GNU Taler

Christian Grothoff

Berner Fachhochschule
The GNU Project
Taler Systems SA

21.6.2022

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?"*

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?"*

"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)

Surveilance concerns

On the Internet:

- IP packets do not include your name
- You can anonymously access the Web using Tor or find open access points without authentication
- ISPs typically store this meta data for days, weeks or months

Surveilance concerns

On the Internet:

- IP packets do not include your name
- You can anonymously access the Web using Tor or find open access points without authentication
- ISPs typically store this meta data for days, weeks or months

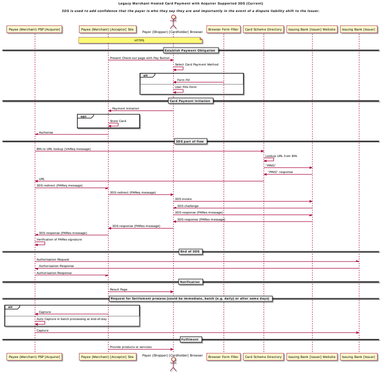
With CC payments:

- The information includes your name
- Anonymous prepaid cards are difficult to get and you rarely can use someone else's CC
- Payment information is typically stored for at least 6 years

Banks have Problems, too!

3D secure ("verified by visa") is a nightmare:

- Complicated process
- Shifts liability to consumer
- Significant latency
- Can refuse valid requests
- Legal vendors excluded
- No privacy for buyers


Legacy Merchant Hosted Card Payment with Acquirer Supported 3DS (Current)
3DS is used to add confidence that the payer is who they say they are and importantly in the event of a dispute liability shift to the Issuer.
Payee (Merchant) PSP [Acquirer]
Payee (Merchant) [Acceptor] Site
Payer (Shopper) [Cardholder] Browser
Browser Form Filler
Card Scheme Directory
Issuing Bank [Issuer] Website
Issuing Bank [Issuer]
HTTPS
Establish Payment Obligation
Present Check-out page with Pay Button
Select Card Payment Method
alt
Form Fill
User Fills Form
Card Payment Initiation
Payment Initiation
opt
Store Card
Authorise
3DS part of flow
BIN to URL lookup (VAReq message)
Lookup URL from BIN
"PING"
"PING" response
URL
3DS redirect (PAReq message)
3DS redirect (PAReq message)
3DS invoke
3DS challenge
3DS response (PARes message)
3DS response (PARes message)
3DS response (PARes message)
3DS response (PARes message)
Verification of PARes signature
End of 3DS
Authorisation Request
Authorisation Response
Authorisation Response
Notification
Result Page
Request for Settlement process (could be immediate, batch (e.g. daily) or after some days)
alt
Capture
Auto Capture in batch processing at end-of-day
Capture
Fulfilment
Provide products or services
Payee (Merchant) PSP [Acquirer]
Payee (Merchant) [Acceptor] Site
Payer (Shopper) [Cardholder] Browser
Browser Form Filler
Card Scheme Directory
Issuing Bank [Issuer] Website
Issuing Bank [Issuer]

Online credit card payments will be replaced, but with what?

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 and Apple will be your bank and run your payment system
- They can 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 they dominate 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 policy and go bankrupt
- The imperium will have another major tool for its financial warfare

Plan B: Pay with cash

Cash is:

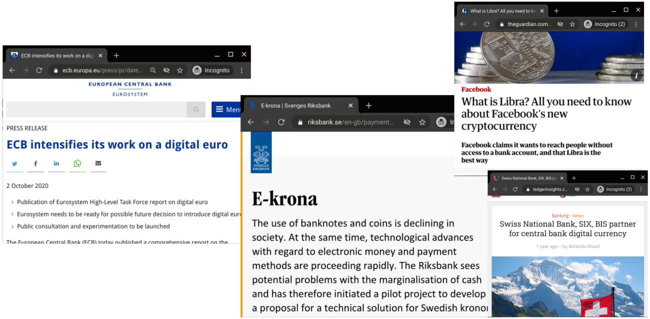
- Privacy-friendly
- Offline-capable
- Inexpensive
- Broadly accessible
- Central bank liability

Central Bank Digital Currency (CBDC)

Over 80 central banks have started initiatives to introduce a CBDC:

- ECB: Report on a Digital Euro / Eurosystem report on the public consultation on a Digital Euro
- Bank of England: Just initiated a task force

China is leading with the most widely deployed solution today.


ECB intensifies its work on a digi
ecb.europa.eu/press/pr/date...
Incognito
EUROPEAN CENTRAL BANK
EUROSYSTEM
Menu
E-krona | Sveriges Riksbank
riksbank.se/en-gb/payment...
SVERIGES RIKSBANK
What is Libra? All you need to kn
theguardian.com...
Incognito (2)
Swiss National Bank, SIX, BIS pa
ledgerinsights.c...
Incognito (2)

PRESS RELEASE

ECB intensifies its work on a digital euro

2 October 2020

- Publication of Eurosystem High-Level Task Force report on digital euro
- Eurosystem needs to be ready for possible future decision to introduce digital eur
- Public consultation and experimentation to be launched

The European Central Bank (ECB) today published a comprehensive report on the

E-krona

The use of banknotes and coins is declining in society. At the same time, technological advances with regard to electronic money and payment methods are proceeding rapidly. The Riksbank sees potential problems with the marginalisation of cash and has therefore initiated a pilot project to develop a proposal for a technical solution for Swedish kronor

Facebook

What is Libra? All you need to know about Facebook's new cryptocurrency

Facebook claims it wants to reach people without access to a bank account, and that Libra is the best way

Banking · News

Swiss National Bank, SIX, BIS partner for central bank digital currency

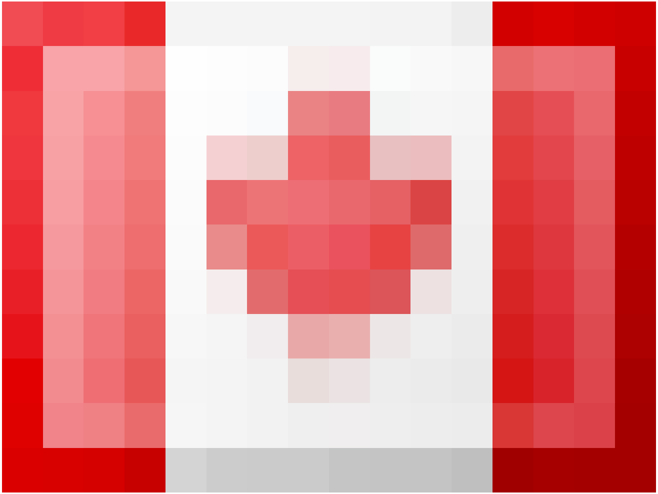
1 year ago · by Miranda Wood

So what are their plans?

The Bank of International Settlements

But CFT is good! No more financial crime supporting terrorism!

The Emergency Act of Canada[1]



https://www.youtube.com/watch?v=NehMAj492SA (2'2022)

[1] Speech by Premier Kenney, Alberta, February 2022

Offline-capability is core objective for many CBDC projects.

This will mostly hurt cash availability.

Offline-capability is core objective for many CBDC projects.

This will mostly hurt cash availability.

Privacy is non-goal or not assured (see ECB&China).

$\Rightarrow$ **Most CBDC projects will hurt democracy, not help.**

GNU Taler

Digital cash, made **socially responsible**.

TALER

Privacy-Preserving, Practical, Taxable, Free Software, Efficient

What is Taler?

https://taler.net/en/features.html

Taler is

- a Free/Libre software *payment system* infrastructure project
- ... with a surrounding software ecosystem
- ... and a company (Taler Systems S.A.) and community that wants to deploy it as widely as possible.

However, Taler is

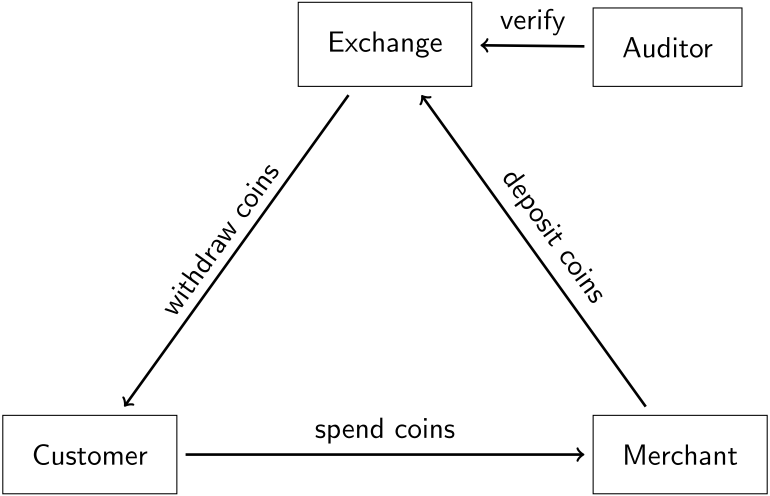
- *not* a currency
- *not* a long-term store of value
- *not* a network or instance of a system
- *not* decentralized
- *not* based on proof-of-work or proof-of-stake
- *not* a speculative asset / “get-rich-quick scheme”

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



Exchange

verify

Auditor

withdraw coins

deposit coins

spend coins

Customer

Merchant

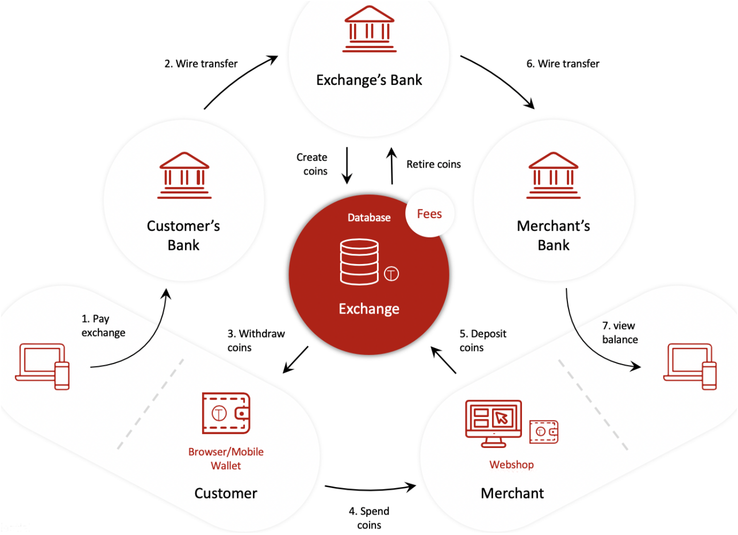
The Taler Software Ecosystem

https://taler.net/en/docs.html

Taler is based on modular components that work together to provide a complete payment system:

- **Exchange:** Service provider for digital cash
  - Core exchange software (cryptography, database)
  - Air-gapped key management, real-time **auditing**
  - **LibEuFin**: Modular integration with banking systems
- **Merchant:** Integration service for existing businesses
  - Core merchant backend software (cryptography, database)
  - Back-office interface for staff
  - Frontend integration (E-commerce, Point-of-sale)
- **Wallet:** Consumer-controlled applications for e-cash
  - Multi-platform wallet software (for browsers & mobile phones)
  - Wallet backup storage providers
  - **Anastasis**: Recovery of lost wallets based on secret splitting

Architecture of Taler



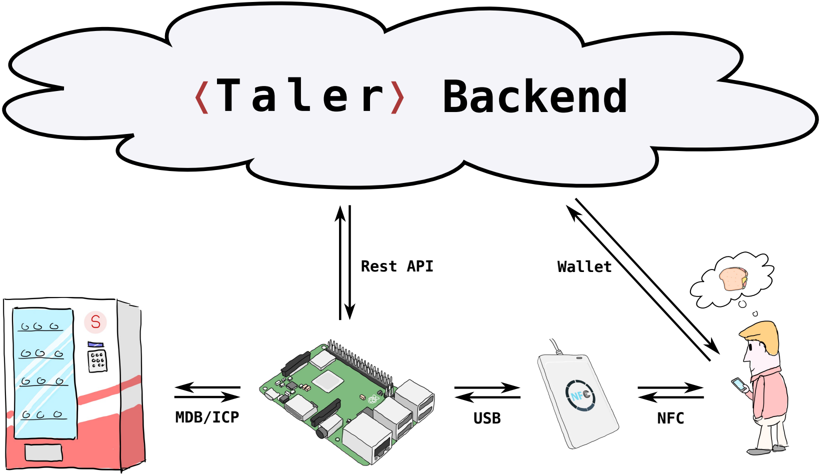
Usability of Taler

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

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

Example: The Taler Snack Machine[2]

Integration of a MDB/ICP to Taler gateway.
Implementation of a NFC or QR-Code to Taler wallet interface.



[2] By M. Boss and D. Hofer

Performance

Legacy Payment Systems

Bitcoin

4 TPS

Performance

Legacy Payment Systems

Bitcoin

4 TPS

Performance

Legacy Payment Systems

Bitcoin	PayPal
4 TPS	193 TPS

Performance

Legacy Payment Systems

Bitcoin	PayPal
4 TPS	193 TPS
📈 ⛏	🔒

Performance

Legacy Payment Systems

Bitcoin	PayPal	Visa
4 TPS	193 TPS	1’667 TPS

Performance

Legacy Payment Systems

Bitcoin	PayPal	Visa
4 TPS	193 TPS	1'667 TPS
📈 ⛏	🔒	🔒

Performance

CBDC Projects

e-Krona (Sweden)

100 TPS

Performance

CBDC Projects

e-Krona (Sweden)

100 TPS

📈 🔒

Performance

CBDC Projects

e-Krona (Sweden)	e-CNY (China)
100 TPS	10’000 TPS
📈 🔒	

Performance

CBDC Projects

e-Krona (Sweden)	e-CNY (China)
100 TPS	10’000 TPS
📈 🔒	🔒

Performance

CBDC Projects

e-Krona (Sweden)	e-CNY (China)	GNU Taler
100 TPS	10’000 TPS	28’500 TPS
📈 🔒	🔒	

Performance

CBDC Projects

e-Krona (Sweden)	e-CNY (China)	GNU Taler
100 TPS	10’000 TPS	28’500 TPS
📈 🔒	🔒	📈

GNU Taler Capabilities

Today:

- Free software
- Gives change
- Can provide refunds
- Integrates nicely with HTTP
- Handles network failures
- High performance
- Formal security proofs

Ongoing work for the next release:

- Wallet-to-wallet payments
- Payments with zero-knowledge age verification
- Internationalization ⇒ `https://weblate.taler.net/`

Visions

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

Many ideas for future work

- Address remaining scalability challenges (get to 100'000 TPS)
- Porting to more platforms (Web shops, iOS, embedded)
- Integration of P2P payments (e-mail, SMS, twitter, Signal, etc.)
- Implement currency conversion service
- Improve design and usability for illiterate and innumerate users
- Integration with KYC/AML providers
- Federated exchange

... except not funded yet:
EIC did not fund our "IP-less" FLOSS company.

CBDC Initiatives and Taler

Taler can serve as the foundation for a *bearer-based retail* CBDC.

- Taler replicates physical cash rather than bank deposits
- Taler has unique design principles and regulatory features that align with CBDC requirements[3]
- ECB survey has identified privacy as a primary requirement of end users

But privacy is **not** what any of them are implementing today!

[3] Modulo those from central banks that want "complete control".

Taler: Unique Regulatory Features for CBDCs

https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03

- Central bank issues digital coins equivalent to issuing cash
  ⇒ monetary policy remains under CB control
- Architecture with consumer accounts at commercial banks
  ⇒ no competition for commercial banking (S&L)
  ⇒ CB does not have to manage KYC, customer support
- Withdrawal limits and denomination expiration
  ⇒ protects against bank runs and hoarding
- Income transparency and possibility to set fees
  ⇒ additional insights into economy and new policy options
- Revocation protocols and loss limitations
  ⇒ exit strategy and handles catastrophic security incidents
- Privacy by cryptographic design not organizational compliance
  ⇒ CB cannot be forced to facilitate mass-surveillance

Requirements: Online vs. Offline CBDC

https://taler.net/papers/euro-bearer-online-2021.pdf

- Offline capabilities are often cited as a requirement for CBDC
- All implementations must either use restrictive hardware elements and/or introduce counterparty risk.

⇒ Permanent offline features weaken a CBDC solution (privacy, security)

⇒ Introduces unwarranted competition for physical cash (endangers emergency-preparedness).

We recommend a tiered approach:

1. Online-first, bearer-based CBDC
2. (Optional:) Limited offline mode for network outages
3. Physical cash for emergencies (power outage, catastrophic cyber incidents)

Switzerland?

- SNB published paper on GNU Taler design: “How to issue a CBDC”.

Switzerland?

- SNB published paper on GNU Taler design: "How to issue a CBDC".
- SNB official line is: "We do not need a CBDC for Switzerland" (yet?).

Switzerland?

- SNB published paper on GNU Taler design: “How to issue a CBDC”.
- SNB official line is: “We do not need a CBDC for Switzerland” (yet?).
- BoJ waits for ECB/US Fed to “make first move”. Same for SNB?

Switzerland?

- SNB published paper on GNU Taler design: “How to issue a CBDC”.
- SNB official line is: “We do not need a CBDC for Switzerland” (yet?).
- BoJ waits for ECB/US Fed to “make first move”. Same for SNB?

Digitization is NOT something you just sit out.

Early movers will set the standards.

For now, that’s the Chinese.

What's next?

What Taler **developer** community will try to do:

1. Work out kinks in the GNU Taler implementation. (Help and funding appreciated!)
2. Deploy GNU Taler in Switzerland or Lichtenstein as a commercial payment system.
3. Integrate GNU Taler wherever possible. (Help required!)

What **all** of you can do:

1. Spread the word.
2. Demand to use it, when available!

What's next?

What Taler **developer** community will try to do:

1. Work out kinks in the GNU Taler implementation. (Help and funding appreciated!)
2. Deploy GNU Taler in Switzerland or Lichtenstein as a commercial payment system.
3. Integrate GNU Taler wherever possible. (Help required!)

What **all** of you can do:

1. Spread the word.
2. Demand to use it, when available!

Or, simply wait for the Chinese present to be our future:

> "Citizens blocked from attending protest against freezing of their bank accounts by Covid-apps turning red."
> –`https://shorturl.at/jvzAG` (CNN.com)

References

- Jeffrey Burdges, Florian Dold, Christian Grothoff, and Marcello Stanisci.
Enabling secure web payments with GNU Taler.
In Claude Carlet, M. Anwar Hasan, and Vishal Saraswat, editors, *6th International Conference on Security, Privacy and Applied Cryptographic Engineering*, number 10076 in LNCS, pages 251–270. Springer, Dec 2016.

- David Chaum, Christian Grothoff, and Thomas Moser.
How to issue a central bank digital currency.
In *SNB Working Papers*, number 2021-3. Swiss National Bank, February 2021.