NEXT GENERATION INTERNET

GNU Taler

Christian Grothoff

07.06.2024

NEXT GENERATION INTERNET
GNU Taler
Christian Grothoff
07.06.2024

1. In this lecture, we will do a deep dive into the cryptography behind GNU Taler.

Learning objectives

How should we pay?

Introduction to GNU Taler

How does cut-and-choose work?

How to prove protocols secure with cryptographic games?

What are the future plans for GNU Taler?

How should we pay?
Introduction to GNU Taler
How does cut-and-choose work?
How to prove protocols secure with cryptographic games?
What are the future plans for GNU Taler?

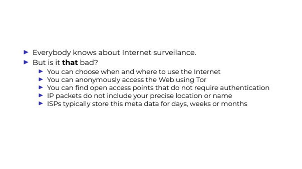
1. First, following Prof. Rogaway's call [**?**] for a community-wide effort to develop more effective means to resist mass surveillance, we will start with a moral analysis of the problem: How should we pay?
2. Then, you will get an overview of GNU Taler and its architecture. You should already be familiar with blind signatures, one key cryptographic building block.
3. We will then use GNU Taler's cryptography to introduce two more advanced cryptographic concepts, namely cut-and-choose protocols and an advanced example for provable security using cryptographic games.
4. Finally, we'll take a brief peek at the GNU Taler roadmap to see what probably lies ahead.

Surveillance

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

Surveilance concerns

- Everybody knows about Internet surveilance.
- 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



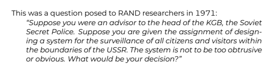
- Everybody knows about Internet surveilance.
- But is it **that** bad?
  - You can choose when and where to use the Internet
  - You can anonymously access the Web using Tor
  - You can find open access points that do not require authentication
  - IP packets do not include your precise location or name
  - ISPs typically store this meta data for days, weeks or months

1. Internet mass-surveilance may be bad, but it is to some degree avoidable or escapable.

Where is it worse?

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?"

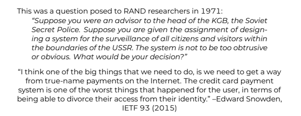
1. The result: an electronic funds transfer system that looks strikingly similar today's debit card system.
2. What is surprising is that Snowden says this is **one of the worst things**, as he obviously had a bunch of rather large concerns.

Where is it worse?

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)



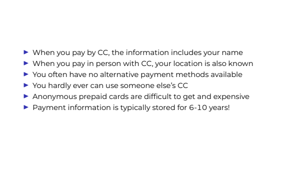
This was a question posed to RAND researchers in 1971:
"Suppose you were an advisor to the head of the KGB, the Soviet Secret Police. Suppose you are given the assignment of designing a system for the surveillance of all citizens and visitors within the boundaries of the USSR. The system is not to be 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)

1. The result: an electronic funds transfer system that looks strikingly similar today's debit card system.
2. What is surprising is that Snowden says this is **one of the worst things**, as he obviously had a bunch of rather large concerns.

Why is it 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 6-10 years!



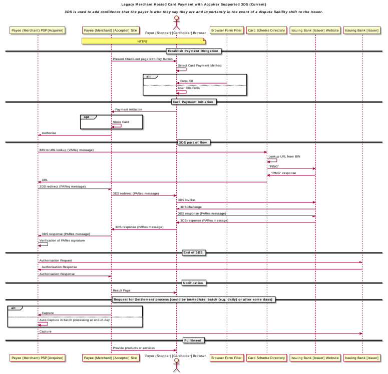
- When you pay by CC, the information includes your name
- When you pay in person with CC, your location is also known
- You often have no alternative payment methods available
- You hardly ever can use someone else's CC
- Anonymous prepaid cards are difficult to get and expensive
- Payment information is typically stored for 6-10 years!

1. For digital payments, surveilance has become completely normalized.
2. It is also basically inescapable, except by using cash. and cash sometimes cannot be used!

Credit cards have problems, too!

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

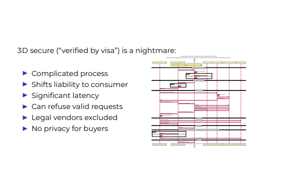
- ▶ Complicated process
- ▶ Shifts liability to consumer
- ▶ Significant latency
- ▶ Can refuse valid requests
- ▶ Legal vendors excluded
- ▶ No privacy for buyers



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



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

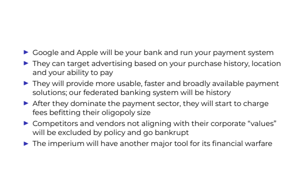
1. Now, the modern online CC process is also a nightmare, from privacy, security, usability and cost perspectives.
2. Our claim: online credit card payments will be replaced. The question is, with what?

The bank's Problem

- Global tech companies push oligopolies
- Privacy and federated finance are at risk
- Economic sovereingity is in danger

1. And Apple would like us to pay 30% fees on everything for their walled surveilance garden.

- 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



- 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

1. "Do you want to live under total surveillance?" Sure, this may sound unlikely, but let's listen to some experts on this.

The Bank of International Settlements on CBDC

1. The key sentence here is that they **will have absolute control** over how we use digital cash.
2. The director of the BIS points to this as a fact. Note that the BIS is basically the United Nations of the central banks of the world. Their headquarters is in Basel.

2024-05-24

NEXT GENERATION INTERNET
└How should we pay?

The Emergency Act of Canada, February 2022 `https://www.youtube.com/watch?`

The Emergency Act of Canada, February 2022 `https://www.youtube.com/watch?`

Digital cash, made **socially responsible**.

TALER

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

Digital cash, made **socially responsible**.

TALER

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

1. Bold claims.

What is Taler?

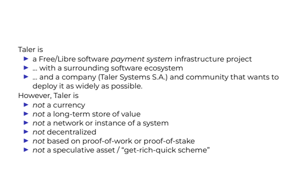
https://taler.net/en/features.html

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"



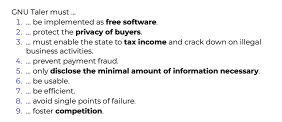
Taler is
- a Free/Libre software *payment system* infrastructure project
- ... with a surrounding software ecosystem
- ... and a company (Taler Systems S.A.) and community that wants to deploy it as widely as possible.

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"

1. Not a currency, not a crypto-currency, no blockchain, just a payment system.
2. For your day-to-day expenses, not your retirement fund or buying a house.
3. Not like PayPal where you have one operator, primarily a protocol, like HTTP!
4. Not a P2P network, there are still easily identifiable (and accountable) payment service providers.
5. Efficient, no burning down the plant for 3 transactions per second.
6. Again, not a currency, you pay with GNU Taler, not *in* Taler. You pay in EUR/CHF/USD.

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**.

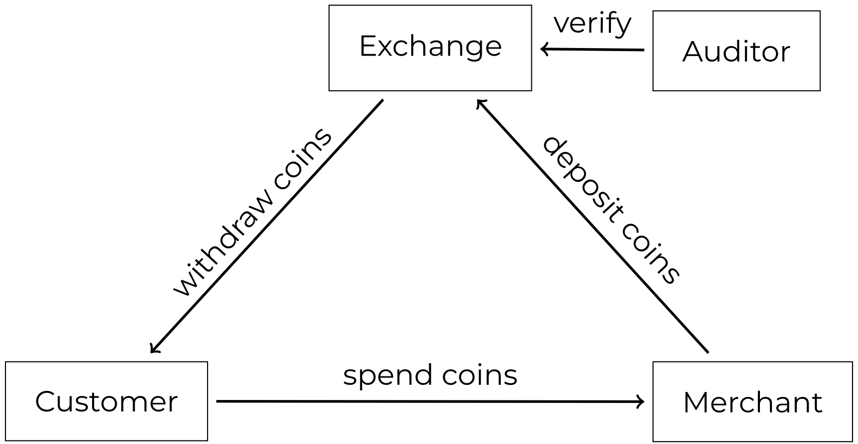


GNU Taler must ...

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**.

1. The design goals are presented in order of priority. Those higher up are more important.
2. If you have other priorities, you will end up with a different design. When designing a system, try to come up with priorities first.
3. Of course the order is not absolute: we would not sacrifice an insane amount of efficiency for a tiny gain in usability. But it is important to have priorities when the trade-offs are plausible.
4. Objective 5 is relevant as objective 2 is only about privacy of buyers, but there is other data to minimize in a complex system.
5. How do you foster competition? By making it possible for various components to be commercially offered by different parties; using proper protocols ensures there can be different implementations, operators and integrators.

Taler overview



Exchange

verify

Auditor

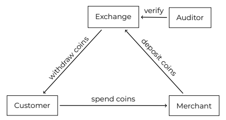
withdraw coins

deposit coins

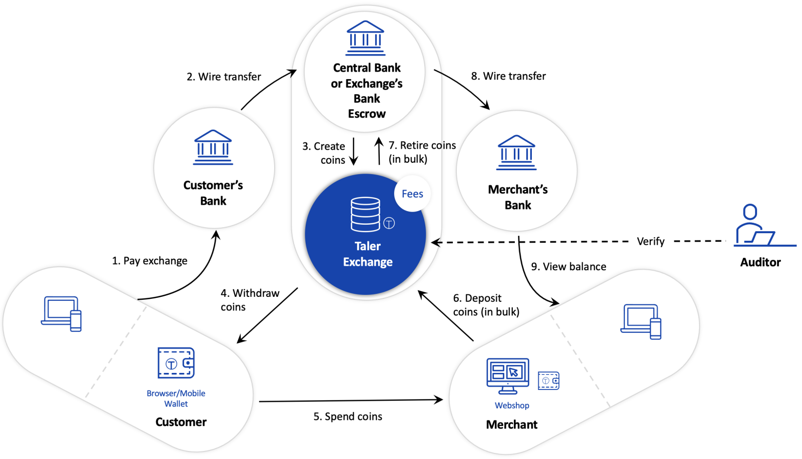
Customer

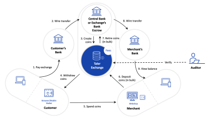
spend coins

Merchant



1. This figure shows the key parties in the GNU Taler system.
2. The exchange operates the payment system: it issues digital coins and allows them to be redeemed.
3. Customers obtain digital cash can can spend it.
4. Merchants accept digital cash.
5. The auditor checks that the exchange is operating correctly.

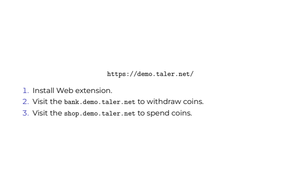




1. Illustration of the payment process of GNU Taler and its integration with an existing core banking system. Macro-payments between bank accounts (steps 2 and 8) are for large sums. Step 2 represents buyers withdrawing money from their bank accounts, and step 8 merchants receiving their aggregated (daily, weekly, monthly, etc.) revenues. In contrast, cryptographic payments within GNU Taler (steps 4, 5 and 6) are much cheaper.
2. The purchase in step 5 is unlinkable to the withdrawal in step 4 due to the use of blind signatures, which protect the anonymity for the buyer spending coins in step 5.

`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.



`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.

1. KUDOS is a “fake” currency used for the demonstration, EUR or CHF would be used in practice.
2. The demo can be done using a WebExtension or a Taler wallet running on a mobile phone, or both.
3. You can also demonstrate P2P payments between the Taler walelt browser extension and the mobile phone.

Taxability

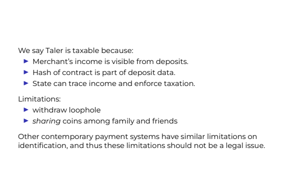
We say Taler is taxable because:

- Merchant’s income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.

Limitations:

- withdraw loophole
- *sharing* coins among family and friends

Other contemporary payment systems have similar limitations on identification, and thus these limitations should not be a legal issue.



We say Taler is taxable because:

- Merchant’s income is visible from deposits.
- Hash of contract is part of deposit data.
- State can trace income and enforce taxation.

Limitations:

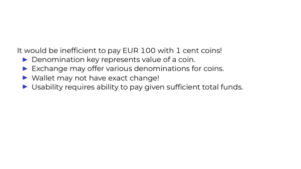
- withdraw loophole
- *sharing* coins among family and friends

Other contemporary payment systems have similar limitations on identification, and thus these limitations should not be a legal issue.

1. When withdrawing, Taler does not exactly determine that the owner of the account is also the owner of the wallet. The withdraw loophole is basically equivalent to somebody putting their bank card into an ATM and someone else taking the cash. While [**?**] explains a way to address the loophole, doing so would put the privacy of payer’s at risk, so we decided against it and will not cover it here.
2. The sharing loophole is when the owner of a coin decides to simply give the private key and signature of a digital coin to another user. As the user cannot be sure that the owner really deleted their copy of the private key material (without any backup), both users then *share* access to the value of the coin. The first to spend it, will succeed. We call this *sharing* as opposed to a transaction: in a transaction, ownership is transferred between parties that do not trust each other.
3. Sharing is thus like giving your spouse the password to your bank account.

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.



It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

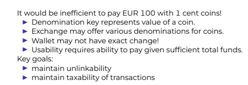
1. Taler issues digital cash using blind signatures, where each signature conveys the respective coin a particular value.
2. We want to avoid cryptographic expenses linear in the amount being paid!
3. Thus we need a way to get change, but doing so must not void our security assurances, specifically unlinkability (and anonymity) for the payer, and income transparency for the payee.
4. The high-level approach for getting change is pretty simple: when paying with a coin, the (EdDSA) coin signature can specify that not the full value of the coin is to be spent, but only a fraction. The exchange then allows a wallet to request change by creating a second signature using the partially spent coin's private (EdDSA) key over a change request with fresh (blinded) digital coins that total up to the amount of change that is due.

It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Key goals:

- maintain unlinkability
- maintain taxability of transactions



It would be inefficient to pay EUR 100 with 1 cent coins!

- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Key goals:

- maintain unlinkability
- maintain taxability of transactions

1. Taler issues digital cash using blind signatures, where each signature conveys the respective coin a particular value.
2. We want to avoid cryptographic expenses linear in the amount being paid!
3. Thus we need a way to get change, but doing so must not void our security assurances, specifically unlinkability (and anonymity) for the payer, and income transparency for the payee.
4. The high-level approach for getting change is pretty simple: when paying with a coin, the (EdDSA) coin signature can specify that not the full value of the coin is to be spent, but only a fraction. The exchange then allows a wallet to request change by creating a second signature using the partially spent coin's private (EdDSA) key over a change request with fresh (blinded) digital coins that total up to the amount of change that is due.

Giving change

It would be inefficient to pay EUR 100 with 1 cent coins!

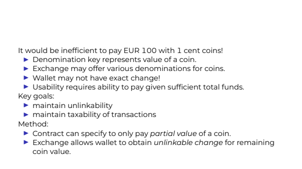
- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.

Key goals:

- maintain unlinkability
- maintain taxability of transactions

Method:

- Contract can specify to only pay *partial value* of a coin.
- Exchange allows wallet to obtain *unlinkable change* for remaining coin value.

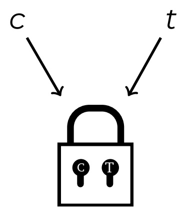


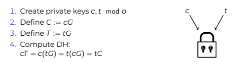
It would be inefficient to pay EUR 100 with 1 cent coins!
- Denomination key represents value of a coin.
- Exchange may offer various denominations for coins.
- Wallet may not have exact change!
- Usability requires ability to pay given sufficient total funds.
Key goals:
- maintain unlinkability
- maintain taxability of transactions
Method:
- Contract can specify to only pay *partial value* of a coin.
- Exchange allows wallet to obtain *unlinkable change* for remaining coin value.

1. Taler issues digital cash using blind signatures, where each signature conveys the respective coin a particular value.
2. We want to avoid cryptographic expenses linear in the amount being paid!
3. Thus we need a way to get change, but doing so must not void our security assurances, specifically unlinkability (and anonymity) for the payer, and income transparency for the payee.
4. The high-level approach for getting change is pretty simple: when paying with a coin, the (EdDSA) coin signature can specify that not the full value of the coin is to be spent, but only a fraction. The exchange then allows a wallet to request change by creating a second signature using the partially spent coin's private (EdDSA) key over a change request with fresh (blinded) digital coins that total up to the amount of change that is due.

Diffie-Hellman (ECDH)

1. Create private keys $c, t \mod o$
2. Define $C := cG$
3. Define $T := tG$
4. Compute DH:
   $cT = c(tG) = t(cG) = tC$



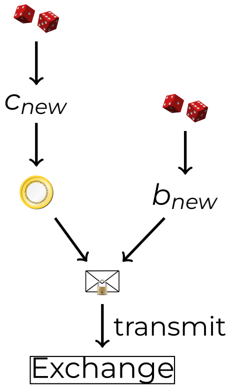

1. Create private keys $c, t \mod o$
2. Define $C := cG$
3. Define $T := tG$
4. Compute DH:
   $cT = c(tG) = t(cG) = tC$

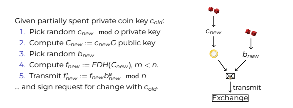
1. Before we can introduce the change protocol, we need another pretty picture for a well-known cryptographic primitive, Diffie-Hellman (DH). Taler uses ECDH, but that does not matter except for performance.
2. A good way to think of DH is a lock with two keys where either key opens the lock.
3. Note that we will use DH in a rather unusual way in the following protocol.

Given partially spent private coin key c_{old}:

1. Pick random $c_{new} \mod o$ private key
2. Compute $C_{new} := c_{new}G$ public key
3. Pick random b_{new}
4. Compute $f_{new} := FDH(C_{new})$, $m < n$.
5. Transmit $f'_{new} := f_{new} b^e_{new} \mod n$

… and sign request for change with c_{old}.



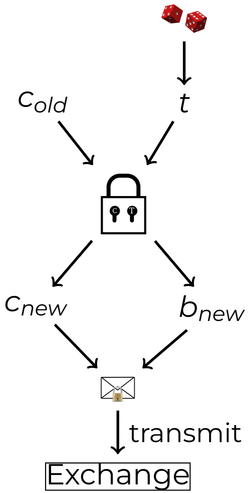

Given partially spent private coin key c_{old}:
1. Pick random $c_{new} \mod o$ private key
2. Compute $C_{new} := c_{new}G$ public key
3. Pick random b_{new}
4. Compute $f_{new} := FDH(C_{new})$, $m < n$.
5. Transmit $f'_{new} := f_{new} b^e_{new} \mod n$
… and sign request for change with c_{old}.
c_{new}
b_{new}
transmit
Exchange

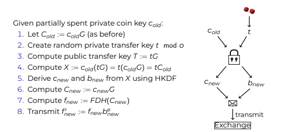
1. A strawman solution is one that does not work, but still could be useful to illuminate the issue.
2. Here, the protocol allows users to obtain change (c_{new}) by signing the request for change (the envelope) with an old coin c_{old} that has some residual value from a previous purchase (that signature is not shown).
3. **Problem**: Owner of c_{new} may differ from owner of c_{old} breaks income-transparency / enables tax evasion!

Customer: Transfer key setup (ECDH)

Given partially spent private coin key c_{old}:

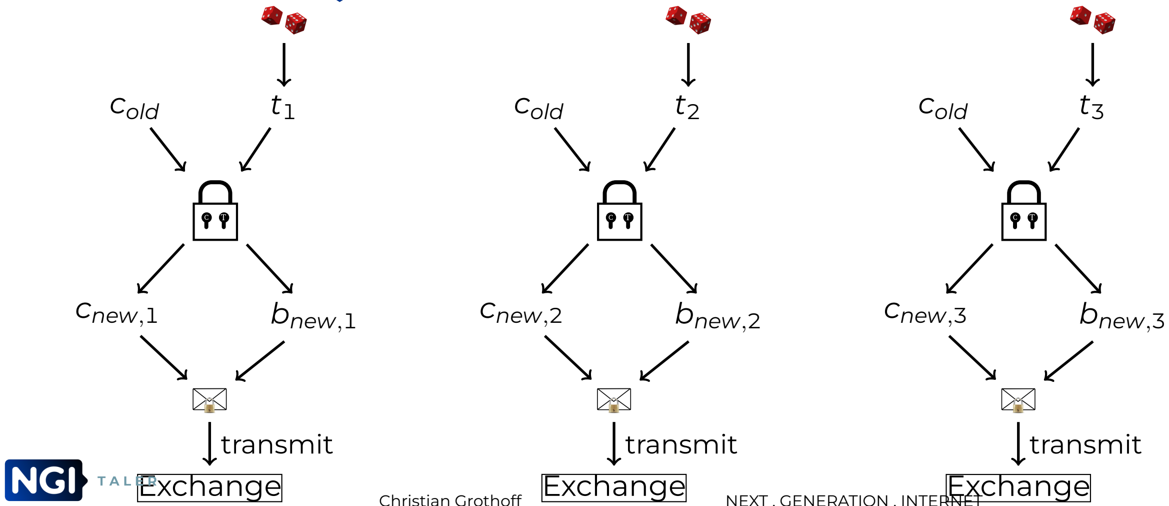
1. Let $C_{old} := c_{old}G$ (as before)
2. Create random private transfer key $t \mod o$
3. Compute public transfer key $T := tG$
4. Compute $X := c_{old}(tG) = t(c_{old}G) = tC_{old}$
5. Derive c_{new} and b_{new} from X using HKDF
6. Compute $C_{new} := c_{new}G$
7. Compute $f_{new} := FDH(C_{new})$
8. Transmit $f'_{new} := f_{new}b^e_{new}$




Given partially spent private coin key c_{old}:
1. Let $C_{old} := c_{old}G$ (as before)
2. Create random private transfer key $t \mod o$
3. Compute public transfer key $T := tG$
4. Compute $X := c_{old}(tG) = t(c_{old}G) = tC_{old}$
5. Derive c_{new} and b_{new} from X using HKDF
6. Compute $C_{new} := c_{new}G$
7. Compute $f_{new} := FDH(C_{new})$
8. Transmit $f'_{new} := f_{new}b^e_{new}$

1. In this construction, we *derive* the blinding factor b_{new} and the private key of the new coin c_{new} from the DH of the c_{old} and a newly created transfer key t. Note that it is a bit unusual but perfectly find that we here have **both** private keys to compute the DH.
2. The resulting blinded public key of the new coin (public key derivation and blinding are elided to keep the diagram concise) is then signed with c_{old} to request change.
3. This approach has an obvious problem: from the perspective of the Exchange, we cannot even tell that the user followed this procedure as the resulting request with the blinded coin is indistinguishable from the previous construction.

Cut-and-Choose



c_{old} t_1

$c_{new,1}$ $b_{new,1}$

transmit

Exchange

c_{old} t_2

$c_{new,2}$ $b_{new,2}$

transmit

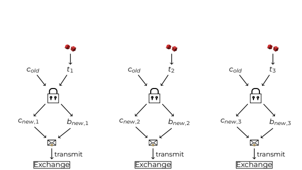
Exchange

c_{old} t_3

$c_{new,3}$ $b_{new,3}$

transmit

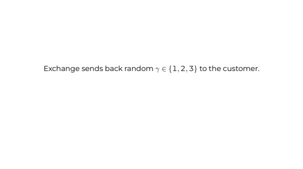
Exchange



1. This DH-construction thus obviously does not work, so in the usual approach of an insane person, we don't just do it once, but three times using three different transfer keys t_1, t_2, and t_3 instead of just t.
2. Now, before you decide that we have just gone mad, this is actually a well-known technique called **cut-and-choose**. Here, we do a protocol step multiple times to basically be able to **burn** some of these iterations to **prove** our honesty.
3. There are also **non-interactive** cut-and-choose protocols, but this one is a simple interactive one.

Exchange: Choose!

Exchange sends back random $\gamma \in \{1, 2, 3\}$ to the customer.

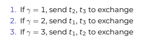


Exchange sends back random $\gamma \in \{1, 2, 3\}$ to the customer.

1. This is the typical interaction: the Exchange picks one of the three at random, basically deciding on which iterations to challenge the wallet's honesty.
2. γ primarily needs to be **unpredictable** for the wallet.
3. Note that the protocol has a security parameter $\kappa = 3$, and so the wallet could guess correctly in $\frac{1}{3}$ of the cases. Usually in security we would think of this to be way too low, and you will see much higher values in other cut-and-choose protocols. But, we will see why $\kappa = 3$ is actually enough for GNU Taler!

Customer: Reveal

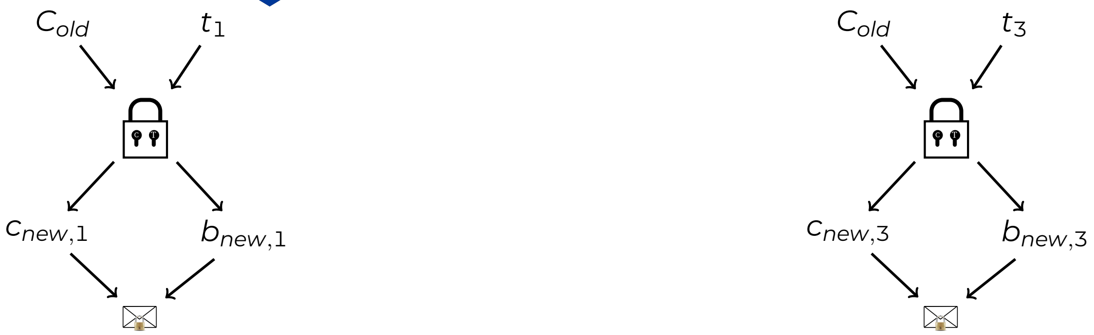
1. If $\gamma = 1$, send t_2, t_3 to exchange
2. If $\gamma = 2$, send t_1, t_3 to exchange
3. If $\gamma = 3$, send t_1, t_2 to exchange



1. If $\gamma = 1$, send t_2, t_3 to exchange
2. If $\gamma = 2$, send t_1, t_3 to exchange
3. If $\gamma = 3$, send t_1, t_2 to exchange

1. So given the γ challenge value, the wallet has to send back the t_i values for $i \neq \gamma$.

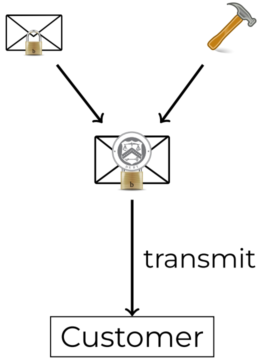
Exchange: Verify ($\gamma = 2$)

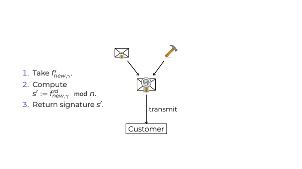


1. Given those two values the exchange can **validate** the construction as it can compute the DH from the **transfer private keys** t_i and the **coin public key** C_{old}.
2. If the result matches with the original request from the wallet, the exchange has established that with $\frac{2}{3}$ probability the wallet made an honest request for change following the prescribed construction.
3. If the wallet is unable (or unwilling) to produce the required t_i values, or if the resulting blinded values do not match, the entire change is forfeit, and the customer looses their money.
4. Thus, trying to cheat on income-transparency is punished with what amounts to a **66.67% tax**. Thus, a security level of κ is sufficient as long as the *effective* income tax (after deductions, on the full income) is below $\frac{\kappa-1}{\kappa}$. Taler always uses $\kappa = 3$.

Exchange: Blind sign change (RSA)

1. Take $f'_{new,\gamma}$.
2. Compute $s' := f'^{d}_{new,\gamma} \mod n$.
3. Return signature s'.

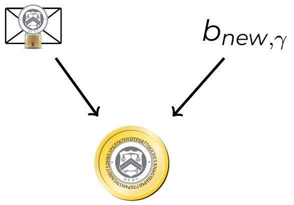


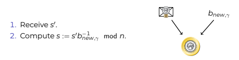


1. If the customer's request did follow the DH-construction, the exchange takes the third envelope, the one where t_γ was not disclosed, and signs this one to issue the change.

Customer: Unblind change (RSA)

1. Receive s'.
2. Compute $s := s' b_{new,\gamma}^{-1} \mod n$.



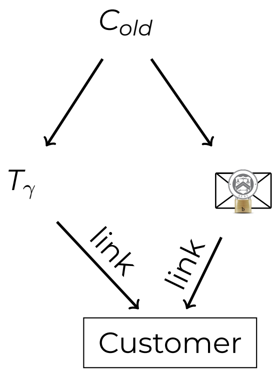


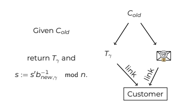
1. As with the ordinary blind-signature based withdraw, the customer can then unblind the signature and has a valid coin.
2. Without knowledge of c_{old} or t_γ, the coins derived from this process are indistinguishable from coins that were withdrawn directly from an account.
3. Most importantly, without knowledge of t_γ or c_{old}, the c_{new} is unlinkable to c_{old}.

Given C_{old}

return T_γ and

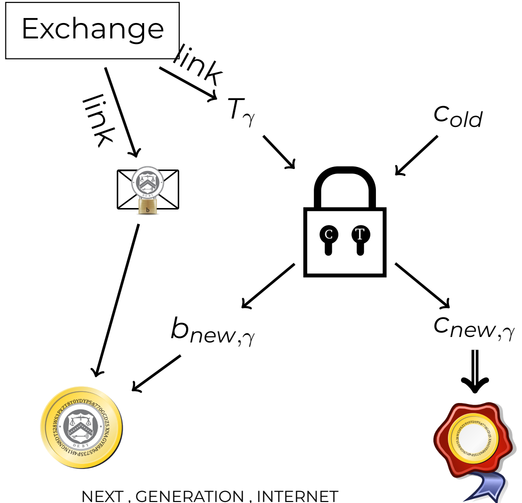
$s := s' b_{new,\gamma}^{-1} \mod n.$





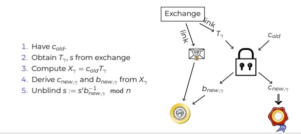
1. But, how does this address the issue that c_{old} may have a different owner from $c_{new,\gamma}$? Well, so far it does not! In principle, the envelope can easily be constructed by someone who was not the original owner of c_{old}.
2. So how does this help? Well, the exchange has one more sub-protocol, which is the **link** protocol. Given the old coin's public key, C_{old}, it returns T_γ, the **public transfer key**, and the blind signature over the new coin that was rendered as change.
3. Note that this is a request that the owner of c_{old} can always trivially make, as they know C_{old}.
4. So how does that help?

1. Have c_{old}.
2. Obtain T_γ, s from exchange
3. Compute $X_\gamma = c_{old}T_\gamma$
4. Derive $c_{new,\gamma}$ and $b_{new,\gamma}$ from X_γ
5. Unblind $s := s'b_{new,\gamma}^{-1} \mod n$



└How does cut-and-choose work?

└Customer: Link (threat!)



1. Well, given these two values, the owner of the original c_{old} can **also** compute the DH (this time from c_{old} and T_γ), and then also derive $c_{new,\gamma}$ and also unblind the exchange's signature using $b_{new,\gamma}$.
2. As a result, the owner of the old coin can always compute the change, and thus is effectively **also** always an owner of the change rendered!
3. Thus, we have **reduced** the possibility of abusing the change protocol for a transaction that would result in a **mutually exclusive transfer of ownership** to the case where the ownership of the change is **shared**.
4. But, we previously explained that **sharing** is not something we can or would care to prevent, so the change protocol does not weaken income transparency.

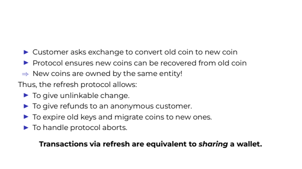
- Customer asks exchange to convert old coin to new coin
- Protocol ensures new coins can be recovered from old coin

⇒ New coins are owned by the same entity!

Thus, the refresh protocol allows:

- To give unlinkable change.
- To give refunds to an anonymous customer.
- To expire old keys and migrate coins to new ones.
- To handle protocol aborts.

Transactions via refresh are equivalent to *sharing* a wallet.



- Customer asks exchange to convert old coin to new coin
- Protocol ensures new coins can be recovered from old coin

⇒ New coins are owned by the same entity!

Thus, the refresh protocol allows:

- To give unlinkable change.
- To give refunds to an anonymous customer.
- To expire old keys and migrate coins to new ones.
- To handle protocol aborts.

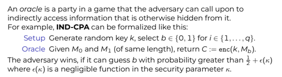
Transactions via refresh are equivalent to *sharing* a wallet.

1. In Taler, the overall protocol is called the **refresh** protocol, not the **change** protocol, as it has uses beyond getting unlinkable change.
2. A merchant can grant a refund to an anonymous customer by telling the exchange to nullify the original deposit. Then the anonymous owner of the original coin can obtain the refund via the refresh protocol.
3. If a coin is about to expire (because the exchange only accepts deposits for a certain denomination key for a limited amount of time), the refresh protocol can be used to obtain fresh coins, signed with the current denomination key. This is like rolling over to a fresh series of bank notes.
4. Finally, we can handle situations where the customer did try to spend digital cash, but then the message was lost, say due to a power outage, before the transaction was actually completed. But, the customer might not be sure that nobody else saw the public key of the coin! So, to ensure that transactions remain unlinkable (and that the merchant cannot deposit the coin later), the wallet can again use the refresh protocol.

An *oracle* is a party in a game that the adversary can call upon to indirectly access information that is otherwise hidden from it.
For example, **IND-CPA** can be formalized like this:

- Setup: Generate random key k, select $b \in \{0, 1\}$ for $i \in \{1, \ldots, q\}$.
- Oracle: Given M_0 and M_1 (of same length), return $C := \texttt{enc}(k, M_b)$.

The adversary wins, if it can guess b with probability greater than $\frac{1}{2} + \epsilon(\kappa)$ where $\epsilon(\kappa)$ is a negligible function in the security parameter κ.



An *oracle* is a party in a game that the adversary can call upon to indirectly access information that is otherwise hidden from it.
For example, **IND-CPA** can be formalized like this:

- Setup: Generate random key k, select $b \in \{0, 1\}$ for $i \in \{1, \ldots, q\}$.
- Oracle: Given M_0 and M_1 (of same length), return $C := \texttt{enc}(k, M_b)$.

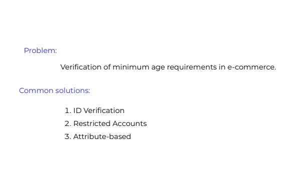
The adversary wins, if it can guess b with probability greater than $\frac{1}{2} + \epsilon(\kappa)$ where $\epsilon(\kappa)$ is a negligible function in the security parameter κ.

Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

1. ID Verification
2. Restricted Accounts
3. Attribute-based



Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

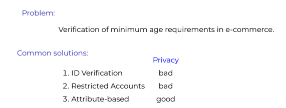
1. ID Verification
2. Restricted Accounts
3. Attribute-based

Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

	Privacy
1. ID Verification	bad
2. Restricted Accounts	bad
3. Attribute-based	good



Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

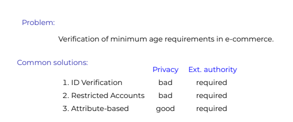
	Privacy
1. ID Verification	bad
2. Restricted Accounts	bad
3. Attribute-based	good

Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

	Privacy	Ext. authority
1. ID Verification	bad	required
2. Restricted Accounts	bad	required
3. Attribute-based	good	required



Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

	Privacy	Ext. authority
1. ID Verification	bad	required
2. Restricted Accounts	bad	required
3. Attribute-based	good	required

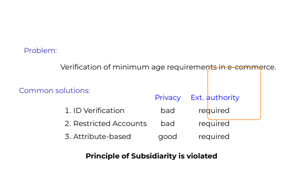
Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

	Privacy	Ext. authority
1. ID Verification	bad	required
2. Restricted Accounts	bad	required
3. Attribute-based	good	required

Principle of Subsidiarity is violated



Problem:

Verification of minimum age requirements in e-commerce.

Common solutions:

	Privacy	Ext. authority
1. ID Verification	bad	required
2. Restricted Accounts	bad	required
3. Attribute-based	good	required

Principle of Subsidiarity is violated

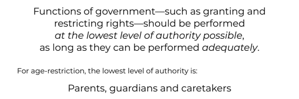
Functions of government—such as granting and restricting rights—should be performed *at the lowest level of authority possible*, as long as they can be performed *adequately*.

Functions of government—such as granting and restricting rights—should be performed *at the lowest level of authority possible*, as long as they can be performed *adequately*.

Functions of government—such as granting and restricting rights—should be performed *at the lowest level of authority possible*, as long as they can be performed *adequately*.

For age-restriction, the lowest level of authority is:

Parents, guardians and caretakers



Functions of government—such as granting and restricting rights—should be performed *at the lowest level of authority possible*, as long as they can be performed *adequately*.

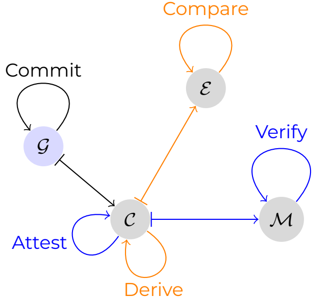
For age-restriction, the lowest level of authority is:

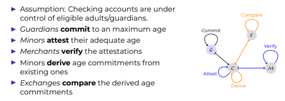
Parents, guardians and caretakers

1. Tie age restriction to the **ability to pay** (not to ID's)
2. maintain **anonymity of buyers**
3. maintain **unlinkability of transactions**
4. align with **principle of subsidiartiy**
5. be **practical and efficient**

1. Tie age restriction to the **ability to pay** (not to ID's)
2. maintain **anonymity of buyers**
3. maintain **unlinkability of transactions**
4. align with **principle of subsidiartiy**
5. be **practical and efficient**

- Assumption: Checking accounts are under control of eligible adults/guardians.
- *Guardians* **commit** to an maximum age
- *Minors* **attest** their adequate age
- *Merchants* **verify** the attestations
- Minors **derive** age commitments from existing ones
- *Exchanges* **compare** the derived age commitments




- Assumption: Checking accounts are under control of eligible adults/guardians.
- *Guardians* **commit** to an maximum age
- *Minors* **attest** their adequate age
- *Merchants* **verify** the attestations
- Minors **derive** age commitments from existing ones
- *Exchanges* **compare** the derived age commitments

1. This scheme is independent of payment service protocol.

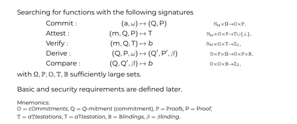
Searching for functions with the following signatures

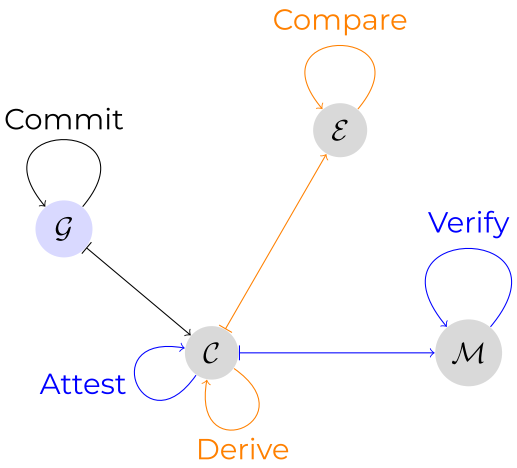
$$\begin{array}{lll}
\text{Commit :} & (a,\omega) \mapsto (Q,P) & \mathbb{N}_M \times \Omega \to \mathbb{O} \times \mathbb{P}, \\
\text{Attest :} & (m,Q,P) \mapsto T & \mathbb{N}_M \times \mathbb{O} \times \mathbb{P} \to \mathbb{T} \cup \{\bot\}, \\
\text{Verify :} & (m,Q,T) \mapsto b & \mathbb{N}_M \times \mathbb{O} \times \mathbb{T} \to \mathbb{Z}_2, \\
\text{Derive :} & (Q,P,\omega) \mapsto (Q',P',\beta) & \mathbb{O} \times \mathbb{P} \times \Omega \to \mathbb{O} \times \mathbb{P} \times \mathbb{B}, \\
\text{Compare :} & (Q,Q',\beta) \mapsto b & \mathbb{O} \times \mathbb{O} \times \mathbb{B} \to \mathbb{Z}_2,
\end{array}$$

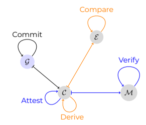
with $\Omega, \mathbb{P}, \mathbb{O}, \mathbb{T}, \mathbb{B}$ sufficiently large sets.

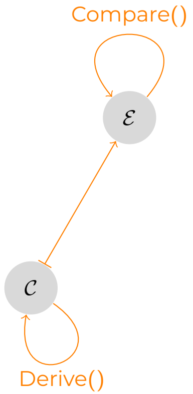
Basic and security requirements are defined later.

Mnemonics:
$\mathbb{O}$ = *c$\mathbb{O}$mmitments*, Q = *Q-mitment* (commitment), $\mathbb{P}$ = *$\mathbb{P}$roofs*, P = *Proof*,
$\mathbb{T}$ = *a$\mathbb{T}$testations*, T = *aTtestation*, $\mathbb{B}$ = *$\mathbb{B}$lindings*, β = *βlinding*.


Searching for functions with the following signatures
Commit : (a, ω) ↦ (Q, P) $\mathbb{N}_M \times \Omega \to \mathbb{O} \times \mathbb{P}$,
Attest : (m, Q, P) ↦ T $\mathbb{N}_M \times \mathbb{O} \times \mathbb{P} \to \mathbb{T} \cup \{\bot\}$,
Verify : (m, Q, T) ↦ b $\mathbb{N}_M \times \mathbb{O} \times \mathbb{T} \to \mathbb{Z}_2$,
Derive : (Q, P, ω) ↦ (Q′, P′, β) $\mathbb{O} \times \mathbb{P} \times \Omega \to \mathbb{O} \times \mathbb{P} \times \mathbb{B}$,
Compare : (Q, Q′, β) ↦ b $\mathbb{O} \times \mathbb{O} \times \mathbb{B} \to \mathbb{Z}_2$,
with Ω, ℙ, 𝕆, 𝕋, 𝔹 sufficiently large sets.
Basic and security requirements are defined later.
Mnemonics:
𝕆 = c𝕆mmitments, Q = Q-mitment (commitment), ℙ = ℙroofs, P = Proof,
𝕋 = a𝕋testations, T = aTtestation, 𝔹 = 𝔹lindings, β = βlinding.


Compare
$\mathcal{E}$
Commit
$\mathcal{G}$
Verify
$\mathcal{C}$
$\mathcal{M}$
Attest
Derive



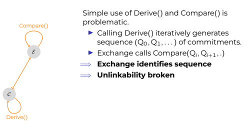


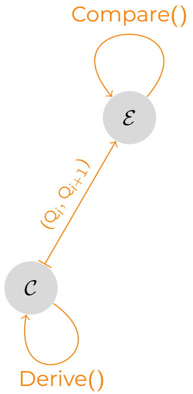
Simple use of Derive() and Compare() is problematic.

- Calling Derive() iteratively generates sequence $(Q_0, Q_1, \ldots)$ of commitments.
- Exchange calls Compare$(Q_i, Q_{i+1}, \cdot)$

$\Longrightarrow$ **Exchange identifies sequence**

$\Longrightarrow$ **Unlinkability broken**


Simple use of Derive() and Compare() is problematic.
- Calling Derive() iteratively generates sequence $(Q_0, Q_1, \ldots)$ of commitments.
- Exchange calls Compare$(Q_i, Q_{i+1}, \cdot)$
$\Longrightarrow$ **Exchange identifies sequence**
$\Longrightarrow$ **Unlinkability broken**

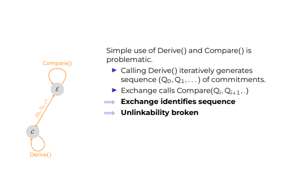


Simple use of Derive() and Compare() is problematic.

- Calling Derive() iteratively generates sequence $(Q_0, Q_1, \dots)$ of commitments.
- Exchange calls Compare$(Q_i, Q_{i+1}, .)$

$\Longrightarrow$ **Exchange identifies sequence**

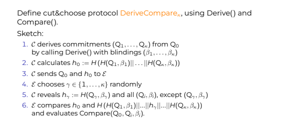
$\Longrightarrow$ **Unlinkability broken**


Simple use of Derive() and Compare() is problematic.
Calling Derive() iteratively generates sequence $(Q_0, Q_1, \dots)$ of commitments.
Exchange calls Compare$(Q_i, Q_{i+1}, .)$
Exchange identifies sequence
Unlinkability broken

Define cut&choose protocol DeriveCompare$_\kappa$, using Derive() and Compare().

Sketch:

1. $\mathcal{C}$ derives commitments $(\mathsf{Q}_1, \dots, \mathsf{Q}_\kappa)$ from Q_0 by calling Derive() with blindings $(\beta_1, \dots, \beta_\kappa)$
2. $\mathcal{C}$ calculates $h_0 := H\left(H(\mathsf{Q}_1, \beta_1) || \dots || H(\mathsf{Q}_\kappa, \beta_\kappa)\right)$
3. $\mathcal{C}$ sends Q_0 and h_0 to $\mathcal{E}$
4. $\mathcal{E}$ chooses $\gamma \in \{1, \dots, \kappa\}$ randomly
5. $\mathcal{C}$ reveals $h_\gamma := H(\mathsf{Q}_\gamma, \beta_\gamma)$ and all (Q_i, β_i), except $(\mathsf{Q}_\gamma, \beta_\gamma)$
6. $\mathcal{E}$ compares h_0 and $H\left(H(\mathsf{Q}_1, \beta_1)||...||h_\gamma||...||H(\mathsf{Q}_\kappa, \beta_\kappa)\right)$ and evaluates Compare$(\mathsf{Q}_0, \mathsf{Q}_i, \beta_i)$.



Define cut&choose protocol DeriveCompare$_\kappa$, using Derive() and Compare().

Sketch:

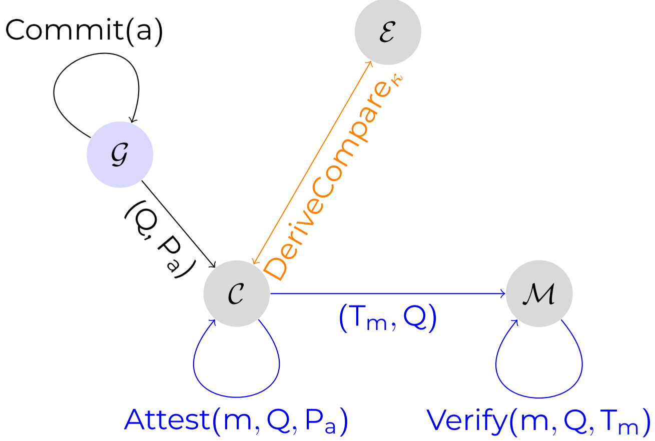
1. $\mathcal{C}$ derives commitments $(\mathsf{Q}_1, \dots, \mathsf{Q}_\kappa)$ from Q_0 by calling Derive() with blindings $(\beta_1, \dots, \beta_\kappa)$
2. $\mathcal{C}$ calculates $h_0 := H\left(H(\mathsf{Q}_1, \beta_1) || \dots || H(\mathsf{Q}_\kappa, \beta_\kappa)\right)$
3. $\mathcal{C}$ sends Q_0 and h_0 to $\mathcal{E}$
4. $\mathcal{E}$ chooses $\gamma \in \{1, \dots, \kappa\}$ randomly
5. $\mathcal{C}$ reveals $h_\gamma := H(\mathsf{Q}_\gamma, \beta_\gamma)$ and all (Q_i, β_i), except $(\mathsf{Q}_\gamma, \beta_\gamma)$
6. $\mathcal{E}$ compares h_0 and $H\left(H(\mathsf{Q}_1, \beta_1)||...||h_\gamma||...||H(\mathsf{Q}_\kappa, \beta_\kappa)\right)$ and evaluates Compare$(\mathsf{Q}_0, \mathsf{Q}_i, \beta_i)$.

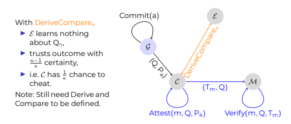
1. Scheme is similar to the *refresh* protocol in GNU Taler.

With DeriveCompare$_\kappa$

- $\mathcal{E}$ learns nothing about Q_γ,
- trusts outcome with $\frac{\kappa-1}{\kappa}$ certainty,
- i.e. $\mathcal{C}$ has $\frac{1}{\kappa}$ chance to cheat.

Note: Still need Derive and Compare to be defined.





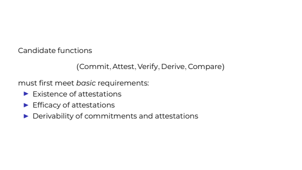
1. The image on the right shows the refined scheme using DeriveCompare$_\kappa$ for unlinkability.

Candidate functions

$$(\text{Commit}, \text{Attest}, \text{Verify}, \text{Derive}, \text{Compare})$$

must first meet *basic* requirements:

- Existence of attestations
- Efficacy of attestations
- Derivability of commitments and attestations

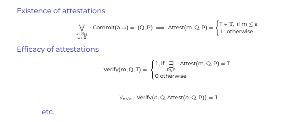


Candidate functions

$$(\text{Commit}, \text{Attest}, \text{Verify}, \text{Derive}, \text{Compare})$$

must first meet *basic* requirements:

- Existence of attestations
- Efficacy of attestations
- Derivability of commitments and attestations



Existence of attestations

$$\underset{\substack{a\in\mathbb{N}_M\\ \omega\in\Omega}}{\forall} : \mathrm{Commit}(a,\omega) =: (Q,P) \implies \mathrm{Attest}(m,Q,P) = \begin{cases} T\in\mathbb{T},\ \text{if } m\le a \\ \perp\ \text{otherwise}\end{cases}$$

Efficacy of attestations

$$\mathrm{Verify}(m,Q,T) = \begin{cases} 1,\ \text{if } \underset{P\in\mathbb{P}}{\exists} : \mathrm{Attest}(m,Q,P) = T \\ 0\ \text{otherwise}\end{cases}$$

$$\forall_{n\le a} : \mathrm{Verify}\big(n,Q,\mathrm{Attest}(n,Q,P)\big) = 1.$$

etc.

Candidate functions must also meet *security* requirements. Those are defined via security games:

- ► Game: Age disclosure by commitment or attestation
- ↔ Requirement: Non-disclosure of age
- ► Game: Forging attestation
- ↔ Requirement: Unforgeability of minimum age
- ► Game: Distinguishing derived commitments and attestations
- ↔ Requirement: Unlinkability of commitments and attestations

Meeting the security requirements means that adversaries can win those games only with negligible advantage.

Adversaries are arbitrary polynomial-time algorithms, acting on all relevant input.

Candidate functions must also meet *security* requirements. Those are defined via security games:

- ► Game: Age disclosure by commitment or attestation
- ↔ Requirement: Non-disclosure of age
- ► Game: Forging attestation
- ↔ Requirement: Unforgeability of minimum age
- ► Game: Distinguishing derived commitments and attestations
- ↔ Requirement: Unlinkability of commitments and attestations

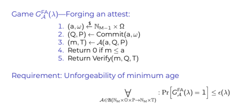
Meeting the security requirements means that adversaries can win those games only with negligible advantage.
Adversaries are arbitrary polynomial-time algorithms, acting on all relevant input.

Game $G^{\mathsf{FA}}_{\mathcal{A}}(\lambda)$—Forging an attest:

1. $(\mathsf{a},\omega) \xleftarrow{\$} \mathbb{N}_{\mathsf{M}-1} \times \Omega$
2. $(\mathsf{Q},\mathsf{P}) \leftarrow \mathsf{Commit}(\mathsf{a},\omega)$
3. $(\mathsf{m},\mathsf{T}) \leftarrow \mathcal{A}(\mathsf{a},\mathsf{Q},\mathsf{P})$
4. Return 0 if $\mathsf{m} \leq \mathsf{a}$
5. Return $\mathsf{Verify}(\mathsf{m},\mathsf{Q},\mathsf{T})$

Requirement: Unforgeability of minimum age

$$\underset{\mathcal{A}\in\mathfrak{A}(\mathbb{N}_{\mathsf{M}}\times\mathbb{O}\times\mathbb{P}\to\mathbb{N}_{\mathsf{M}}\times\mathbb{T})}{\forall} : \Pr\left[G^{\mathsf{FA}}_{\mathcal{A}}(\lambda)=1\right] \leq \epsilon(\lambda)$$



Game $G^{\mathsf{FA}}_{\mathcal{A}}(\lambda)$—Forging an attest:

1. $(\mathsf{a},\omega) \xleftarrow{\$} \mathbb{N}_{\mathsf{M}-1} \times \Omega$
2. $(\mathsf{Q},\mathsf{P}) \leftarrow \mathsf{Commit}(\mathsf{a},\omega)$
3. $(\mathsf{m},\mathsf{T}) \leftarrow \mathcal{A}(\mathsf{a},\mathsf{Q},\mathsf{P})$
4. Return 0 if $\mathsf{m} \leq \mathsf{a}$
5. Return $\mathsf{Verify}(\mathsf{m},\mathsf{Q},\mathsf{T})$

Requirement: Unforgeability of minimum age

$$\underset{\mathcal{A}\in\mathfrak{A}(\mathbb{N}_{\mathsf{M}}\times\mathbb{O}\times\mathbb{P}\to\mathbb{N}_{\mathsf{M}}\times\mathbb{T})}{\forall} : \Pr\left[G^{\mathsf{FA}}_{\mathcal{A}}(\lambda)=1\right] \leq \epsilon(\lambda)$$

To Commit to age (group) $a \in \{1, \ldots, M\}$

1. Guardian generates ECDSA-keypairs, one per age (group):

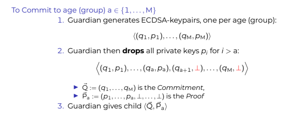
$$\langle (q_1, p_1), \ldots, (q_M, p_M) \rangle$$

2. Guardian then **drops** all private keys p_i for $i > a$:

$$\Big\langle (q_1, p_1), \ldots, (q_a, p_a), (q_{a+1}, \bot), \ldots, (q_M, \bot) \Big\rangle$$

   - $\vec{Q} := (q_1, \ldots, q_M)$ is the *Commitment*,
   - $\vec{P}_a := (p_1, \ldots, p_a, \bot, \ldots, \bot)$ is the *Proof*

3. Guardian gives child $\langle \vec{Q}, \vec{P}_a \rangle$



To Commit to age (group) $a \in \{1, \ldots, M\}$

1. Guardian generates ECDSA-keypairs, one per age (group):

$$\langle (q_1, p_1), \ldots, (q_M, p_M) \rangle$$

2. Guardian then **drops** all private keys p_i for $i > a$:

$$\Big\langle (q_1, p_1), \ldots, (q_a, p_a), (q_{a+1}, \bot), \ldots, (q_M, \bot) \Big\rangle$$

   - $\vec{Q} := (q_1, \ldots, q_M)$ is the *Commitment*,
   - $\vec{P}_a := (p_1, \ldots, p_a, \bot, \ldots, \bot)$ is the *Proof*

3. Guardian gives child $\langle \vec{Q}, \vec{P}_a \rangle$

Child has

- ordered public-keys $\vec{Q} = (q_1, \dots, q_M)$,
- (some) private-keys $\vec{P} = (p_1, \dots, p_a, \bot, \dots, \bot)$.

To Attest a minimum age $m \leq a$:

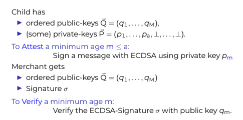
Sign a message with ECDSA using private key p_m

Merchant gets

- ordered public-keys $\vec{Q} = (q_1, \dots, q_M)$
- Signature σ

To Verify a minimum age m:

Verify the ECDSA-Signature σ with public key q_m.



Child has

- ordered public-keys $\vec{Q} = (q_1, \dots, q_M)$,
- (some) private-keys $\vec{P} = (p_1, \dots, p_a, \bot, \dots, \bot)$.

To Attest a minimum age $m \leq a$:

Sign a message with ECDSA using private key p_m

Merchant gets

- ordered public-keys $\vec{Q} = (q_1, \dots, q_M)$
- Signature σ

To Verify a minimum age m:

Verify the ECDSA-Signature σ with public key q_m.

Child has $\vec{Q} = (q_1, \ldots, q_M)$ and $\vec{P} = (p_1, \ldots, p_a, \perp, \ldots, \perp)$.

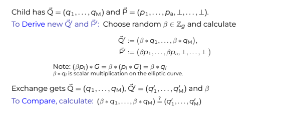
To Derive new $\vec{Q}'$ and $\vec{P}'$: Choose random $\beta \in \mathbb{Z}_g$ and calculate

$$\begin{aligned} \vec{Q}' &:= (\beta * q_1, \ldots, \beta * q_M), \\ \vec{P}' &:= (\beta p_1, \ldots, \beta p_a, \perp, \ldots, \perp\ ) \end{aligned}$$

Note: $(\beta p_i) * G = \beta * (p_i * G) = \beta * q_i$
$\beta * q_i$ is scalar multiplication on the elliptic curve.

Exchange gets $\vec{Q} = (q_1, \ldots, q_M)$, $\vec{Q}' = (q'_1, \ldots, q'_M)$ and β

To Compare, calculate: $(\beta * q_1, \ldots, \beta * q_M) \overset{?}{=} (q'_1, \ldots, q'_M)$



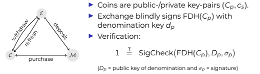
Child has $\vec{Q} = (q_1, \ldots, q_M)$ and $\vec{P} = (p_1, \ldots, p_a, \perp, \ldots, \perp)$.
To Derive new $\vec{Q}'$ and $\vec{P}'$: Choose random $\beta \in \mathbb{Z}_g$ and calculate
$\vec{Q}' := (\beta * q_1, \ldots, \beta * q_M)$,
$\vec{P}' := (\beta p_1, \ldots, \beta p_a, \perp, \ldots, \perp\ )$
Note: $(\beta p_i) * G = \beta * (p_i * G) = \beta * q_i$
$\beta * q_i$ is scalar multiplication on the elliptic curve.
Exchange gets $\vec{Q} = (q_1, \ldots, q_M)$, $\vec{Q}' = (q'_1, \ldots, q'_M)$ and β
To Compare, calculate: $(\beta * q_1, \ldots, \beta * q_M) \overset{?}{=} (q'_1, \ldots, q'_M)$

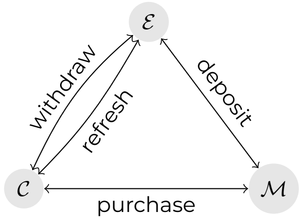
Functions (Commit, Attest, Verify, Derive, Compare)
as defined in the instantiation with ECDSA

- meet the basic requirements,
- also meet all security requirements.
  Proofs by security reduction, details are in the paper.

Functions (Commit, Attest, Verify, Derive, Compare)
as defined in the instantiation with ECDSA

- meet the basic requirements,
- also meet all security requirements.
  Proofs by security reduction, details are in the paper.





- Coins are public-/private key-pairs (C_p, c_s).
- Exchange blindly signs FDH(C_p) with denomination key d_p
- Verification:

$$1 \overset{?}{=} \text{SigCheck}\big(\text{FDH}(C_p), D_p, \sigma_p\big)$$

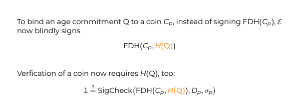
(D_p = public key of denomination and σ_p = signature)

To bind an age commitment Q to a coin C_p, instead of signing FDH(C_p), $\mathcal{E}$ now blindly signs

$$\text{FDH}(C_p, H(\text{Q}))$$

Verfication of a coin now requires H(Q), too:

$$1 \overset{?}{=} \text{SigCheck}\big(\text{FDH}(C_p, H(\text{Q})), D_p, \sigma_p\big)$$

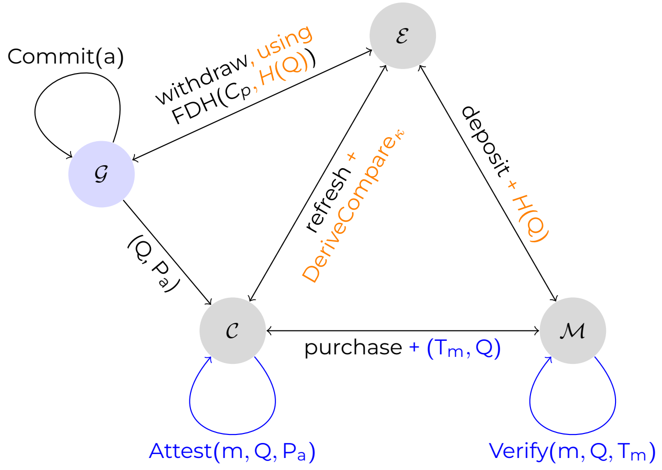


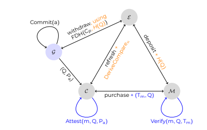
To bind an age commitment Q to a coin C_p, instead of signing FDH(C_p), $\mathcal{E}$ now blindly signs

$$\text{FDH}(C_p, H(\text{Q}))$$

Verfication of a coin now requires H(Q), too:

$$1 \overset{?}{=} \text{SigCheck}(\text{FDH}(C_p, H(\text{Q})), D_p, \sigma_p)$$


Commit(a)
withdraw, using FDH(C_p, H(Q))
$\mathcal{E}$
$\mathcal{G}$
(Q, P_a)
refresh + DeriveCompare$_\kappa$
deposit + H(Q)
$\mathcal{C}$
$\mathcal{M}$
purchase + (T_m, Q)
Attest(m, Q, P_a)
Verify(m, Q, T_m)



Paper also formally defines another signature scheme: Edx25519.

- Scheme already in use in GNUnet,
- based on EdDSA (Bernstein et al.),
- generates compatible signatures and
- allows for key derivation from both, private and public keys, independently.

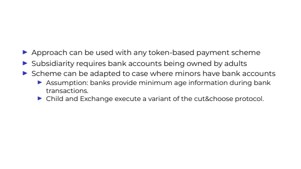
Current implementation of age restriction in GNU Taler uses Edx25519.

Paper also formally defines another signature scheme: Edx25519.

- Scheme already in use in GNUnet,
- based on EdDSA (Bernstein et al.),
- generates compatible signatures and
- allows for key derivation from both, private and public keys, independently.

Current implementation of age restriction in GNU Taler uses Edx25519.

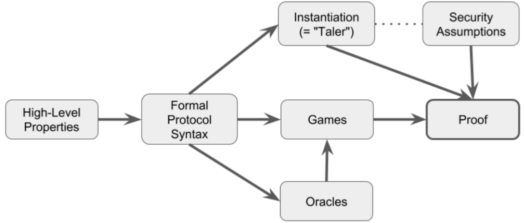
- Approach can be used with any token-based payment scheme
- Subsidiarity requires bank accounts being owned by adults
- Scheme can be adapted to case where minors have bank accounts
    - Assumption: banks provide minimum age information during bank transactions.
    - Child and Exchange execute a variant of the cut&choose protocol.

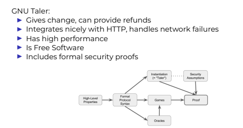


- Approach can be used with any token-based payment scheme
- Subsidiarity requires bank accounts being owned by adults
- Scheme can be adapted to case where minors have bank accounts
    - Assumption: banks provide minimum age information during bank transactions.
    - Child and Exchange execute a variant of the cut&choose protocol.

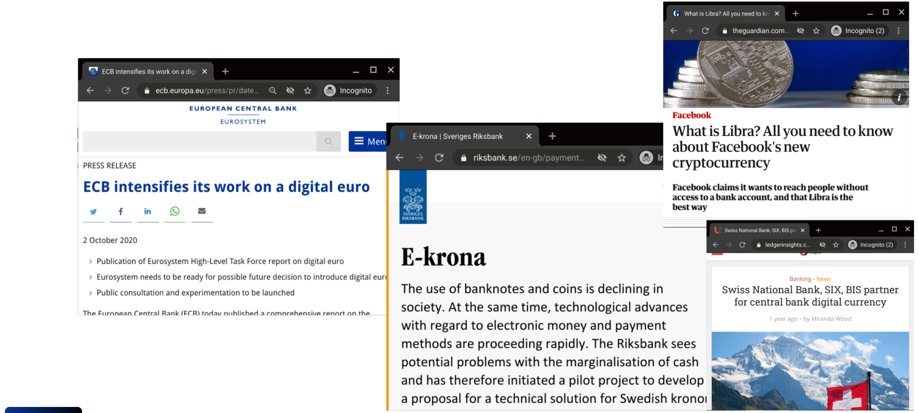
GNU Taler:

- Gives change, can provide refunds
- Integrates nicely with HTTP, handles network failures
- Has high performance
- Is Free Software
- Includes formal security proofs




GNU Taler:
- Gives change, can provide refunds
- Integrates nicely with HTTP, handles network failures
- Has high performance
- Is Free Software
- Includes formal security proofs

Many initiatives are currently at the level of requirements discussion:


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

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

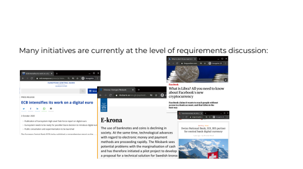
E-krona

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 krono

Banking • News

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

1 year ago • by Miranda Wood

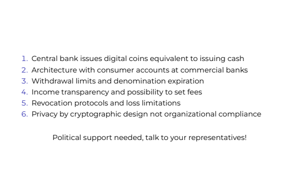


1. CBDC = Central Bank Digital Currency, so digital payment systems operated by the central bank and where the money is a liability of the central bank.
2. Taler can serve as the foundation for a *bearer-based retail* CBDC.
3. Taler replicates physical cash rather than bank deposits

1. Central bank issues digital coins equivalent to issuing cash
2. Architecture with consumer accounts at commercial banks
3. Withdrawal limits and denomination expiration
4. Income transparency and possibility to set fees
5. Revocation protocols and loss limitations
6. Privacy by cryptographic design not organizational compliance

Political support needed, talk to your representatives!

└Unique regulatory features for CBs



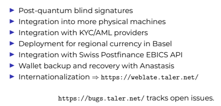
1. Central bank issues digital coins equivalent to issuing cash
2. Architecture with consumer accounts at commercial banks
3. Withdrawal limits and denomination expiration
4. Income transparency and possibility to set fees
5. Revocation protocols and loss limitations
6. Privacy by cryptographic design not organizational compliance

Political support needed, talk to your representatives!

1. ⇒ monetary policy remains under CB control
2. ⇒ no competition for commercial banking (S&L) and
   ⇒ CB does not have to manage KYC, customer support
3. ⇒ protects against bank runs and hoarding
4. ⇒ additional insights into economy and new policy options
5. ⇒ exit strategy and handles catastrophic security incidents
6. ⇒ **CB cannot be forced to facilitate mass-surveillance**

- Post-quantum blind signatures
- Integration into more physical machines
- Integration with KYC/AML providers
- Deployment for regional currency in Basel
- Integration with Swiss Postfinance EBICS API
- Wallet backup and recovery with Anastasis
- Internationalization ⇒ `https://weblate.taler.net/`

`https://bugs.taler.net/` tracks open issues.



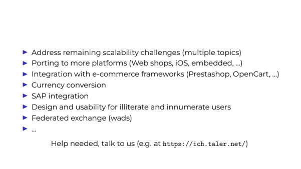
- Post-quantum blind signatures
- Integration into more physical machines
- Integration with KYC/AML providers
- Deployment for regional currency in Basel
- Integration with Swiss Postfinance EBICS API
- Wallet backup and recovery with Anastasis
- Internationalization ⇒ https://weblate.taler.net/

https://bugs.taler.net/ tracks open issues.

1. This list naturally changes frequently.
2. The key message at this time is that Taler is currently operated at a small scale, but we expect to grow it much bigger soon.
3. Help with translations is always welcome.

- Address remaining scalability challenges (multiple topics)
- Porting to more platforms (Web shops, iOS, embedded, ...)
- Integration with e-commerce frameworks (Prestashop, OpenCart, ...)
- Currency conversion
- SAP integration
- Design and usability for illiterate and innumerate users
- Federated exchange (wads)
- ...

Help needed, talk to us (e.g. at `https://ich.taler.net/`)

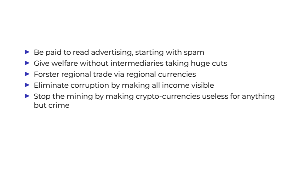


- Address remaining scalability challenges (multiple topics)
- Porting to more platforms (Web shops, iOS, embedded, ...)
- Integration with e-commerce frameworks (Prestashop, OpenCart, ...)
- Currency conversion
- SAP integration
- Design and usability for illiterate and innumerate users
- Federated exchange (wads)
- ...

Help needed, talk to us (e.g. at `https://ich.taler.net/`)

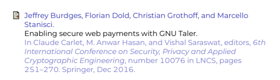
1. GNU Taler already performs well, but there are many, many scenarios to test and further optimize. So plenty of work to go around!
2. Similarly, payments have many applications, so integrating GNU Taler into any business process that involves a customer payment is literally work that will never end. But, it should be simple if you actually understand the business process.
3. Usability is another critical topic, and we hope to address the needs of more than just the 99% of commercially viable users.

- 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


- 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

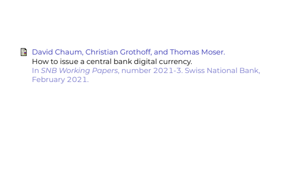
1. These are some of the more speculative results that we hope to eventually achieve using GNU Taler.
2. Do you have any interesting ideas of what one could also accomplish with this system?

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.



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.



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.

Co-funded by the European Union (Project 101135475).

Co-funded by the European Union

Co-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.

Co-funded by the European Union (Project 101135475).
Co-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
Co-funded by the European Union
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.