identification such as an **attribute-backed credential**.

Institutionally Mediated Private Value Exchange

Main challenge: how can we ensure that privacy is achieved and preserved?

Privacy is an ongoing endeavour of vigilance, responsiveness, and improvement (cf. P. Zimmermann 1991[2], R. Spagni 2018[3]).

The system must remain **distributed**, to ensure that no one has a panopticon view.

There must be an **open process** for admitting new participants, to ensure that harmful procedures do not develop away from the public eye.

There must be **continuous auditing** by the security community, to ensure that the claimed privacy characteristics are achieved.

There must be a **funded commitment** to maintain and develop the system to address technical shortcomings in achieving privacy requirements.

There must be a **diversity** of implementations, so that sporadic vulnerabilities do not threaten a large share of the users.

---

[2] `https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html`

[3] `https://www.wired.com/story/monero-privacy/amp`

Comparison of Various Payment Methods

	cash	modern retail banking	traditional cryptocurrency (e.g. Bitcoin)	privacy-enabling cryptocurrency (e.g. Monero)	inst. supported privacy-enabling cryptocurrency	institutionally mediated private value exchange
Robust to cyberattacks	●	○	○	○	○	○
Usable without registration	●	○	●	●	●	○
Unlinkable* transactions	◑	○	○	●	●	●
Electronic transactions	○	●	●	●	●	●
Fungible	●	●	○	●	●	●
Suitable for taxation	◑	●	○	○	●	●
Can block some illicit uses	○	●	○	○	○	●
Supports monetary policy	●	●	○	○	○	●

Discussion

Photo Credit: https://www.pinterest.co.uk/pin/736268239051855079/