

The Bank's Problem

- ▶ Global tech companies push oligopolies
- ▶ Privacy and federated finance are at risk
- ▶ Economic sovereignty is in danger



Predicting the Future

- ▶ Google, Apple or Facebook's Libra will be your bank and run your payment system
- ▶ They target advertising based on your purchase history, location and your ability to pay
- ▶ They will provide more usable, faster and broadly available payment solutions; our federated banking system will be history
- ▶ After dominating the payment sector, they will start to charge fees befitting their oligopoly size
- ▶ Competitors and vendors not aligning with their corporate "values" will be excluded by terms of service and go bankrupt

GNU

<Taler>

Digital cash, made **socially**
responsible.

taler.net
twitter@taler
mail@taler.net

Christian Grothoff
grothoff@taler.net



Berner Fachhochschule
Technik und Informatik

What is Taler?

Taler is an electronic instant payment system.

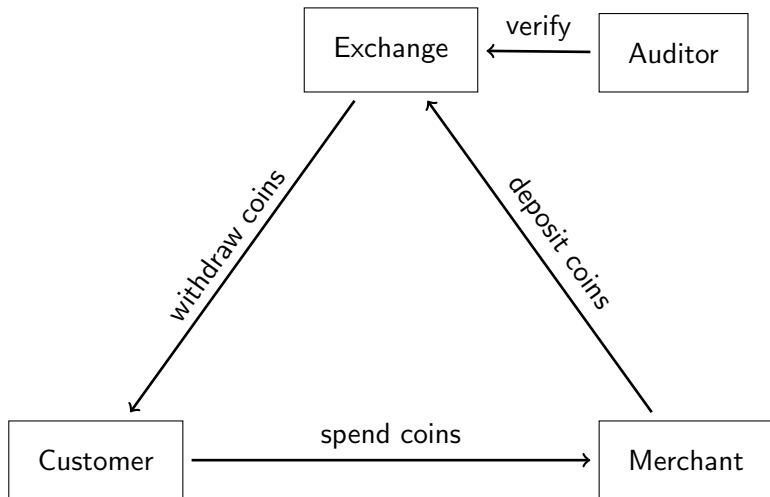
- ▶ Uses electronic coins stored in **wallets** on customer's device
- ▶ Like **cash**
- ▶ Pay in **existing currencies** (i.e. EUR, USD, CHF)

Design goals for the GNU Taler Payment System

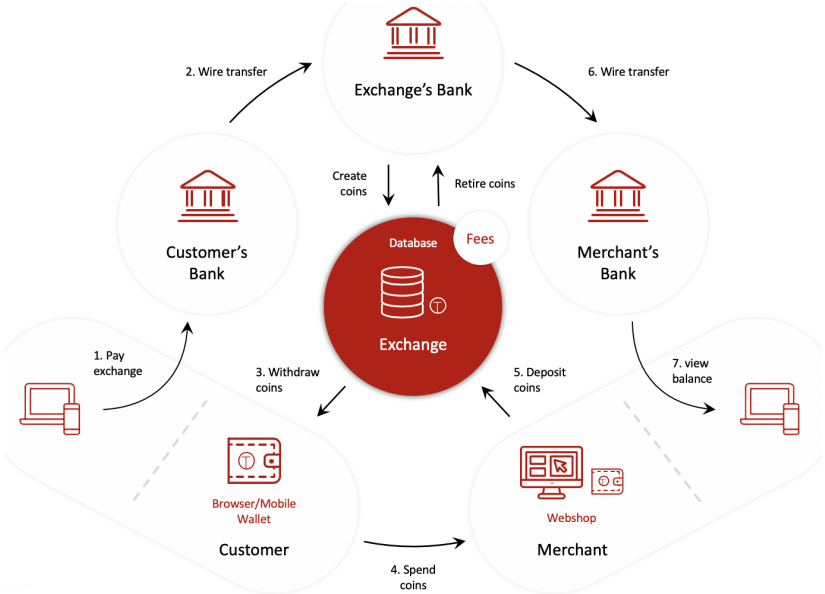
GNU Taler must ...

1. ... be implemented as **free software**.
2. ... protect the **privacy of buyers**.
3. ... must enable the state to **tax income** and crack down on illegal business activities.
4. ... prevent payment fraud.
5. ... only **disclose the minimal amount of information necessary**.
6. ... be usable.
7. ... be efficient.
8. ... avoid single points of failure.
9. ... foster **competition**.

Taler Overview



Taler in Operation



Usability of Taler

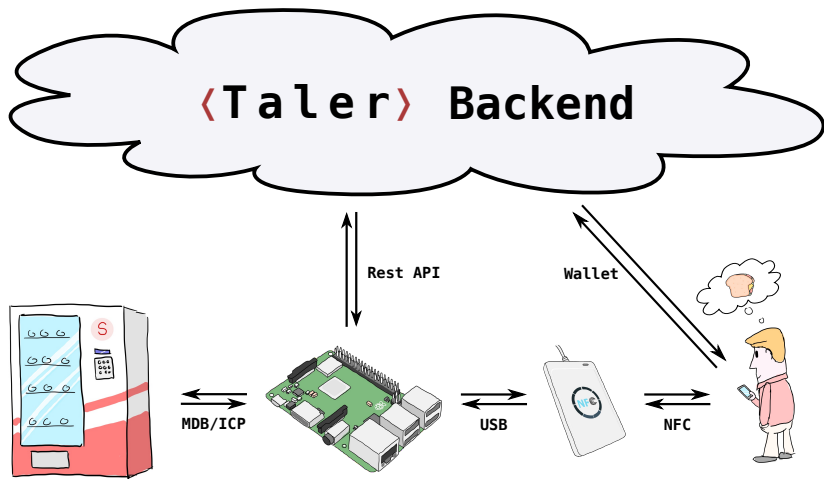
`https://demo.taler.net/`

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

The Taler Snack Machine¹

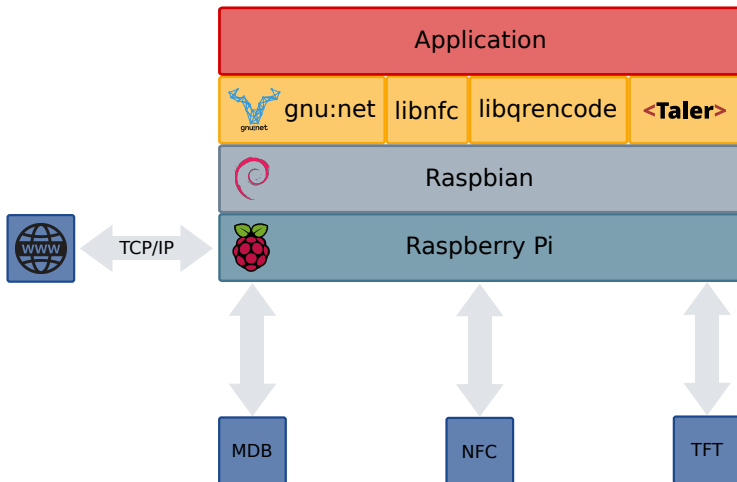
Integration of a MDB/ICP to Taler gateway.

Implementation of a NFC or QR-Code to Taler wallet interface.

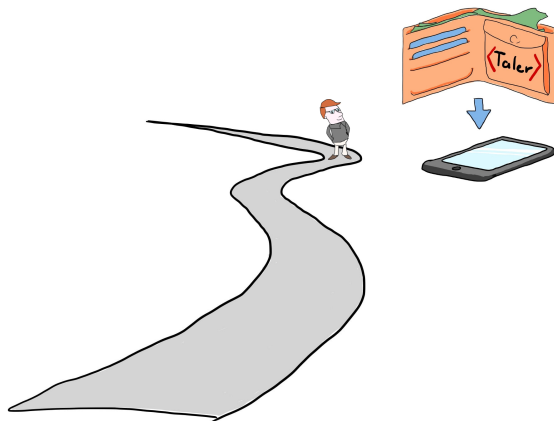


¹By M. Boss and D. Hofer

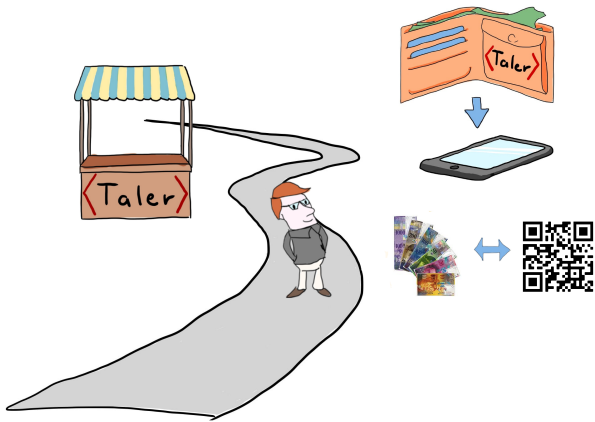
Software



How to use at WCEF: Install App on Android²



How to use at WCEF: Exchange cash for e-cash



How to use at WCEF: Buy autographed copy of GRM!



How to use afterwards: Shop online³

<https://buywith.taler.net/>

³Operational until 31.1.2020



Berner Fachhochschule
Technik und Informatik

Use Case: Journalism

Today:

- ▶ Corporate structure
- ▶ Advertising primary revenue
- ▶ Tracking readers critical for business success
- ▶ Journalism and marketing hard to distinguish

Use Case: Journalism

Today:

- ▶ Corporate structure
- ▶ Advertising primary revenue
- ▶ Tracking readers critical for business success
- ▶ Journalism and marketing hard to distinguish

With GNU Taler:

- ▶ One-click micropayments per article
- ▶ Hosting requires no expertise
- ▶ Reader-funded reporting separated from marketing
- ▶ Readers can remain anonymous

Use Case: Anti-Spam

Today, PGP provides authenticated encryption for e-mail:

- ▶ Free software
- ▶ Easy to use opportunistic encryption
- ▶ Available for Outlook, Android, Enigmail
- ▶ Spies & spam filters can no longer inspect content

Use Case: Anti-Spam

Today, p≡p provides authenticated encryption for e-mail:

- ▶ Free software
- ▶ Easy to use opportunistic encryption
- ▶ Available for Outlook, Android, Enigmail
- ▶ Spies & spam filters can no longer inspect content

With GNU Taler:

- ▶ Peer-to-peer payments via e-mail
- ▶ If unsolicited sender, hide messages from user & automatically request payment from sender
- ▶ Sender can attach payment to be moved to inbox
- ▶ Receiver may grant refund to sender

Where might this get us exactly?

Visions

- ▶ Be paid to read advertising, starting with spam
- ▶ Give welfare without intermediaries taking huge cuts
- ▶ Eliminate corruption by making all income visible
- ▶ Stop the mining by making crypto-currencies useless for anything but crime

Competitor comparison

	Cash	Bitcoin	Zerocoin	Creditcard	GNU Taler
Online	---	++	++	+	+++
Offline	+++	--	--	+	--
Trans. cost	+	----	----	-	++
Speed	+	----	----	o	++
Taxation	-	--	----	+++	+++
Payer-anon	++	o	++	----	+++
Payee-anon	++	o	++	----	----
Security	-	o	o	--	++
Conversion	+++	----	----	+++	+++
Libre	-	+++	+++	---	+++

Technology

How does it work?

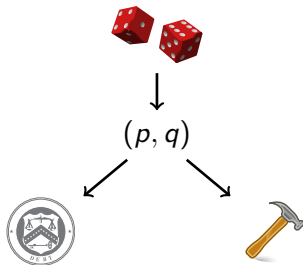
We use a few ancient constructions:

- ▶ Cryptographic hash function (1989)
- ▶ Blind signature (1983)
- ▶ Schnorr signature (1989)
- ▶ Diffie-Hellman key exchange (1976)
- ▶ Cut-and-choose zero-knowledge proof (1985)

But of course we use modern instantiations.

Exchange setup: Create a denomination key (RSA)

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



Merchant: Create a signing key (EdDSA)

- ▶ pick random $m \pmod{o}$ as private key
- ▶ $M = mG$ public key



↓
 m

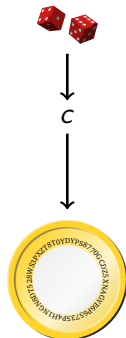
↓
 M

Capability: $m \Rightarrow$



Customer: Create a planchet (EdDSA)

- ▶ Pick random $c \pmod{o}$ private key
- ▶ $C = cG$ public key

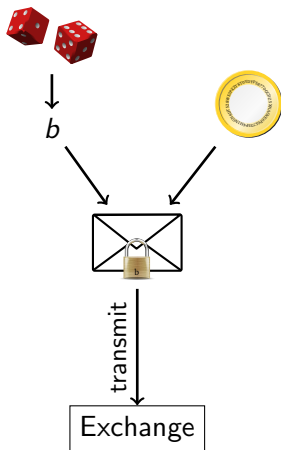


Capability: $c \Rightarrow$



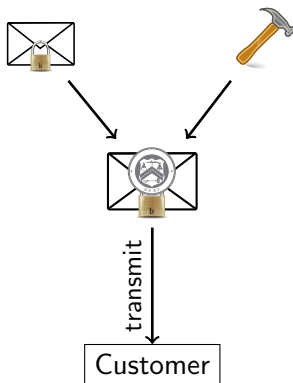
Customer: Blind planchet (RSA)

1. Obtain public key (e, n)
2. Compute $f := FDH(C)$, $f < n$.
3. Pick blinding factor $b \in \mathbb{Z}_n$
4. Transmit $f' := fb^e \pmod n$



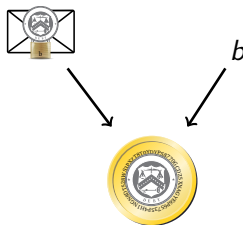
Exchange: Blind sign (RSA)

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

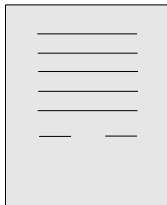


Customer: Unblind coin (RSA)

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



Customer: Build shopping cart

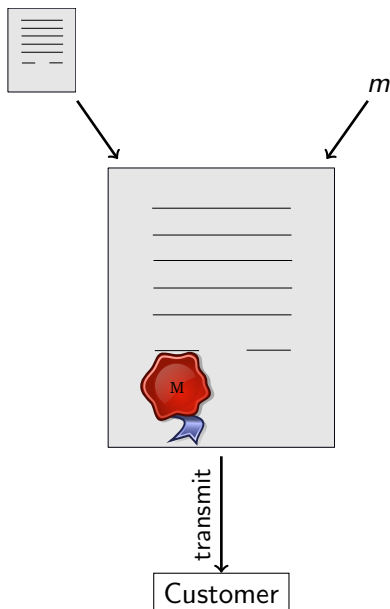


transmit



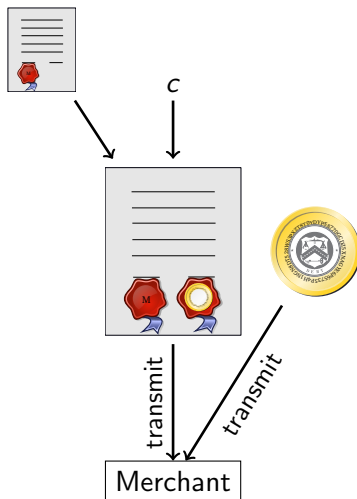
Merchant: Propose contract (EdDSA)

1. Complete proposal D .
2. Send D , $EdDSA_m(D)$



Customer: Spend coin (EdDSA)

1. Receive proposal D ,
 $EdDSA_m(D)$.
2. Send s , C , $EdDSA_c(D)$



Merchant and Exchange: Verify coin (RSA)

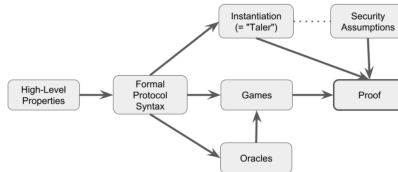
$$s^e \stackrel{?}{\equiv} FDH(C) \pmod{n}$$



Technology

GNU Taler additionally offers:

- ▶ Giving change, can provide refunds
- ▶ Integration with HTTP, handles network failures
- ▶ High performance
- ▶ Bounded losses on key compromise
- ▶ Formal security proofs
- ▶ ...



More information at <https://taler.net/>.

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, and
- ▶ Enjoy the “benefits” of cash



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**.

The Distraction: Bitcoin

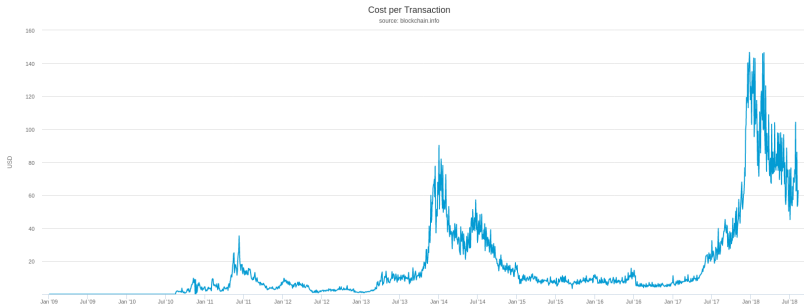
- ▶ Unregulated payment system and currency:
⇒ lack of regulation is a feature!
- ▶ Implemented in free software
- ▶ Decentralised peer-to-peer system

The Distraction: Bitcoin

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

The Distraction: Bitcoin

- ▶ Unregulated payment system and currency:
 - ⇒ lack of regulation is a feature!
- ▶ Implemented in free software
- ▶ Decentralised peer-to-peer system
- ▶ Decentralised banking requires solving Byzantine consensus
- ▶ Creative solution: tie initial accumulation to solving consensus
 - ⇒ Proof-of-work advances ledger
 - ⇒ Very expensive banking



Current average transaction value: \approx 1000 USD

What is there?



Components

- ▶ REST APIs, C APIs
- ▶ Command-line, WebExtension (Firefox, Chrome, Chromium, Brave) and Android wallet
- ▶ GLS bank integration (libeufin, WiP)
- ▶ Escrow/backup solution (Anastasis, WiP)
- ▶ Merchant backend & backoffice (needs improvements)
- ▶ WooCommerce plugin (needs update)
- ▶ Taler-enabled vending machine (MDB)
- ▶ Sample Web frontends