

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

Christian Grothoff

Inria Rennes Bretagne Atlantique

25.4.2016

“Capitalism is using its money; we socialists throw it away.” –Fidel Castro

Where We Are



Where We Are



الموقع محظور

أسف! إن الموقع الذي أردت تصفحه قد أُحجب وذلك بسبب إحتواءه على نشاط مخالف للقيم الاجتماعية أو السياسية أو الثقافية أو الدينية لدرجة الأضرار الفورية المتوقعة.

في حالة أردت فتح الموقع قد أُحجب الرجاء قم بتصفحة إستشارة الملاحظات الموضوعة على موقعنا.

We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political and moral values of the United Arab Emirates.

If you think this site should not be blocked, please visit the [Feedback Form](#) available on our website.

SITE BLOCKED

Source: wikileaks.org



A Matter of Life and Death



The Intercept reports in February 2014:

- ▶ NSA identifies targets based on meta data (social graph, location profiles, cell-phone tracking)
- ▶ Content of calls and identity of individuals is often not even considered
- ▶ Joint Special Operations Command (JSOC) uses geolocation of SIM card for assassinations using drone strikes
- ▶ Individual in possession of SIM card is sometimes not even identified prior to strike

“F3: Find, Fix, Finish” is state terrorism facilitated by networks.

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 GNUet

Internet

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

GNUet

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

Use Cases

- ▶ Internet e-commerce (convenient, efficient)

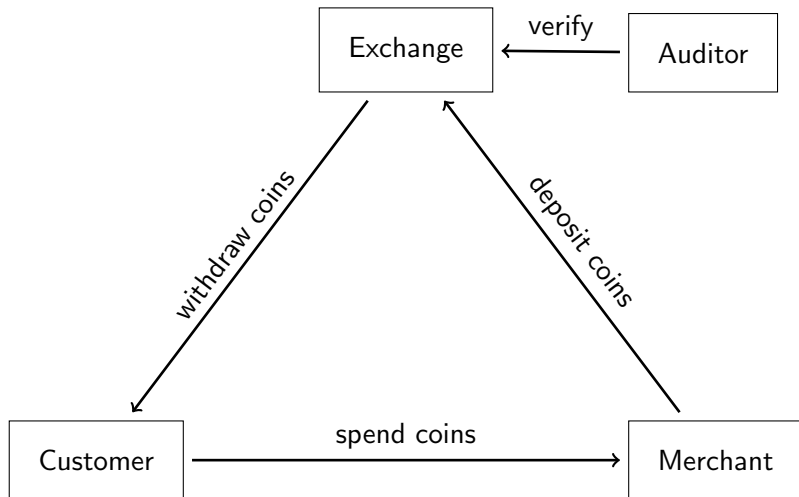
Use Cases

- ▶ 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)

Architecture of GNU Taler



Background: 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
 $d := e^{-1} \pmod{\phi(n)}$ exists.
4. Publish public key (e, n) .

(3) Blind signing

1. Receive m' .
2. Compute $s' := m'^d \pmod{n}$.
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 $m' := mb^e \pmod{n}$.

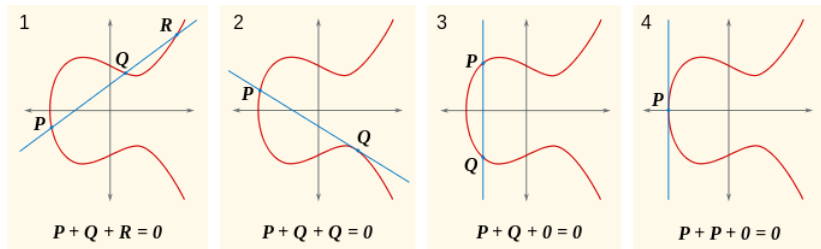
(4) Unblinding

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

(5) Verification

1. Check $s \equiv m^d \pmod{n}$.

Background: Elliptic Curve Cryptography



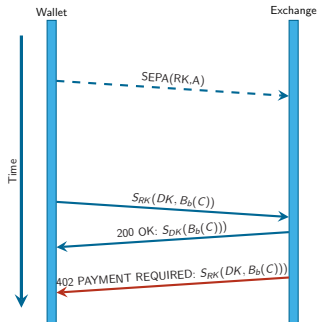
(1) Key generation

1. Pick secret random number $r \bmod n$.
2. Compute $R = rG$. Given R , computing r is “hard”.

(2) ECDH

1. Let $S = sG$, $T = tG$.
2. $sT = stG = tsG = tS$.

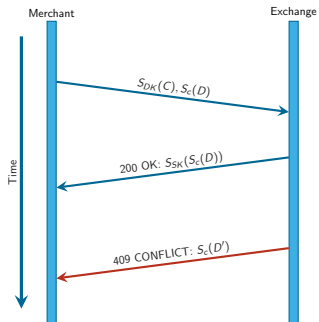
Withdrawing coins with blind signatures



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

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

Depositing coins



- DK Denomination key
- $S_{DK}()$ RSA 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' Conflicting deposit details
 $D' \neq D$

Taxability

We say Taler is taxable because:

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

Limitations:

- ▶ withdraw loophole
- ▶ copying coins among family and friends

Giving change

It would be inefficient to pay CUC 100 with 1 CUP coins!

- ▶ DK 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 CUC 100 with 1 CUP coins!

- ▶ DK 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 CUC 100 with 1 CUP coins!

- ▶ DK 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.

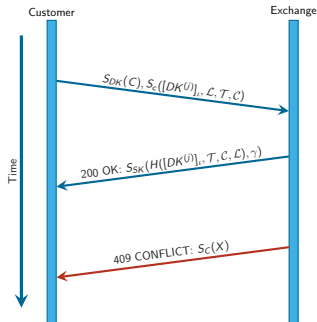
Key goals:

- ▶ maintain unlinkability
- ▶ maintain taxability of transactions

Method:

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

Taler /refresh/melt



κ security parameter
($i \in [1, \kappa]$)

l number of fresh coins being issued ($j \in [1, l]$)

$K(T, C)$ Key from $tcG \equiv cT \equiv tC$

$E_K()$ Symmetric encryption

$DK^{(j)}$ List of denomination keys

$c^{(i,j)}$ List of coin keys,
 $C^{(i,j)} := c^{(i,j)} G.$

$b^{(i,j)}$ List of blinding factors

$B_{b^{(i,j)}}()$ Blinding with $b^{(i,j)}$

T Transfer keys $[T]_{\kappa}$ where
 $T^{(i)} := t^{(i)} G.$

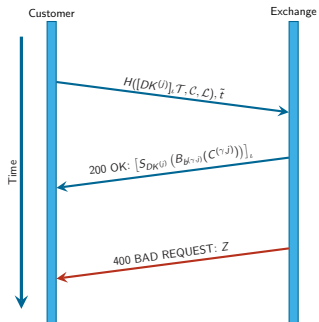
L Linkage information,

$$\left[E_{K(T^{(i)}, C)}([b^{(i,j)}, c^{(i,j)}]_l) \right]_{\kappa}$$

C Commitment:
 $\left[B_{b^{(i,j)}}(C^{(i,j)}), DK^{(i,j)} \right]_l \Big]_{\kappa}$

γ Random value in $[0, \kappa)$

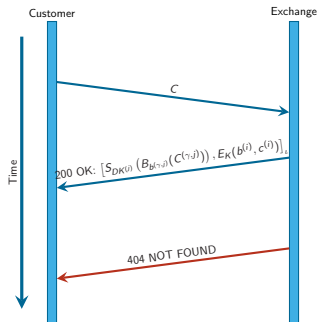
Taler /refresh/reveal



\tilde{t} $[t]_{\kappa \setminus \gamma}$

Z Cut-and-choose mismatch information

Taler /refresh/link



Crypto summary

The cut-and-choose refresh protocol allows:

- ▶ To give unlinkable change.
- ▶ To give refunds to the anonymous customer.
- ▶ 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.

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!

Building the GNUet

Internet

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

GNUet

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

$$1+1=2$$

- ▶ NSA “kills based on meta data” –Michael Hayden (former NSA director)
- ▶ DNS makes it trivial to gather meta data about most Internet activities

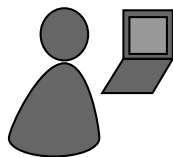
“The Domain Name System is the Achilles heel of the Web.” –Tim Berners-Lee

The GNU Name System (GNS)

Properties of GNS

- ▶ Decentralized name system with secure memorable names
- ▶ Provides alternative public key infrastructure
- ▶ Interoperable with DNS
- ▶ Achieves query and response privacy


Name resolution in GNS



Bob



Bob's webserver

Local Zone: K_{pub}^{Bob}		
www	A	5.6.7.8
		

- ▶ Bob can locally reach his webserver via **www.gnu**

Secure introduction



TUM

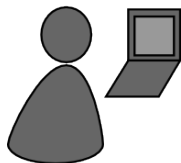


Bob Builder, Ph.D.

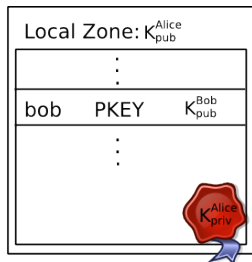
Address: Country, Street Name 23
Phone: 555-12345
Mobile: 666-54321
Mail: bob@H2R84L4JIL3G5C.zkey

- ▶ Bob gives his public key to his **friends**, possibly via QR code

Delegation



Alice



- ▶ Alice learns Bob's public key
- ▶ Alice creates delegation to zone K_{pub}^{Bob} under label **bob**
- ▶ Alice can reach Bob's webserver via **www.bob.gnu**

Building the GNUet

Internet

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

GNUet

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

The importance of Freifunk

Using TCP/IP is problematic:

- ▶ High-end hardware only from US or China
- ▶ Massive spy presence, mass surveillance
- ▶ Access controlled by large corporations and governments
- ▶ Why use Twitter/Facebook/Google as intermediaries?

(W)LAN ad-hoc routing enables local community networks.

Building the GNUet

Internet

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

GNUet

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

SecuShare

- ▶ Fully decentralised social networking platform
- ▶ No administrators, no servers, no surveillance
- ▶ Self-organized, self-healing, self-aware
- ▶ Extensible end-to-end encrypted messaging protocol
- ▶ Well-defined C interfaces for developers to extend
- ▶ GUI not yet ready :-(.

How to help?

- ▶ Think about how computer security may affect causes you care about
- ▶ Translate documentation and user interfaces
- ▶ Deploy WLAN Ad Hoc Networks (“Freifunk”) and make them useful

How to help?

- ▶ Think about how computer security may affect causes you care about
- ▶ Translate documentation and user interfaces
- ▶ Deploy WLAN Ad Hoc Networks (“Freifunk”) and make them useful
- ▶ If you can program:
 - ▶ Write free software with clear licensing terms attached
 - ▶ Turn Taler demonstrator bank into community bank application
 - ▶ Consider using the GNU Name System for naming in network apps
 - ▶ Use GUNet SOCIAL API to write OSN application for your organization
 - ▶ 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
 - ▶ Deploy privacy-preserving decentralized GNU Name System as PKI
 - ▶ Build decentralised, privacy-preserving censorship-resistant OSNs
- ▶ Use free software, ensure computers serve their owners
- ▶ Organize to solve social problems
- ▶ Plan C: Learn to swim



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. Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th International Conference on Cryptology and Network Security**, 2014.
3. Nathan Evans and Christian Grothoff. *R⁵N. Randomized Recursive Routing for Restricted-Route Networks*. **5th International Conference on Network and System Security**, 2011.
4. Florian Dold, Sree Harsha Totakura, Benedikt Müller and Christian Grothoff. *Taler: Taxable Anonymous Libre Electronic Reserves*. Available upon request. 2015.
5. Yves Eudes, Christian Grothoff, Jacob Appelbaum, Monika Ermert, Laura Poitras and Matthias Wachs. *MoreCowBells: Nouvelles révélations sur les pratiques de la NSA*. **Le Monde**, 24.1.2015.
6. Yves Eudes, Christian Grothoff. *Comment fonctionne Skynet, le programme ultra-secret de la NSA créé pour tuer*. **Le Monde**, 20.10.2015.
7. Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt**, 2015.

Let money facilitate trade; but ensure capital serves society.