Anonymous Payment Systems

Christian Grothoff

Institut National de Recherche en Informatique et en Automatique (Inria)
The GNU Project
Ashoka Fellow

1.11.2016

"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)

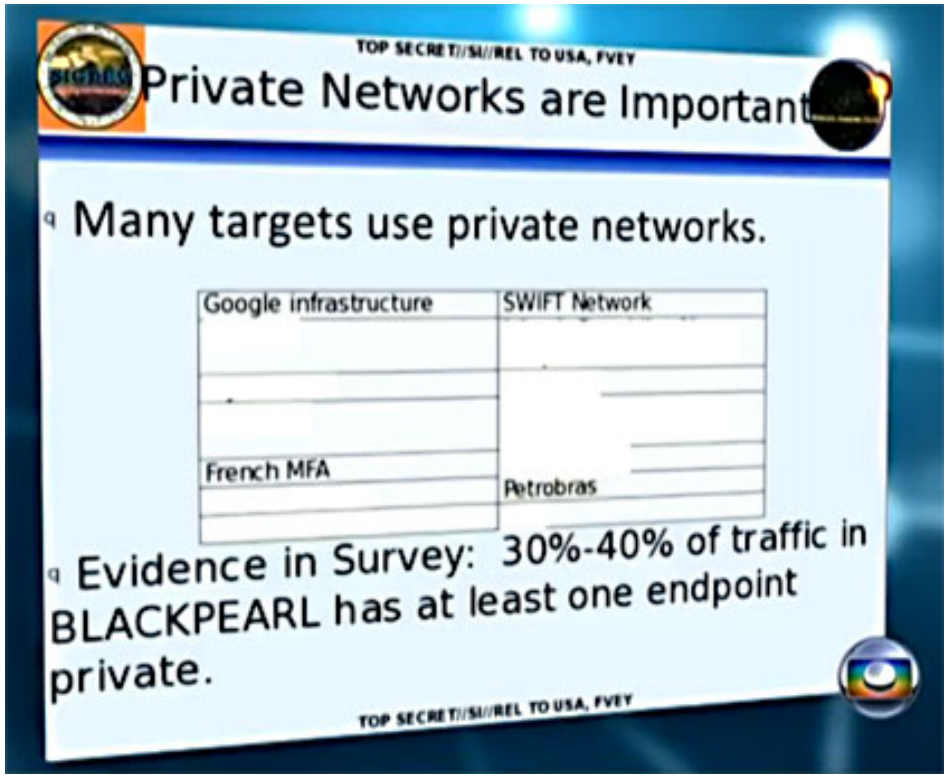
Motivation

Modern economies need currency ...

Motivation

Modern economies need payments online.

SWIFT?



SWIFT/Mastercard/Visa are too transparent.

This was a question posed to RAND researchers in 1971:

> *"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be too obtrusive or obvious. What would be your decision?"*

The result: an electronic funds transfer system that looks strikingly similar today's debit card system.

"I think one of the big things that we need to do, is we need to get a way from true-name payments on the Internet. The credit card payment system is one of the worst things that happened for the user, in terms of being able to divorce their access from their identity."

–Edward Snowden, IETF 93 (2015)

Bitcoin

- Unregulated payment system and currency: lack of regulation is a feature!
- Implemented in free software as a decentralised peer-to-peer system

Bitcoin

- Unregulated payment system and currency: lack of regulation is a feature!
- Implemented in free software as a decentralised peer-to-peer system
- Decentralised banking requires solving Byzantine consensus
- Creative solution: tie initial accumulation to solving consensus problem

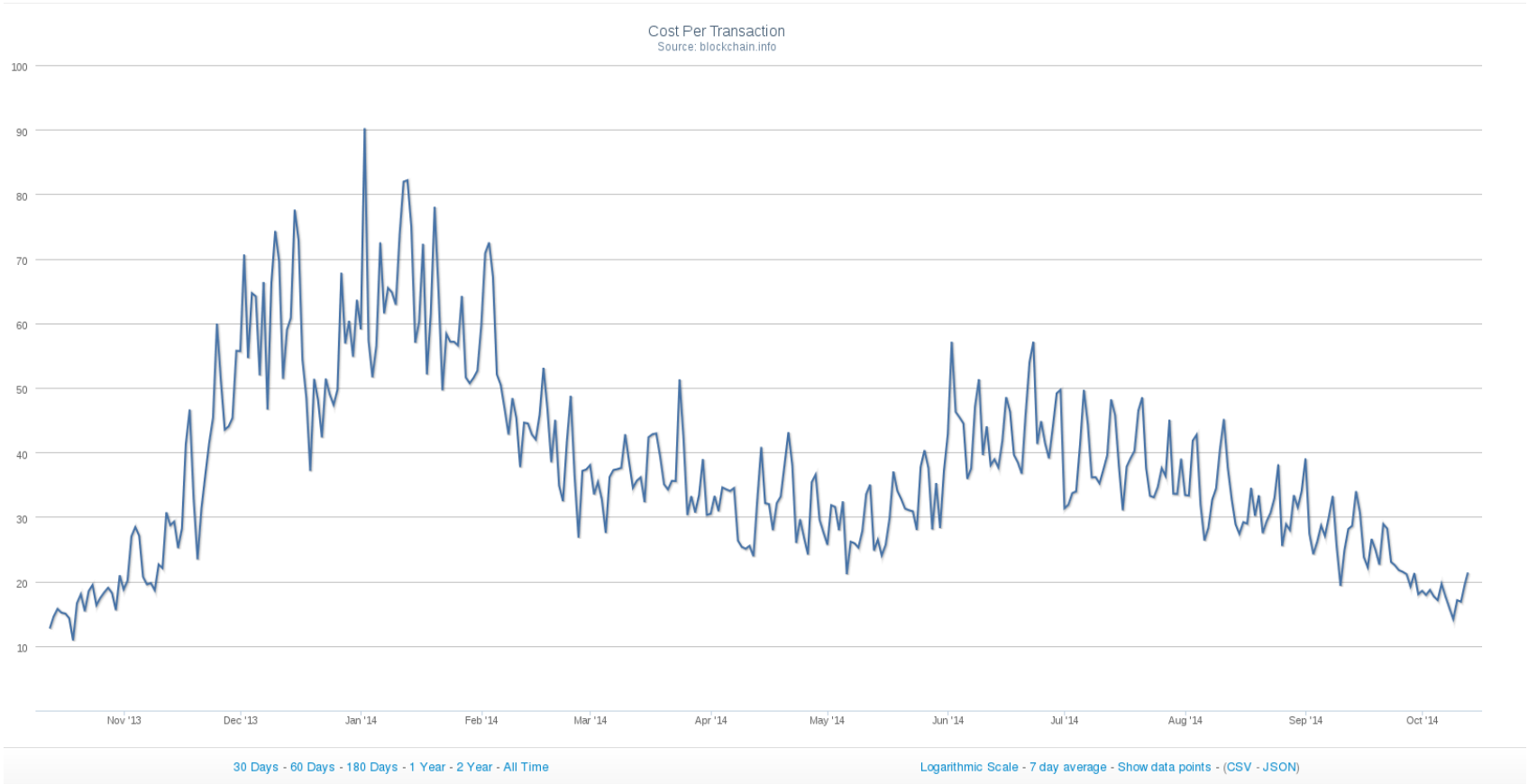
Bitcoin

- Unregulated payment system and currency: lack of regulation is a feature!
- Implemented in free software as a decentralised peer-to-peer system
- Decentralised banking requires solving Byzantine consensus
- Creative solution: tie initial accumulation to solving consensus problem

  $\Rightarrow$ Proof-of-work advances ledger

  $\Rightarrow$ Very expensive banking

?



Current average transaction value: $\approx$ 1000 USD

BitCoin cryptography is rather primitive: All transactions are public and linkable!

$\Rightarrow$ BitCoin does not come with privacy guarantees

$\Rightarrow$ BitCoin was enhanced with "laundering" services

$\Rightarrow$ ZeroCoin, CryptoNote (Monero) and ZeroCash (ZCoin) offer "full" anonymity


Anonymization technology

- Coin creation and distributed ledger basically remain
- Transactions are no longer simply signed by the owner
- Instead, currency is transferred from a *pool of owners* to another *pool of owners*
- Impossible to say which specific owner initiated the transfer (there is just a zero knowledge proof it was somebody authorized)
- Impossible to say who became the new owner (just somebody now can prove that he has the right to authorize a transfer)
- Cryptography used is somewhat experimental (zk-SNARK) and expensive

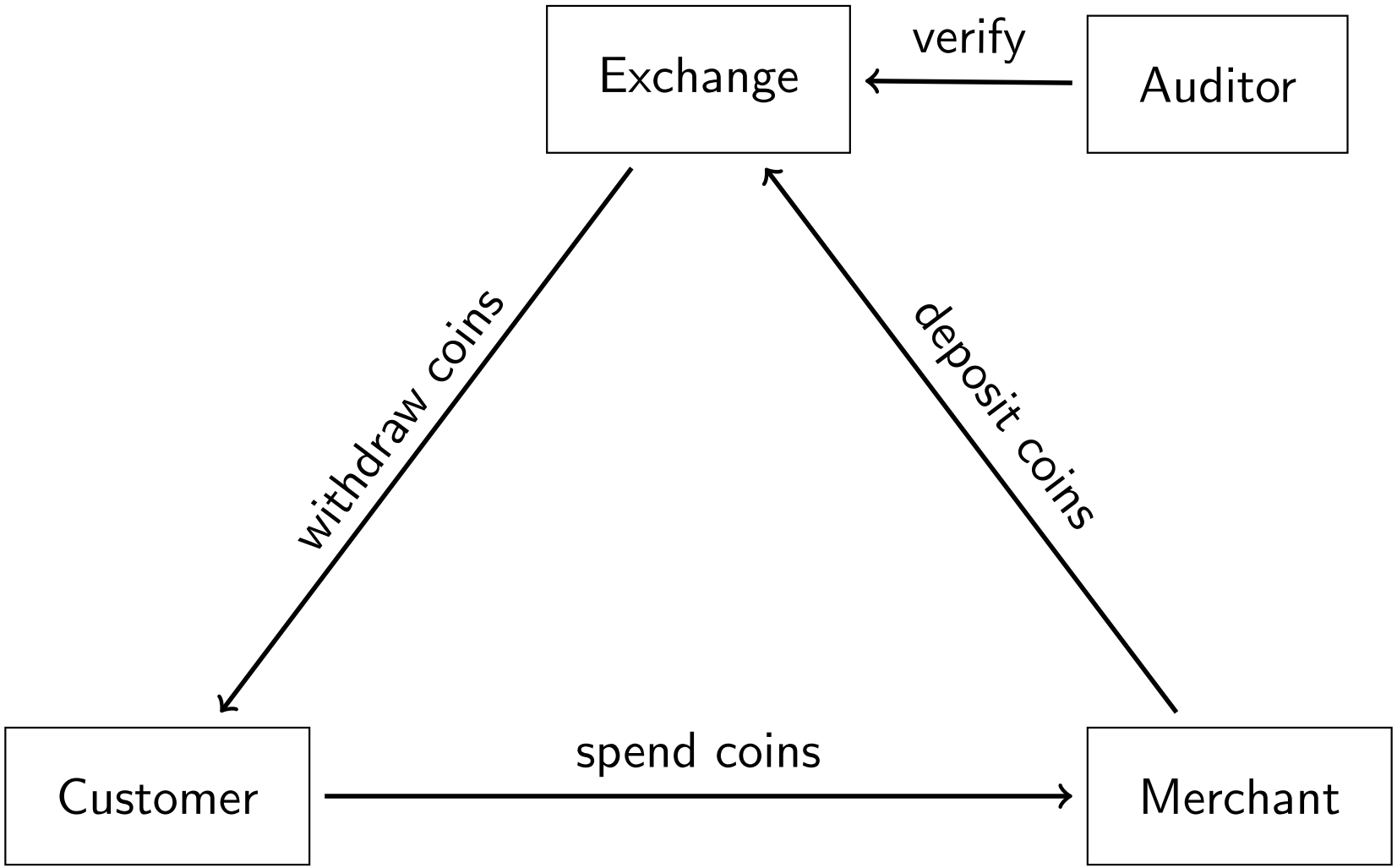
  $\Rightarrow$ Further research might enable us to find attacks (arms race)

Is society ready for an anarchistic economy?

Digital cash, made **socially responsible**.

Taxable, Anonymous, Libre, Practical, Resource Friendly

Architecture of GNU Taler



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.

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

Merchant Integration: Wallet Detection

```
<script src="taler-wallet-lib.js"></script>
<script>
  taler.onPresent(() => {
    alert("Taler␣wallet␣is␣installed");
  });
  taler.onAbsent(() => {
    alert("Taler␣wallet␣is␣not␣installed");
  });
</script>
```

Merchant Integration: Payment Request

```
HTTP/1.1 402 Payment Required
Content-Type: text/html; charset=UTF-8
X-Taler-Contract-Url: https://shop/generate-contract/42

<!DOCTYPE html>
<html>
  <!-- fallback for browsers without the Taler extension -->
  You do not seem to have Taler installed, here are other
  payment options ...
</html>
```


Merchant Integration: Contract


```
{
  "H_wire":"YTH0C4QBCQ10VDNTJN0DCTTV2Z6JHT5NF43F0RQHZ8JYB5NG4W4G..
  "amount":{"currency":"EUR","fraction":1,"value":0},
  "auditors":[{"auditor_pub":"42V6TH91Q83FB846DK1GW3JQ5E8DS273W423
  "exchanges":[{"master_pub":"1T5FA8VQHMMKBHDMYPRZA2ZFK2S63AKF0YTH
                "url":"https://exchange/"}],
  "expiry":"/Date(1480119270)/",
  "fulfillment_url": "https://shop/article/42?tid=249960194066269&
  "max_fee":{"currency":"EUR","fraction":01,"value":0},
  "merchant":{"address":"Mailbox␣4242","jurisdiction":"Jersey","na
  "merchant_pub":"Y1ZAR5346J3ZTEXJCHQY9NJN78EZ2HSKZK8M0MYTNRJG5N0H
  "products":[{
    "description":"Essay:␣The␣GNU␣Project",
    "price":{"currency":"EUR","fraction":1,"value":0},
    "product_id":42,"quantity":1}],
  "refund_deadline":"/Date(1471522470)/",
  "timestamp":"/Date(1471479270)/",
  "transaction_id":249960194066269
}
```


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
- *sharing* 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.

Crypto summary

Taler's cut-and-choose refresh protocol allows:

- To give unlinkable change.
- To give refunds to an anonymous customer.
- To expire old keys and migrate coins to new ones.
- The owner of the original coin to *later* recover the private keys of the change.
- Transaction attempts based on change become equivalent to *sharing* private keys.

Business considerations

- Exchange needs to be a legal (!) business to operate.
- Exchange operator income is from *transaction fees*.
- Now trying to find partners and financing for startup.

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:

- ZCash: 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!

Evolution Matrix

	ZeroCoin	CryptoNote	ZeroCash	GNU Taler
Bandwidth	45000 b	13000 b	1000 b	$\approx$ 1000 b
CPU spend	500 ms	10 ms	45s	1 ms
CPU verify	450 ms	10 ms	6 ms	2 ms
Anonymity set	ZC subset	freq. dep.	all users	customers
Change	no	yes	yes	yes
Scalability	—	?	?	+++
Trans. cost	100 USD?	20 USD?	20 USD?	0.0001 USD

Note: Approximate figures based on current reading of the papers, not on scientific comparative experiments.

Conclusion

What can we do?

- Suffer mass-surveillance enabled by credit card oligopolies with high fees, and
- Engage in arms race with deliberately unregulatable blockchains

OR

- Establish free software alternative balancing social goals

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. Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. *Enabling Secure Web Payments with GNU Taler*. **SPACE 2016**.
3. Florian Dold, Sree Harsha Totakura, Benedikt Müller, Jeffrey Burdges and Christian Grothoff. *Taler: Taxable Anonymous Libre Electronic Reserves*. Available upon request. 2016.
4. Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer and Madars Virza. *Zerocash: Decentralized Anonymous Payments from Bitcoin*. **IEEE Symposium on Security & Privacy, 2016**.
5. David Chaum, Amos Fiat and Moni Naor. *Untraceable electronic cash*. **Proceedings on Advances in Cryptology, 1990**.
6. Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt**, 2015.

Let money facilitate trade; but ensure capital serves society.

RSA blind signatures

(1) RSA key generation

1. Pick random primes p, q.
2. Compute $n := pq$, $\phi(n) = (p-1)(q-1)$
3. Pick small $e < \phi(n)$ such that $d := e^{-1} \mod \phi(n)$ exists.
4. Publish public key (e, n).

(3) Blind signing

1. Receive m'.
2. Compute $s' := m'^d \mod n$.
3. Send signature s'.

(2) Blinding

1. Obtain public key (e, n)
2. Obtain message $m < n$.
3. Pick blinding factor $b \in \mathbb{Z}_n$
4. Transmit $m' := mb^e \mod n$.

(4) Unblinding

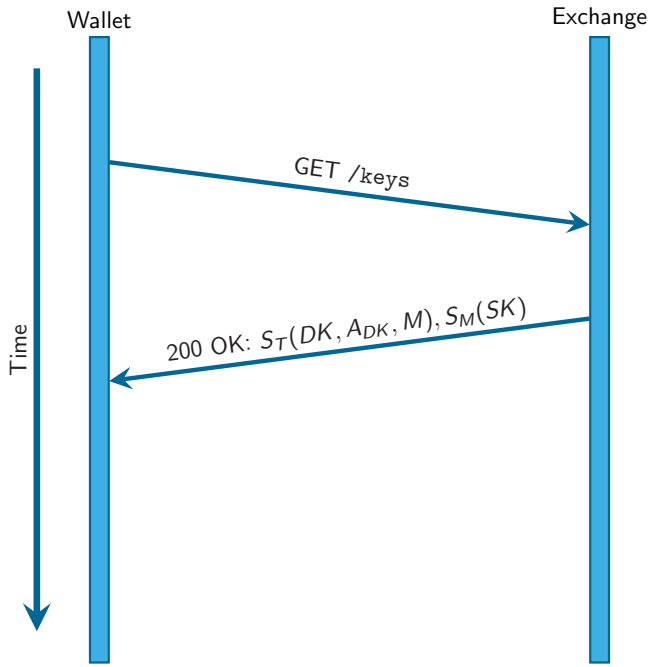
1. Receive s'.
2. Compute $s := s'b^{-1} \mod n$.

(5) Verification

1. Check $s^e \equiv m \mod n$.

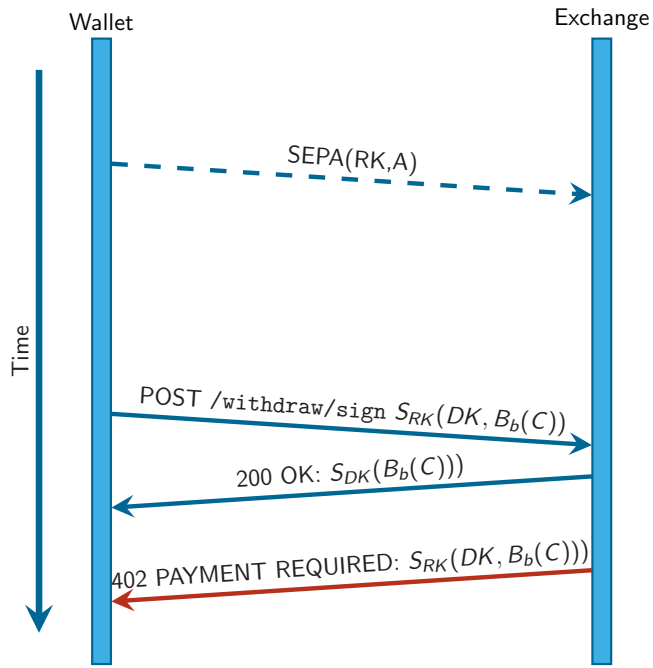
Taler /keys

Money is signed by a bank. What is the PKI?



T	financial regulator key Necessarily pinned
DK	RSA public key ("denomination key")
A_{DK}	Value of coins signed by DK
M	Offline master key of exchange
SK	Online signing key of exchange

Taler `/withdraw/sign`

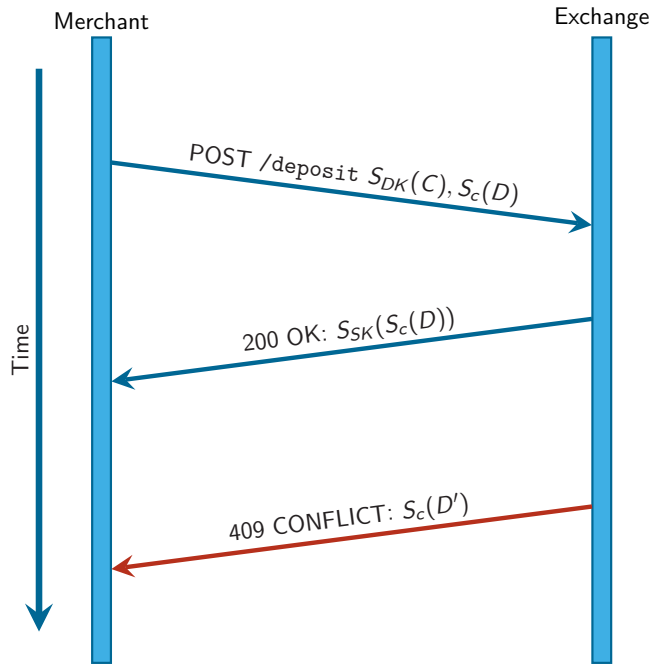


Result: $\langle c, S_{DK}(C) \rangle$.

A	Some amount, $A \geq A_{DK}$
RK	Reserve key
DK	Denomination key
b	Blinding factor
$B_b()$	RSA-FDH blinding
C	Coin public key $C := cG$
$S_{RK}()$	EdDSA signature
$S_{DK}()$	RSA-FDH signature

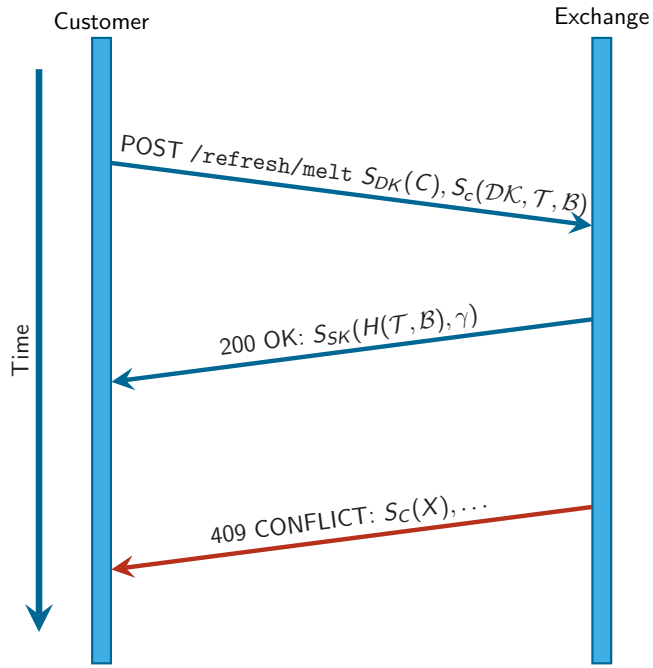
Taler /deposit

Merchant and exchange see only the public coin $\langle C, S_{DK}(C) \rangle$.



DK	Denomination key
$S_{DK}()$	RSA-FDH signature using DK
c	Private coin key, $C := cG$.
$S_C()$	EdDSA signature using c
D	Deposit details
SK	Exchange's signing key
$S_{SK}()$	EdDSA signature using SK
D'	Conficting deposit details $D' \neq D$

Taler /refresh/melt



κ System-wide security parameter, usually 3.

$\mathcal{DK}$ $:= [DK^{(i)}]_i$
List of denomination keys
$D + \sum_i A_{DK^{(i)}} < A_{DK}$

t_j Random scalar for $j < \kappa$

$\mathcal{T}$ $:= [T_j]_\kappa$ where $T_j = t_j G$

k_j $:= cT_j = t_j C$ is an ECDHE

$b_j^{(i)}$ $:= \mathtt{KDFb}(k_j, i)$

$c_j^{(i)}$ $:= \mathtt{KDFc}(k_j, i)$

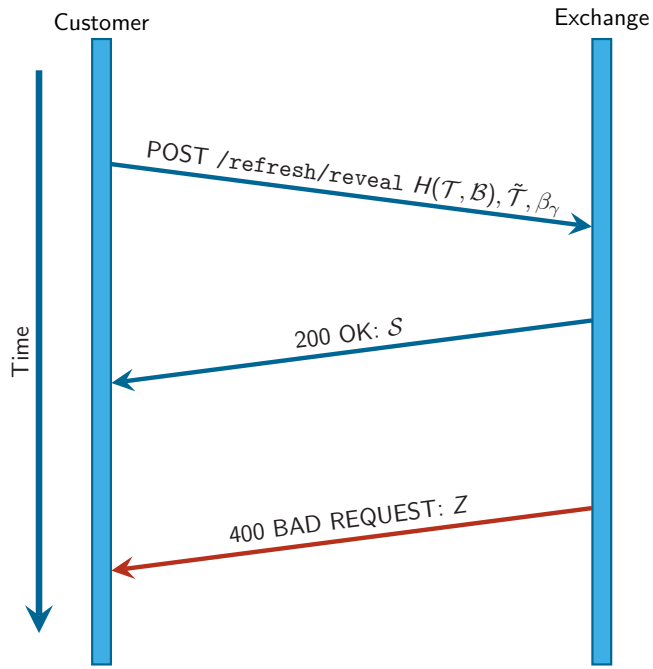
$C_j^{(i)}$ $:= c_j^{(i)} G$

$\mathcal{B}$ $:= [H(\beta_j)]_\kappa$ where

$$\beta_j := \left[B_{b_j^{(i)}}(C_j^{(i)}) \right]_i$$

γ Random value in $[0, \kappa)$

Taler /refresh/reveal



$$\mathcal{DK} := [DK^{(i)}]_i$$

$$t_j \quad ..$$

$$\tilde{\mathcal{T}} := [t_j | j \in \kappa, j \neq \gamma]$$

$$k_\gamma := cT_\gamma = t_\gamma C$$

$$b_\gamma^{(i)} := \texttt{KDFb}(k_\gamma, i)$$

$$c_\gamma^{(i)} := \texttt{KDFc}(k_\gamma, i)$$

$$C_\gamma^{(i)} := c_\gamma^{(i)} G$$

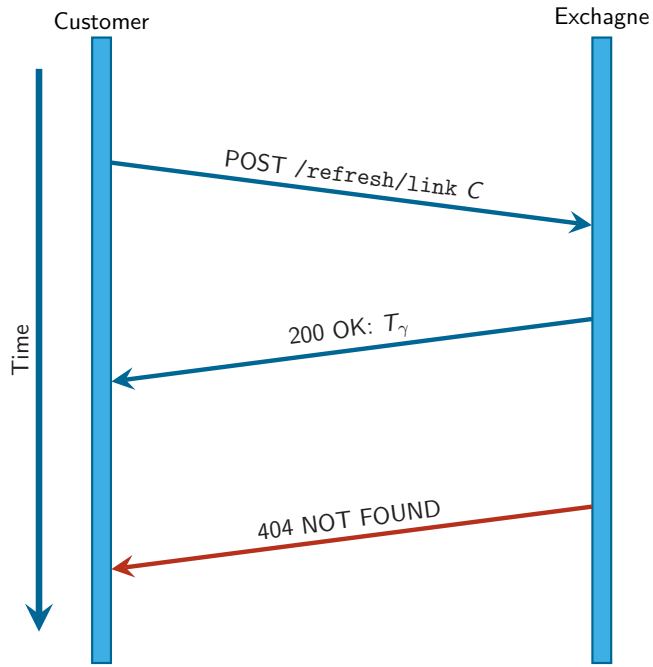
$$B_\gamma^{(i)} := B_{b_\gamma^{(i)}}(C_\gamma^{(i)})$$

$$\beta_\gamma := \left[B_\gamma^{(i)}\right]_i$$

$$\mathcal{S} := \left[S_{DK^{(i)}}(B_\gamma^{(i)})\right]_i$$

Z Cut-and-choose missmatch information

Taler /refresh/link



C Old coind public key

T_γ Linkage data $\mathcal{L}$ at γ

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/...