GNU

Funded by the
European Union

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

taler.net
taler@twitter

Christian Grothoff
& Leo Wittmann

GNU Taler is a privacy-preserving payment system

GNU Taler Design Principles

Freie Software

Schutz der Privatsphäre

Überprüfbarkeit

Zahlungsbetrug unterbinden

Minimum an Notwendigen Daten

Benutzerfreundlichkeit maximieren

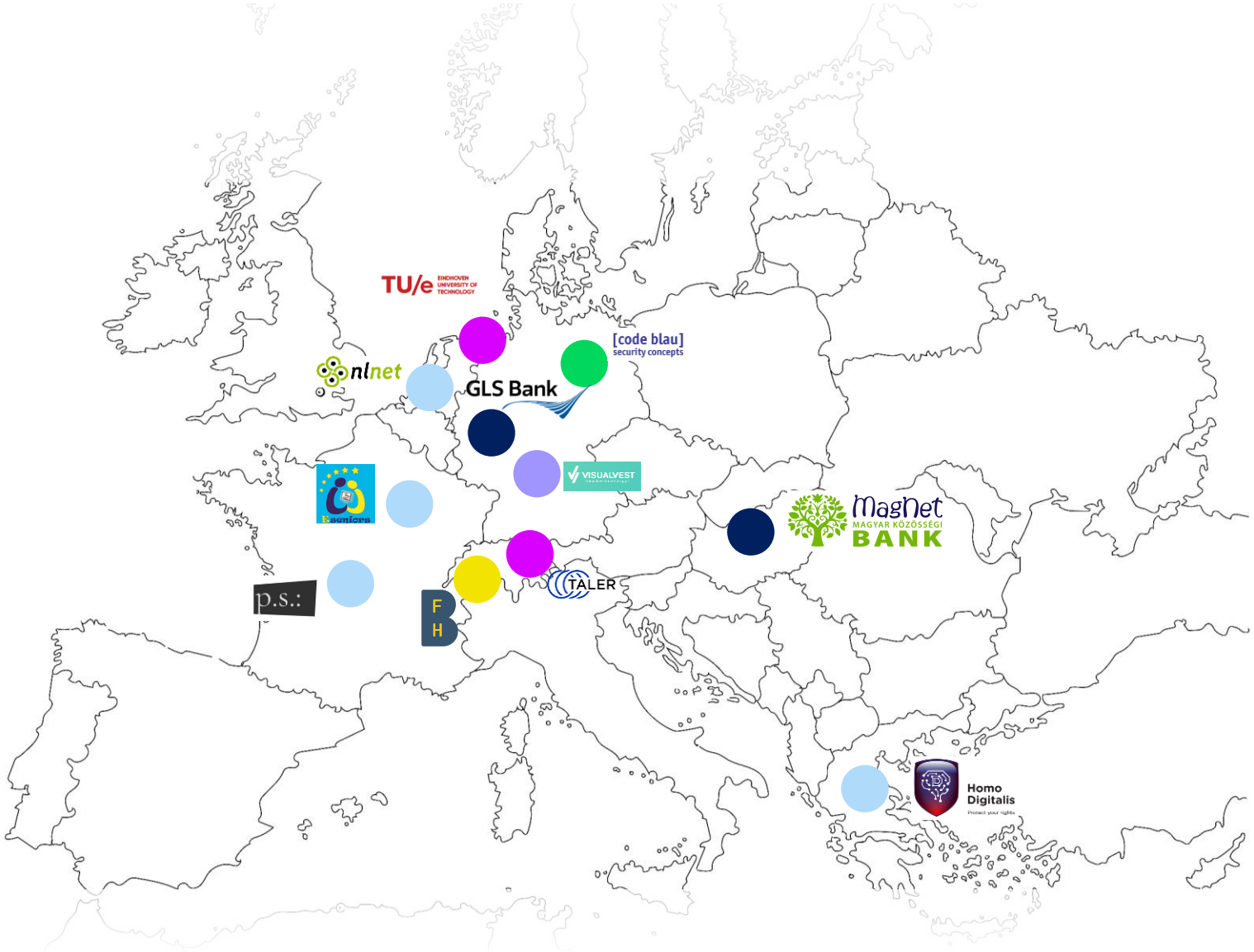
Effizienz steigern und Kosten mindern

Hohe Ausfallsicherheit und Fehlertoleranz

Goal of NGI Taler:

Make privacy preserving payments with GNU Taler available to citizens in the Eurozone, Hungary and in Switzerland

Co-funded by
the European Union


TU/e
EINDHOVEN UNIVERSITY OF TECHNOLOGY
nlnet
[code blau]
security concepts
GLS Bank
VISUALVEST
MagNet
MAGYAR KÖZÖSSÉGI
BANK
TALER
p.s.:
F
H
Homo
Digitalis

Event- & Regionalwährungen

GNU Taler

7

Event- & Regionalwährungen

GNU Taler

Zahlungsdiensteaufsichtsgesetz (ZAG)

Im Zahlungsdiensteaufsichtsgesetz (§ 1 ZAG) ist geregelt, was Zahlungsdienste sind:

- Bargeldein- und Auszahlung über Zahlungskonten
- Zahlungsvorgänge auszuführen, und hier auch die Abwicklung, also die Übermittlung von Geldbeträgen von einem, zum anderen Konto
- Ausführung von Kreditkartenzahlungen
- Ausgabe von Zahlungsinstrumenten

Ausnahmen nach ZAG

Im Zahlungsdiensteaufsichtsgesetz (§ 2 ZAG) sind aber auch Ausnahmen geregelt:

- für den Erwerb von Waren oder Dienstleistungen, in einem spezifischen räumlichen Gebiet oder durch ein begrenztes Netz
- für den Erwerb eines sehr begrenzten Waren- oder Dienstleistungsspektrums eingesetzt werden können

Und überschreitet der Gesamtwert der Zahlungsvorgänge der vorangegangenen zwölf Monate den Betrag von 1 Million Euro, hat es diese Tätigkeit der BaFin anzuzeigen.

Spezifische Anforderungen

- Der Gegenwert der Token pro Event und Kunde*in darf die Grenze von 250€ nicht überschreiten.
- Zusätzlich darf der summierte Gegenwert aller Token innerhalb einer Wallet den Betrag von 250€ nicht überschreiten.
- Gleichzeitig gilt es sicher zu stellen, dass die 250€-Grenze pro Wallet auch für P2P Zahlungen gilt. Dies gilt es technisch sicher zu stellen

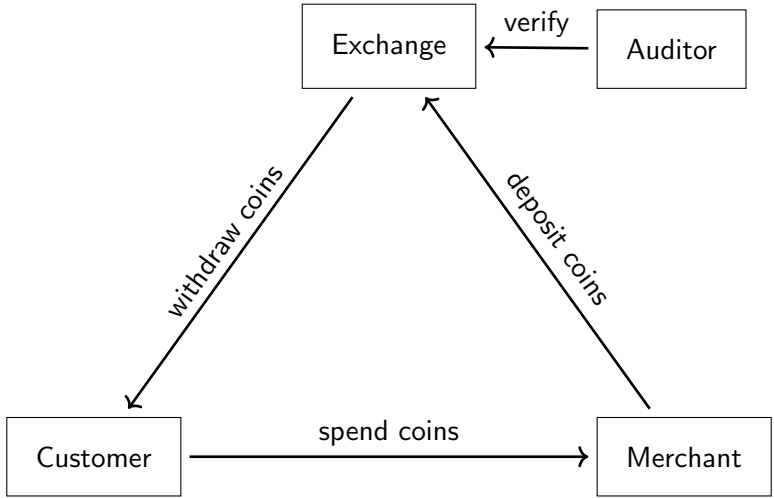
Der Gegenwert des Event-Tokens wird nicht gegen Bargeld ausgezahlt und eine Verzinsung des Gegenwertes des Event-Tokens erfolgt nicht.

Ausnahmen dieser Regelung gilt es dringend mit der BaFin abzusprechen.

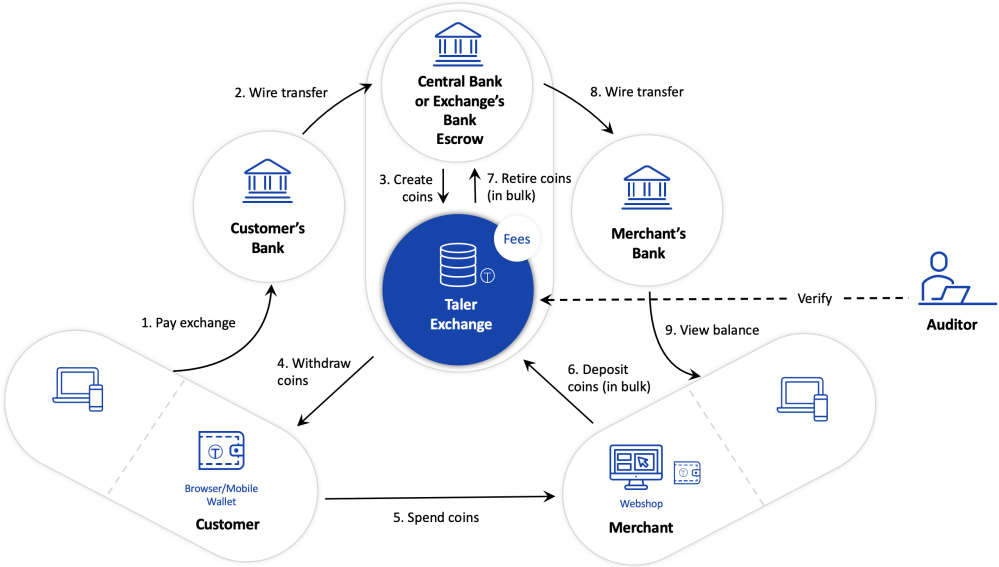
Was braucht man?

Wenn man zB Aufladungen per Überweisung zulassen möchte, bedarf es eines Zahlungskontos bei einer Bank und entsprechende Schnittstellen zur Anbindung der GNU Taler Exchange

Taler Overview



Architecture of Taler

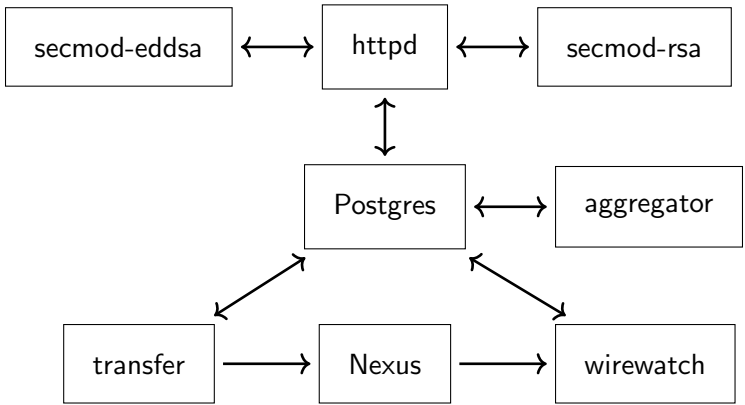


Taler Exchange

The **Exchange** is the core logic of the payment system.

- One exchange at minimum must be operated per currency
- Offers a REST API for merchants and customers
- Uses several helper processes for configuration and to interact with RTGS and cryptography
- KYC support via OAuth 2.0, KycAID or Persona APIs
- SPAs for AML and KYC processes

Taler: Exchange Architecture

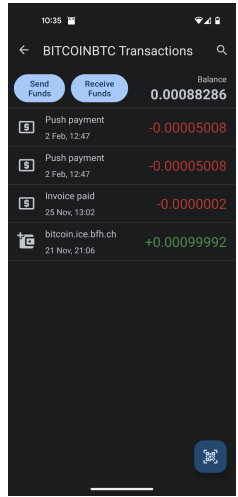


Taler Wallet

The **Wallet** is the software run by consumers to store their digital cash and authorize transactions.

- **wallet-core** is the logic shared by all interfaces
- Applications exist for Android, F-Droid, WebExtension (Chrome, Chromium, Firefox, etc.), iOS
- Features include:
  - Multi-currency support
  - Wallet-to-wallet payments (NFC or QR code)
  - CRDT-like data model

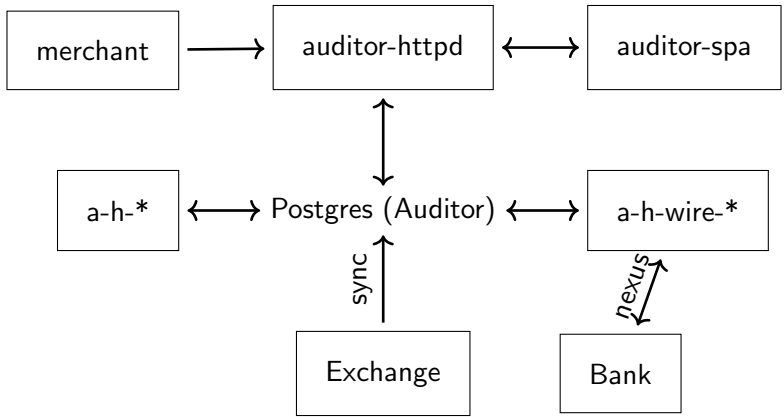
Can be integrated into other Apps if desired.



Taler Auditor

The **Auditor** is the software run by an independent auditor to validate the operation of an Exchange.

- REST API for additional report inputs by merchants (optional)
- Secure database replication logic (`taler-auditor-sync`)
- SPA for viewing results in real-time



libeufin-nexus

libeufin-nexus allows Taler components to interact with a core banking system. It:

- provides an implementation of the Wire Gateway for the exchange
- supports EBICS 2.5 and 3.0
- other APIs such as FinTS or PSD2-style XS2A APIs can be added without requiring changes to the Exchange
- was tested with GLS Bank (DE) and Postfinance (CH) accounts and real EUR/CHF

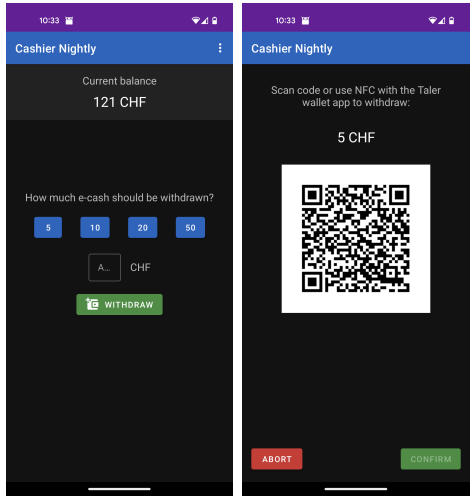
libeufin-bank

libeufin-bank implements a standalone bank with a Web interface. It:

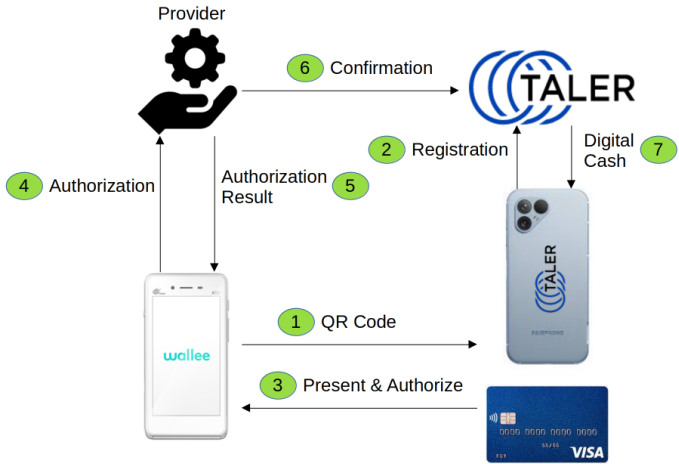
- provides the Taler Core Bank API for RESTful online banking using a Web interface (with multi-factor authentication)
- includes a Taler Wire Gateway for the exchange
- offers the Taler Bank Integration API to allow wallets to easily withdraw digital cash
- optionally provides the Taler Conversion Info API for currency conversion between fiat and regional currencies
- optionally integrates with libeufin-nexus to interact with a core banking system

Cashier App for Android

- Enables staff to convert cash to e-cash
- Staff has special bank accounts with limited funds
- Visitors can pay staff in cash to receive e-cash



Cashless2ecash by Joel Haeberli



Challenger

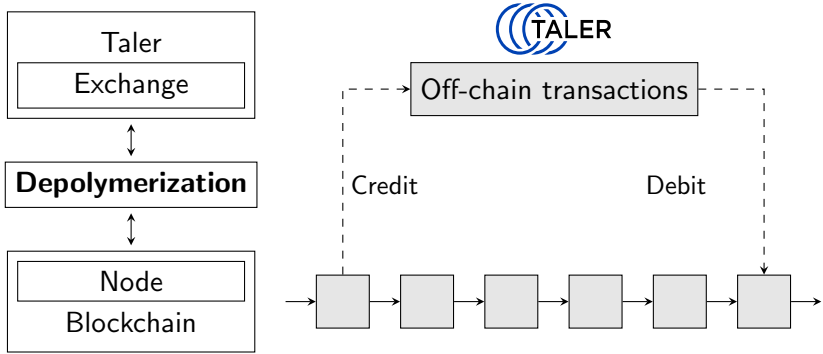
Challenger allows clients to obtain validated address (KYC) data about users:

- Customizable Web-based process for address validation
- Can validate phone numbers, e-mail addresses or physical mailing addresses
- Provides an exchange-compatible OAuth 2.0 API

Depolymerization

Depolymerization is a bridge between GNU Taler and blockchains.

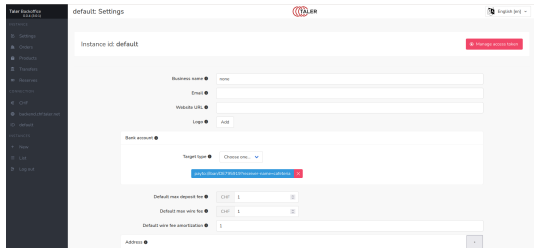
- Works on top of Bitcoin and Ethereum crypto-currencies, with the DLTs as the "RTGS"
- Provides same API to Exchange as libeufin-nexus



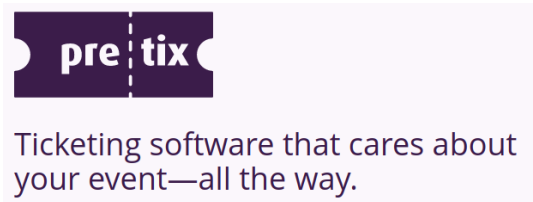
Taler Merchant

The **Merchant** is the software run by merchants to accept GNU Taler payments.

- REST API for integration with e-commerce
- SPA provides Web interface for administration
- Features include:
  - Multi-tenant support
  - Refunds
  - Templates
  - Webhooks
  - Inventory management (optional)



Pretix Taler payment plugin

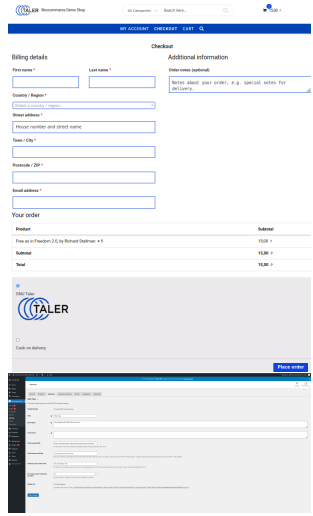


Pretix is a ticket sales system.

- Pretix payment plugin enables payments via GNU Taler
- Developed by Pretix.eu for €3,000 on behalf of Taler Systems SA

WooCommerce Taler payment plugin

- WooCommerce is an e-commerce plugin for WordPress.
- WooCommerce payment plugin enables payments via GNU Taler
- Features include:
  - Trivial configuration
  - Support for refunds
  - Full internationalization

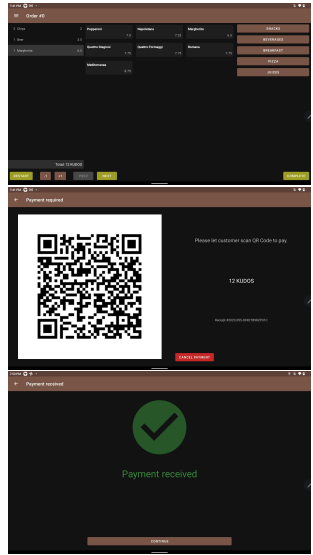


Joomla! Taler payment plugin

- Joomla! is an e-commerce platform
- Joomla! payment plugin enables payments via GNU Taler
- Features include:
  - Trivial configuration
  - Support for refunds
  - Full internationalization

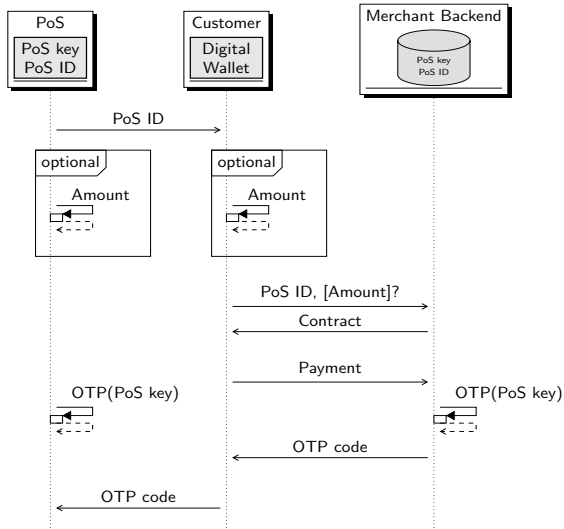
Point-of-Sale App for Android

- Allows merchant to generate orders against Taler backend and display QR code to enable customer to pay in person
- Patterned after ViewTouch restaurant UI
- Features include:
  - Internet-based configuration
  - Products sorted by categories
  - Easy undo of every operation
  - Manages multiple concurrent orders



Taler-mdb

Partially Offline Payments with GNU Taler[1]



[1] Joint work with Emmanuel Benoist, Priscilla Huang and Sebastian Marchano

Other ongoing developments

- Privacy-preserving auctions (trading, currency exchange) (`oezguer@taler.net`)
- Hardware and software support for embedded systems (`mikolai@taler.net`)
- GNU Name System registry with GNU Taler payments (`schanzen@gnunet.org`)
- Performance improvements for RSA in FLOSS crypto libraries (NLnet project)
- Tax-deductable receipts for donations to charities (donau.git)
- Unlinkable anonymous subscriptions and discount tokens (merchant.git, branch)
- Support for illiterate and innumerate users[2]

[2] Background: `https://myoralvillage.org/`

How to support?

Join: `https://lists.gnu.org/mailman/listinfo/taler`

Test: `https://bugs.taler.net/`

Translate: `https://weblate.taler.net/`[3]

Integrate: `https://docs.taler.net/`

Develop: `https://git.taler.net/`

Apply: `https://nlnet.nl/propose`, `https://nlnet.nl/taler`

[3] Contact: `translation-volunteer@taler.net`

Thanks

- Next Generation Internet (NGI) initiative
- Renewablefreedom Foundation
- Sovereigntechfund
- Prototypefund

Next session on GNU Taler:

GNU Taler:
Merchant Integrationsworkshop
18:45 Seminarraum

Do you have any questions?

References:

1. Özgür Kesim, Christian Grothoff, Florian Dold and Martin Schanzenbach. *Zero-Knowledge Age Restriction for GNU Taler*. **27th European Symposium on Research in Computer Security (ESORICS), 2022**.
2. David Chaum, Christian Grothoff and Thomas Moser. *How to issue a central bank digital currency*. **SNB Working Papers, 2021**.
3. 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.
4. Jeffrey Burdges, Florian Dold, Christian Grothoff and Marcello Stanisci. *Enabling Secure Web Payments with GNU Taler*. **SPACE 2016**.
5. Florian Dold, Sree Harsha Totakura, Benedikt Müller, Jeffrey Burdges and Christian Grothoff. *Taler: Taxable Anonymous Libre Electronic Reserves*. Available upon request. 2016.
6. 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**.
7. David Chaum, Amos Fiat and Moni Naor. *Untraceable electronic cash*. **Proceedings on Advances in Cryptology, 1990**.
8. Phillip Rogaway. *The Moral Character of Cryptographic Work*. **Asiacrypt**, 2015.

Acknowledgements

Funded by the European Union (Project 101135475).

Co-funded by
the European Union

Funded by SERI (HEU-Projekt 101135475-TALER).

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.