GNU Taler – A privacy-preserving online payment system for libre societies

Christian Grothoff

Inria Rennes Bretagne Atlantique

27.7.2016

"Real talers have the same existence that the imagined gods have. Has a real taler any existence except in the imagination, if only in the general or rather common imagination of man? Bring paper money into a country where this use of paper is unknown, and everyone will laugh at your subjective imagination." –Karl Marx (Doctoral Thesis)

Design Choices

Internet Design Goals (David Clark, 1988)

1. **Internet communication must continue despite loss of networks or gateways.**
2. The Internet must support multiple types of communications service.
3. The Internet architecture must accommodate a variety of networks.
4. The Internet architecture must permit distributed management of its resources.
5. The Internet architecture must be cost effective.
6. The Internet architecture must permit host attachment with a low level of effort.
7. **The resources used in the internet architecture must be accountable.**

GNUnet Design Goals

1. GNUnet must be implemented as free software.
2. **The GNUnet must only disclose the minimal amount of information necessary.**
3. **The GNUnet must be decentralised and survive Byzantine failures in any position in the network.**
4. **The GNUnet must make it explicit to the user which entities must be trustworthy when establishing secured communications.**
5. **The GNUnet must use compartmentalization to protect sensitive information.**
6. The GNUnet must be open and permit new peers to join.
7. **The GNUnet must be self-organizing and not depend on administrators.**
8. The GNUnet must support a diverse range of applications and devices.
9. The GNUnet architecture must be cost effective.
10. **The GNUnet must provide incentives for peers to contribute more resources than they consume.**

Building the GNUnet

Internet
Facebook/Paypal
DNS/X.509
TCP/UDP
IP/BGP
Ethernet
Phys. Layer

GNUnet
SecuShare / **GNU Taler**
GNU Name System
CADET (Axolotl+SCTP)
R^5N DHT
CORE (OTR)
HTTPS/TCP/WLAN/...

Digital cash, made **socially responsible**.

Taxable, Anonymous, Libre, Practical, Resource Friendly

Dé central isé

informatiques mathématiques

Use Cases

- Internet e-commerce (convenient, efficient)

Use Cases

- Internet e-commerce (convenient, efficient)
- National “currency” (taxable, secure)

Use Cases

- Internet e-commerce (convenient, efficient)
- National “currency” (taxable, secure)
- Regional / community payment system (libre)

Value proposition: Customer

- Convenient: pay with one click
- Guaranteed: never fear being rejected by false-positives in the fraud detection
- Secure: like cash, except no worries about counterfeit
- Privacy-preserving: payment requires no personal information
- Stable: no currency fluctuations, pay in traditional currencies
- Free software: no hidden "gadgets", third parties can verify

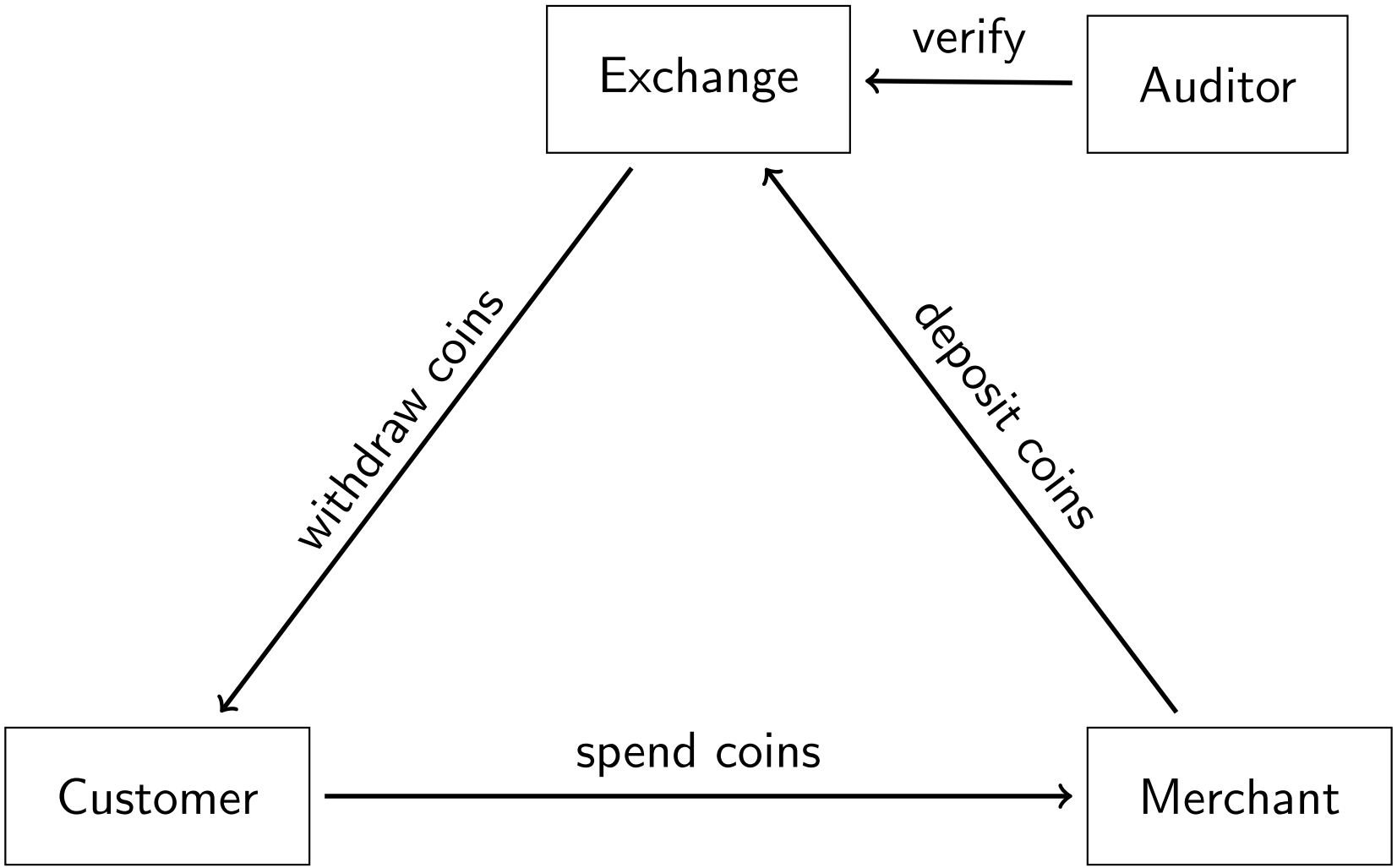
Value proposition: Merchant

- Fast: transactions at Web-speed
- Secure: signed contracts, no legitimate customer rejected by fraud decection
- Free software: competitive pricing and support
- Low fees: efficient protocol + no fraud = low costs
- Flexible: any currency, any amount
- Ethical: no fluctuation risk, no pyramid scheme, not suitable for illegal business

Value proposition: Government

- Free software = commons: no monopoly, preserve independence
- Taxabiliy: reduces black markets
- Efficiency: high transaction costs hurt the economy
- Security: signed contracts, no counterfeit
- Audited: no bad banks
- Privacy: protection against foreign espionage

Architecture of GNU Taler



Taxability

We say Taler is taxable because:

- Merchant's income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.

Taxability

We say Taler is taxable because:

- Merchant's income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.

Limitations:

- withdraw loophole
- copying coins among family and friends

Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Key goals:

- maintain unlinkability
- maintain taxability of transactions

Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Key goals:

- maintain unlinkability
- maintain taxability of transactions

Method:

- Wallet tells exchange to only pay *partial value* of a coin.
- Exchange allows wallet to obtain *unlinkable change* for remaining coin value.

Usability of Taler

`https://demo.taler.net/`

1. Install Chrome extension.
2. Visit the `bank.demo.taler.net` to withdraw coins.
3. Visit the `shop.demo.taler.net` to spend coins.

Business considerations

- Exchange needs a business to operate.
- Exchange operator income is from *transaction fees*.

Community considerations

- Initial accumulation: Who gets to mint currency?
- Speculation: Who controls the money supply?
- Social welfare:
  - Who gets to set tax rules and rates?
  - Who gets to allocate tax revenue?

Politics

Taler is political:

- Anarchists disagree with taxability.
- Authoritarians disagree with privacy.
- Communists disagree with enabling markets.

Politics

Taler is political:

- Anarchists disagree with taxability.
- Authoritarians disagree with privacy.
- Communists disagree with enabling markets.

Alternative solutions:

- ZeroCash: Anonymity for all, no central bank!
- Visa/Mastercard: Let the spies see it all to keep us safe!
- Barter: Hoarding cash is only for 1%-ers!

How to help?

- Think about how computer security may affect causes you care about
- Install and use Taler once it becomes available
- Translate documentation and user interfaces
- If you can program:
  - Write free software with clear licensing terms attached
  - Turn Taler demonstrator bank into community bank application
  - You're welcome to join the upstream development!

Conclusion

What can we do?

- Minimize data leakage:
  - Deploy Taler to establish socially responsible payment system
  - Use Taler to pay for mobile use instead of SIM-card based authentication
- Use free software, ensure computers serve their owners

Do you have any questions?

References:

1. Christian Grothoff, Bart Polot and Carlo von Loesch. *The Internet is broken: Idealistic Ideas for Building a GNU Network*. **W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)**, 2014.
2. Florian Dold, Sree Harsha Totakura, Benedikt Müller, Jeffrey Burdges and Christian Grothoff. *Taler: Taxable Anonymous Libre Electronic Reserves*. Available upon request. 2016.
3. Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt**, 2015.

Let money facilitate trade; but ensure capital serves society.