

Electronic Payment Systems and European Values

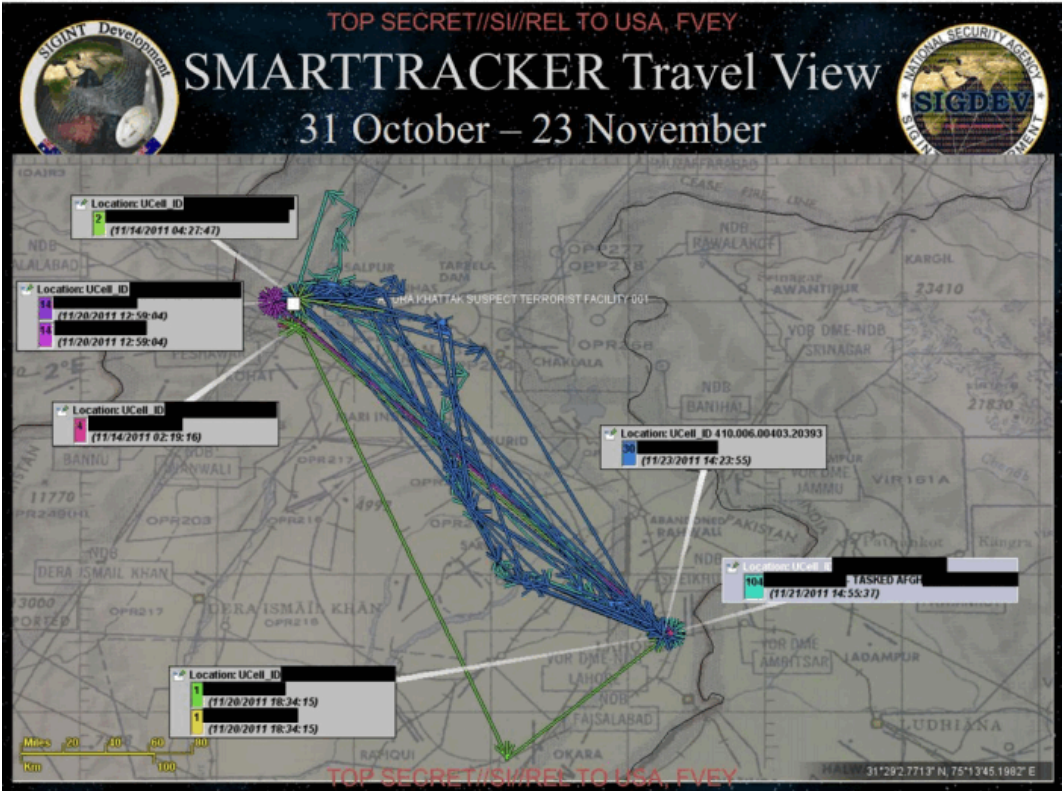
Christian Grothoff



19.8.2019

"Action is indeed the sole medium of expression for ethics." –Jane Addams

Mass-Surveillance can create Mass-Casualties



What domain of digital communication should we be most concerned about?

Surveillance concerns

Everybody knows about Internet surveillance.
But is it **that** bad?

Surveillance concerns

Everybody knows about Internet surveillance.

But is it **that** bad?

- ▶ You can choose when and where to use the Internet
- ▶ You can anonymously access the Web using Tor
- ▶ You can find open access points that do not require authentication
- ▶ IP packets do not include your precise location or name
- ▶ ISPs typically store this meta data for days, weeks or months

Where is it worse?

Where is it worse?



SWIFT/Mastercard/Visa are way more invasive.

What is worse:

- ▶ When you pay by CC, the information includes your name
- ▶ When you pay in person with CC, your location is also known
- ▶ You often have no alternative payment methods available
- ▶ You hardly ever can use someone else's CC
- ▶ Anonymous prepaid cards are difficult to get and expensive
- ▶ Payment information is typically stored for at least 6 years



TOP SECRET//SI//REL TO USA, FVEY

Private Networks are Important



q Many targets use private networks.

Google infrastructure	SWIFT Network
French MFA	Petrobras

q Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.



TOP SECRET//SI//REL TO USA, FVEY

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
- ▶ The imperium will have another major tool for its financial warfare

Which human rights concerns would a solution need to address?

Discuss:

1. Credit cards & W3c Payment Interest Group?
2. BitCoin?
3. Zcash?
4. *-Pay?

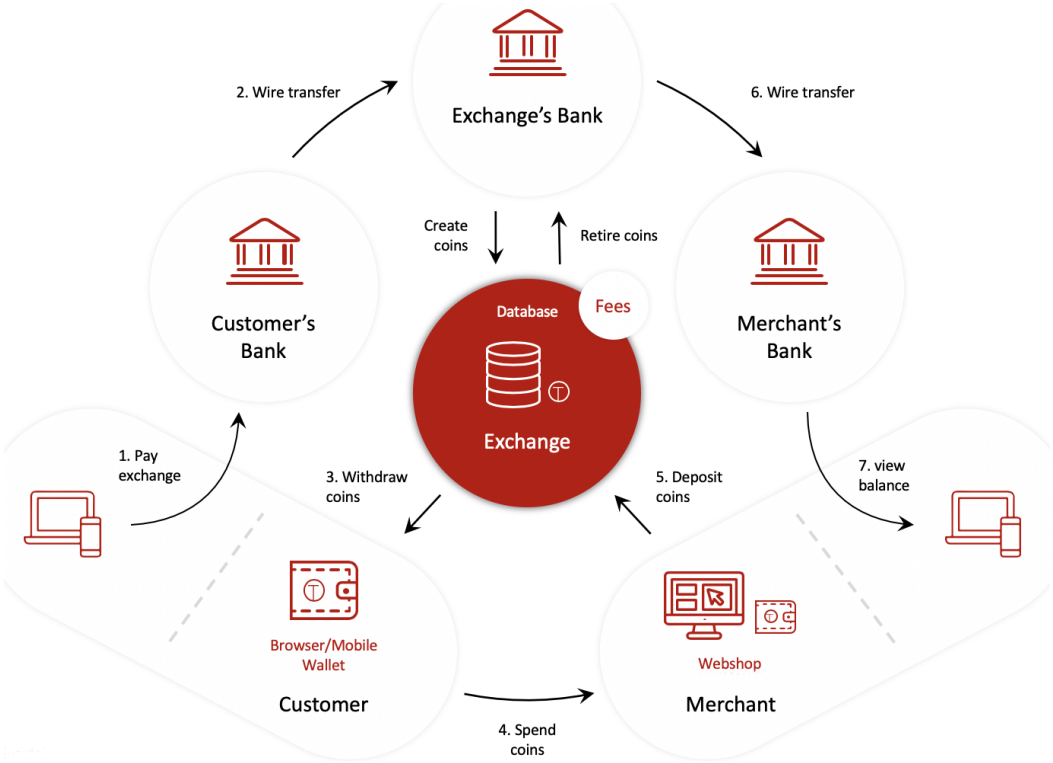
Design goals for the GNU Taler Payment System

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 in Operation

Taler in Operation



What kind of diversity is desirable?

- ▶ GNU Taler promotes **one** payment protocol

Diversity

- ▶ GNU Taler promotes **one** payment protocol
- ▶ There **may** be multiple implementations

Diversity

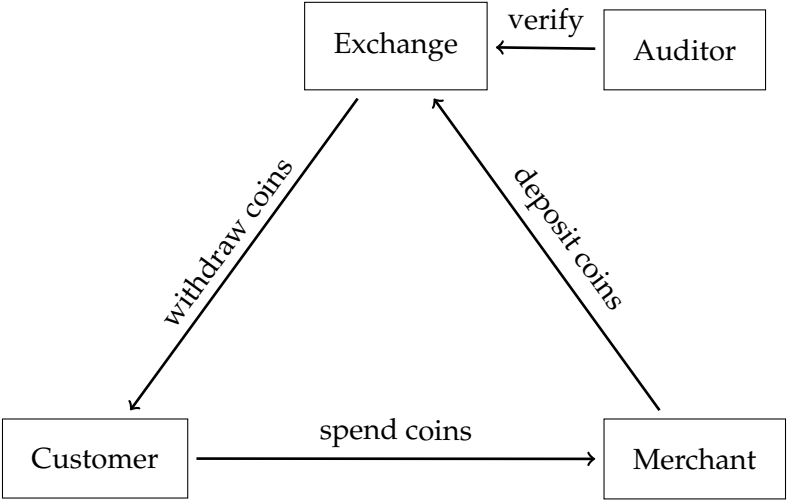
- ▶ GNU Taler promotes **one** payment protocol
- ▶ There **may** be multiple implementations
- ▶ Diversity of **commercial operators** is crucial

What are the requirements to get there?

No more sheep!



Transformation Domains



Where might this get us exactly?

Visions

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

How can you help?

Support Domains

- ▶ Testing: try it out, report issues (<https://bugs.gnunet.org/>)
- ▶ Propaganda: spread the word
- ▶ Documentation: explain things better
- ▶ Translation: translate Web site and software
- ▶ Design: make nice graphics for illustration, design UI/UX
- ▶ Programming: Integrate GNU Taler where it makes sense!
- ▶ Security audits: study our code and design
- ▶ Funding: GNUnet e.V. takes donations, Taler Systems seeks investments (100k+)

Do you have any questions?

- ▶ <https://taler.net/>
- ▶ Slides will be published at <https://grothoff.org/christian/>.
- ▶ Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. *Enabling Secure Web Payments with GNU Taler*. **SPACE 2016**.
- ▶ David Chaum, Amos Fiat and Moni Naor. *Untraceable electronic cash*. **Proceedings on Advances in Cryptology, 1990**.
- ▶ Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt, 2015**.
- ▶ Florian Dold. *The GNU Taler System: Practical and Provably Secure Electronic Payments*. **PhD thesis. University of Rennes 1, 2019**.