NEXT GENERATION INTERNET

NGI TALER & The Digital Euro

Christian Grothoff

28.05.2024

What is Taler?

Taler is

- ► a Free/Libre software *payment system* infrastructure project
- ► ... with a surrounding software ecosystem
- ► ... and a consortium (NGI TALER) and community that wants to deploy it as widely as possible.

However, Taler is

- ► *not* a currency or speculative asset
- ► *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

NGI TALER partners

Design principles

GNU Taler must ...

1. ... be implemented as **free software**.
2. ... protect the **privacy of buyers**.
3. ... 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**.

NGI TALER

Architecture of Taler
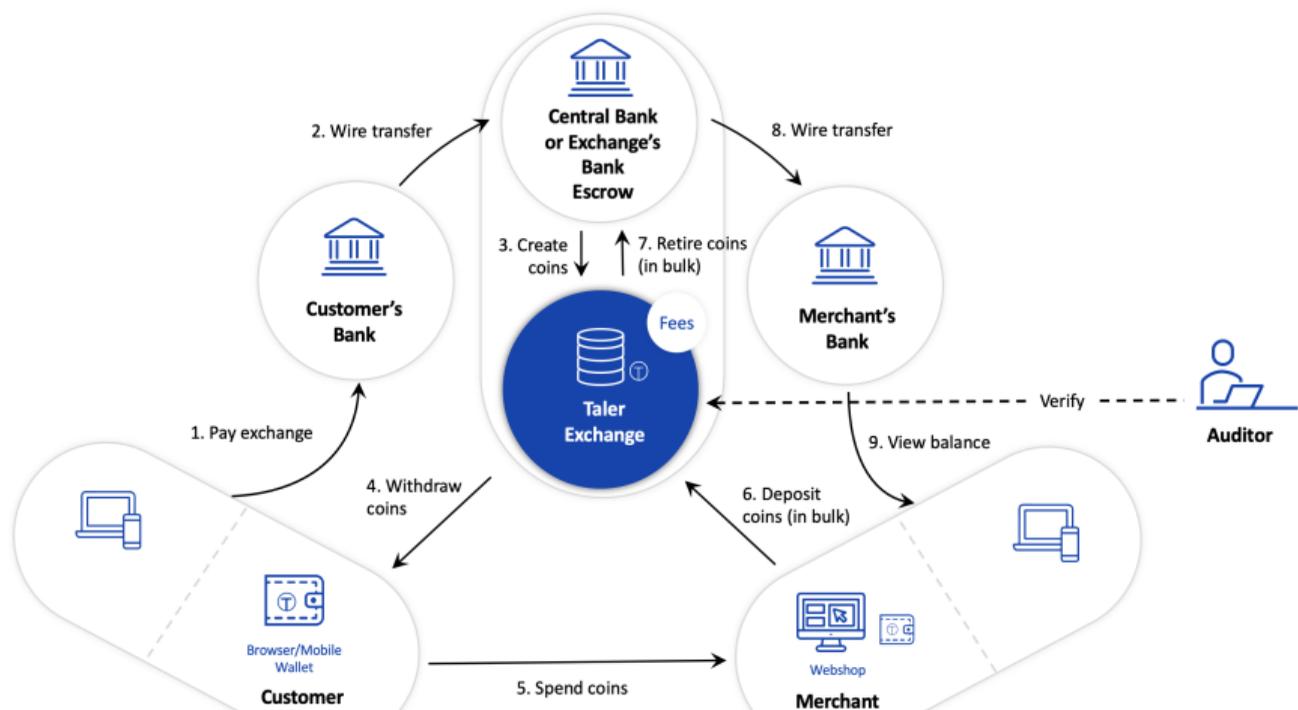
GNU Taler vs. Digital Euro
Fundamentals

GNU Taler:

- ► Payment with one-time **tokens**
- ► Cryptographic privacy for payer
- ► Suitable for children, tourists, ...
- ► Free and Open Source
- ► Deployed by community

Digital Euro:

- ► Payment using bank **accounts**
- ► Privacy by policy, linkable payments
- ► Requires ability to open bank account
- ► ECB proprietary
- ► "Moving target"

GNU Taler vs. Digital Euro
Usability

GNU Taler:

- ► Self-custody
- ► Authorize locally
- ► One-click
- ► 6+ platforms today

Digital Euro:

- ► Account-based
- ► Authenticate to provider
- ► Multi-factor
- ► FAANG-only?

GNU Taler vs. Digital Euro
Use-cases

GNU Taler:

- ► Traditional payments
- ► Micropayments
- ► IoT payments
- ► Non-fiat currencies
- ► Other assets
- ⇒ New type of service

Digital Euro:

- ► Traditional payments
- ► -
- ► -
- ► Only Euros
- ► -
- ⇒ Replacement service

NGI TALER

Digital Euro
Dangerous decisions

- ▶ **Offline requirement** assumes copy-protection unbreakable by NSA & FSB
- ▶ **Waterfall** link to bank account implies compromise of Digital Euro account also compromises linked bank accounts
- ▶ **Lack of privacy** enables "absolute control" of central bank over private finances
- ▶ **Direct competition** for bank accounts and traditional payment services disrupts banking sector financial stability
- ▶ **Non-FLOSS** solution limits interoperability and international adoption

Endgame
Risk management

The ECB tender asks for **redundant** implementations of their design.

The **design** of a CBDC is the hardest problem, not the implementation.

Acknowledgements

Funded by the European Union (Project 101135475).

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

**Co-funded by
the European Union**

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**