Taler
Taxable Anonymous Libre Electronic Reserves

F. Dold, B. Müller, S. H. Totakura, C. Grothoff

TU Munich & Inria Rennes Bretagne Atlantique

19.11.2014
Motivation

Modern economies need a currency.
Modern economies need a currency online.
SWIFT?

SWIFT/Mastercard/Visa are too transparent.
All BitCoin transactions are public

BitCoin does not come with privacy guarantees
⇒ BitCoin was enhanced with “laundering” services
⇒ ZeroCoin and successors offer full anonymity

Is society ready for an anarchistic economy?
All BitCoin transactions are public
- BitCoin does not come with privacy guarantees
  - BitCoin was enhanced with “laundering” services
  - ZeroCoin and successors offer full anonymity

Is society ready for an anarchistic economy?
Let’s make cash digital and socially responsible.
Let’s make cash digital and socially responsible.

Taxable, Anonymous, Libre, Practical, Resource Friendly
Architecture of Taler

- Mint
  - verify (to Auditor)
  - deposit coins (from Merchant)
  - withdraw coins (from Customer)

- Auditor

- Customer

- Merchant
  - spend coins (from Customer)
  - deposit coins (to Mint)

Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macropayments and microdonations
Requirements

- **Customer anonymity**
  It should not be possible to trace the spending behavior of a customer.

- Unlinkability

- Taxability

- Verifiability

- Ease of deployment

- Green / low resource consumption

- Macropayments and microdonations
Requirements

- Customer anonymity
- **Unlinkability**
  It should be infeasible to link a set of transactions (even aborted ones) to the same customer.
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macropayments and microdonations
Requirements

- Customer anonymity
- Unlinkability
- **Taxability**
  As it is the responsibility of the merchant to deduct taxes, he should be fully auditable and non-anonymous. Additionally it must not be possible to transfer cash illicitly (i.e. evading audit).
- Verifiability
- Ease of deployment
- Green / low resource consumption
- Macropayments and microdonations
Requirements

- Customer anonymity
- Unlinkability
- Taxability

- **Verifiability**
  The trust necessary between the participants of the system should be minimized. Signatures over contractual information should be available in order to resolve disputes.

- Ease of deployment
- Green / low resource consumption
- Macropayments and microdonations
Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- **Ease of deployment**
  Low entry-barrier by providing a gateway to the existing financial system (i.e. Internet-banking protocols such as HBCI/FinTS), a free software reference implementation and a open protocol standard.

- Green / low resource consumption
- Macropayments and microdonations
Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment

- **Green / low resource consumption**
  Avoid reliance on expensive and especially "wasteful" computations such as proof-of-work.

- Macropayments and microdonations
Requirements

- Customer anonymity
- Unlinkability
- Taxability
- Verifiability
- Ease of deployment
- Green / low resource consumption

- Macropayments and microdonations
  The system should be able to provide a solution for macropayments ($\geq 10ct$) as well as microdonations ($< 10ct$).
Taler Strong Assumptions

- Existence of anonymous channel (i.e. Tor) “works”
- Curve25519 elliptic curve cryptography “works”
- Chaum-style Blind signatures using RSA “work”
- Hash Functions “work”

Except for Tor, none of these are even remotely broken. Tor seems still safe within Tor’s adversary model.
The Coins

- Identified by public key
- Only owner knows private key
- Signature by mint determines denomination
- Mint signs blindly to provide anonymity
- Operations are authorized by signature of coin private key
The Mint

- Mints new coins in return for customer payments
- Pays merchants when provided with valid coin’s signatures
- Holds list of all (partially) spent coins
- Earns money by collecting transaction fees
- Restricted trust necessary, correctness legally enforceable
Security model: financial security

- Customer is compromised (coins lost) — like loosing wallet
- Customer is malicious — no damage
- Merchant is compromised — limited damage
- Merchant is malicious — customer sues for merchandise
- Mint is compromised (key lost) — limited damage
- Packet loss/network loss — unproblematic
- Mint goes offline — no transactions possible (!)
- Storage failure — need good backups
- Mint is malicious — need escrow, audit!
State of the project

- Cryptography worked out
- Protocol specification
- Prototype mint
- Prototype wallet
- Prototype merchant portal
Licensing

- Protocol must be open standard
- Wallets must be free (GPL or LGPL)
- Merchant integration is with merchant, but reference implementations free (LGPL)
- Mint reference implementation will be free (AGPL)
Possible outcomes (optimistic)

- Replace Mastercard/Visa/Paypal online
  ⇒ Cheaper transactions ≡ 3% reduction in VAT
- Replace cash and credit cards (and, in France, cheques)
  ⇒ Faster business transactions in stores
- Any Taler anyone receives is easily tracked
  ⇒ Less corruption
- Banks & spies can no longer track your spending
- Privacy for citizens!
- Industrial espionage defense for business!
Thank you for your attention.

Questions?

Answers at https://taler.net/ in November 2014!
Why should *governments* be interested?

Why not do online what they do offline?¹

¹Just better: you can anonymously receive cash, but not Taler.
Why should *governments* be interested?

Why not do *online* what they do *offline*?¹

¹Just better: you can anonymously receive cash, but not Taler.
Modes of spending

- **Complete Spending**
  - Online Payment
  - Sign deposit permission for full coin

- **Partial Spending**
  - Online Payment
  - Sign deposit permission for a fraction
  - Repeat with remaining fraction of the coin (*)

- **Incremental spending**
  - Online payment
  - Lock coin at mint (*)
  - Sign incremental deposit permissions
  - Merchant redeems last deposit

- **Probabilistic spending (bona fide)**
  - Offline payment possible
  - Gambling for payment “upgrade”
  - Interaction with mint only when payment gets upgraded
Refreshing (*)

- Spending parts of same coin twice uses the same key
- Merchants could link transactions
  \[\Rightarrow\] Danger to privacy

Mint allows (anonymous) coin owner to refresh coin.
Refreshing (*)

- Spending parts of same coin twice uses the same key
- Merchants could link transactions
  ⇒ Danger to privacy

Mint allows (anonymous) coin owner to refresh coin.