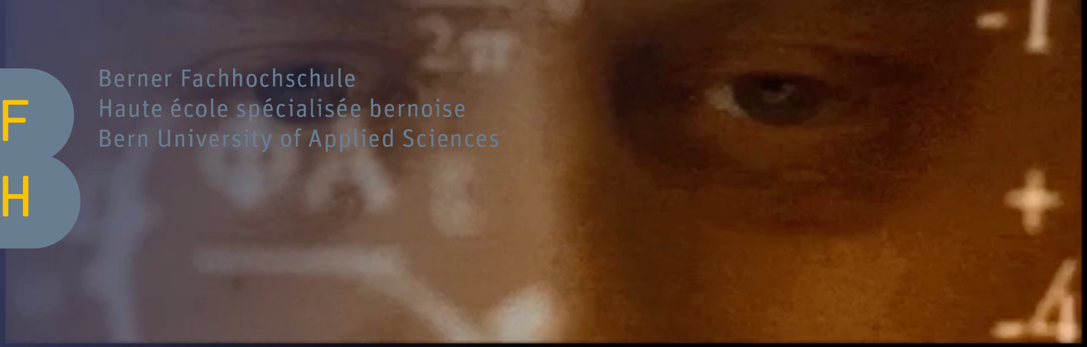
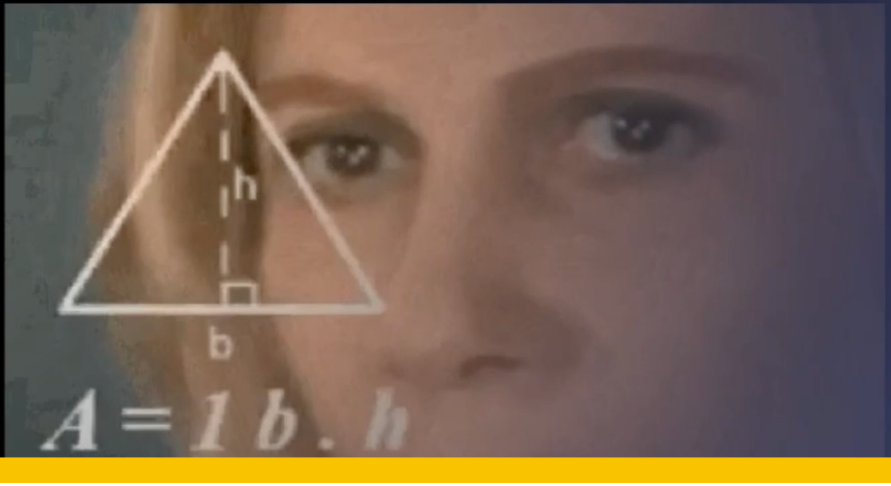
Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences





Privacy-preserving subscriptions and discounts in GNU Taler

Bachelor Thesis Defense

Christian Blättler

▸ School of Engineering and Computer Science

Agenda

- Project recap
- Motivation
- Problem
- Solution
- Database
- Anonymity set
- Management UI
- Other use cases
- Limitations
- Future work

Project recap

16

Advisor meetings

12’053

Lines of code

7

Git repositories

17

Weeks of work

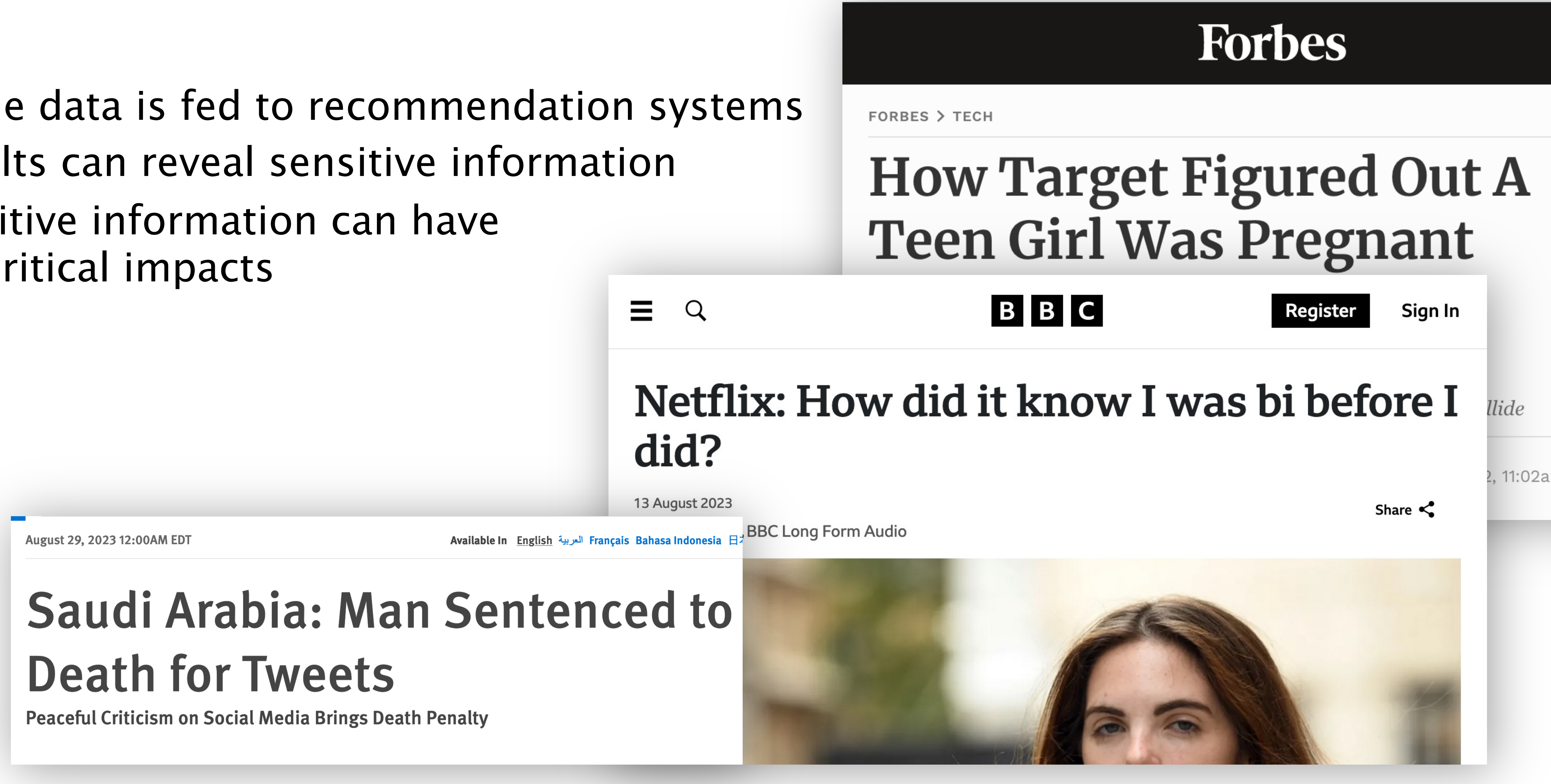
Motivation

Subscriptions are great, but…

- Subscriptions require accounts
- User’s actions are linkable to account
- Profiling user behavior
  - …for profit

Motivation

- Usage data is fed to recommendation systems
- Results can reveal sensitive information
- Sensitive information can have life-critical impacts



Forbes

FORBES › TECH

How Target Figured Out A Teen Girl Was Pregnant

llide

2, 11:02a

Netflix: How did it know I was bi before I did?

13 August 2023

BBC Long Form Audio

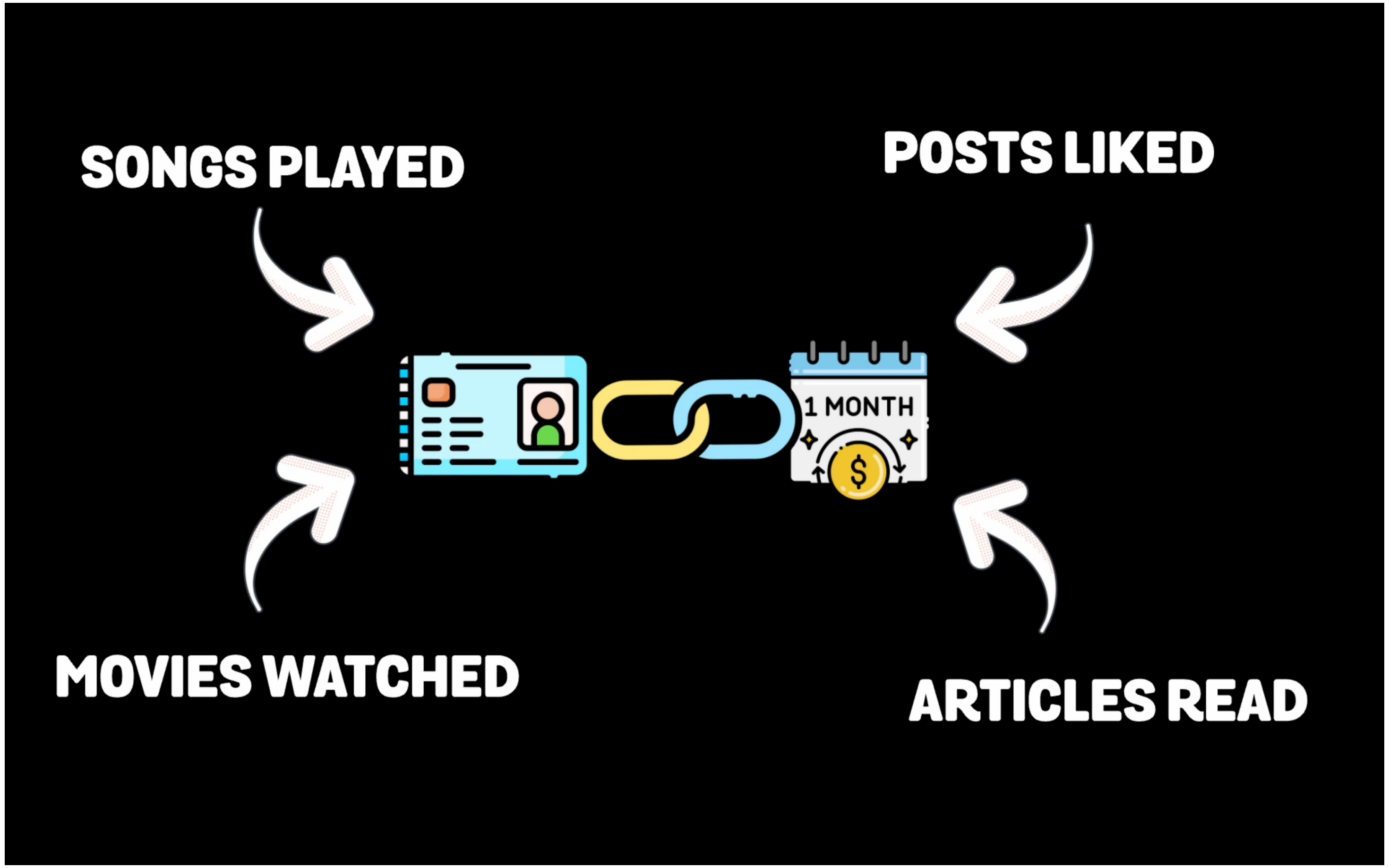
August 29, 2023 12:00AM EDT

Saudi Arabia: Man Sentenced to Death for Tweets

Peaceful Criticism on Social Media Brings Death Penalty

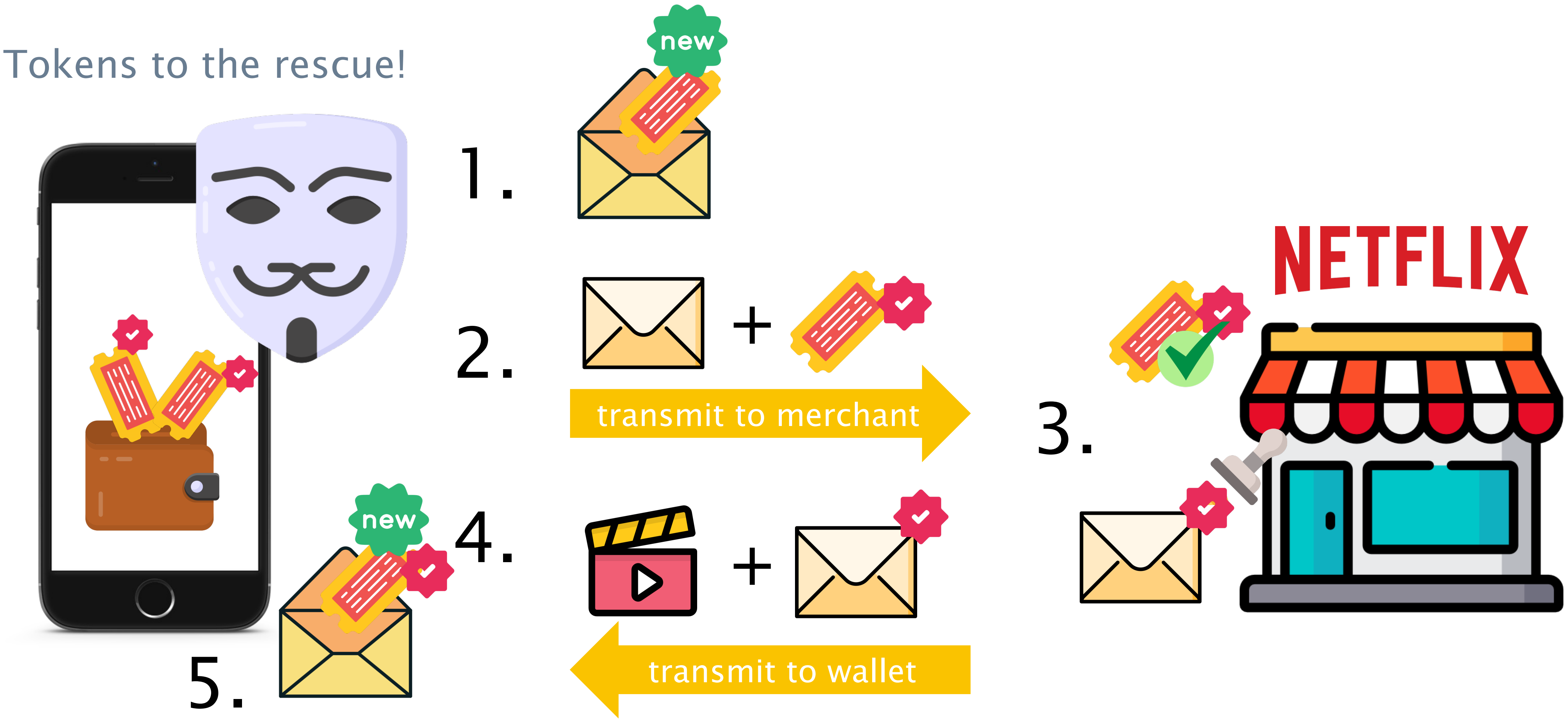
Core problem

Subscription are linked to accounts



Solution

Tokens to the rescue!



1.

2.

transmit to merchant

3.

4.

transmit to wallet

5.

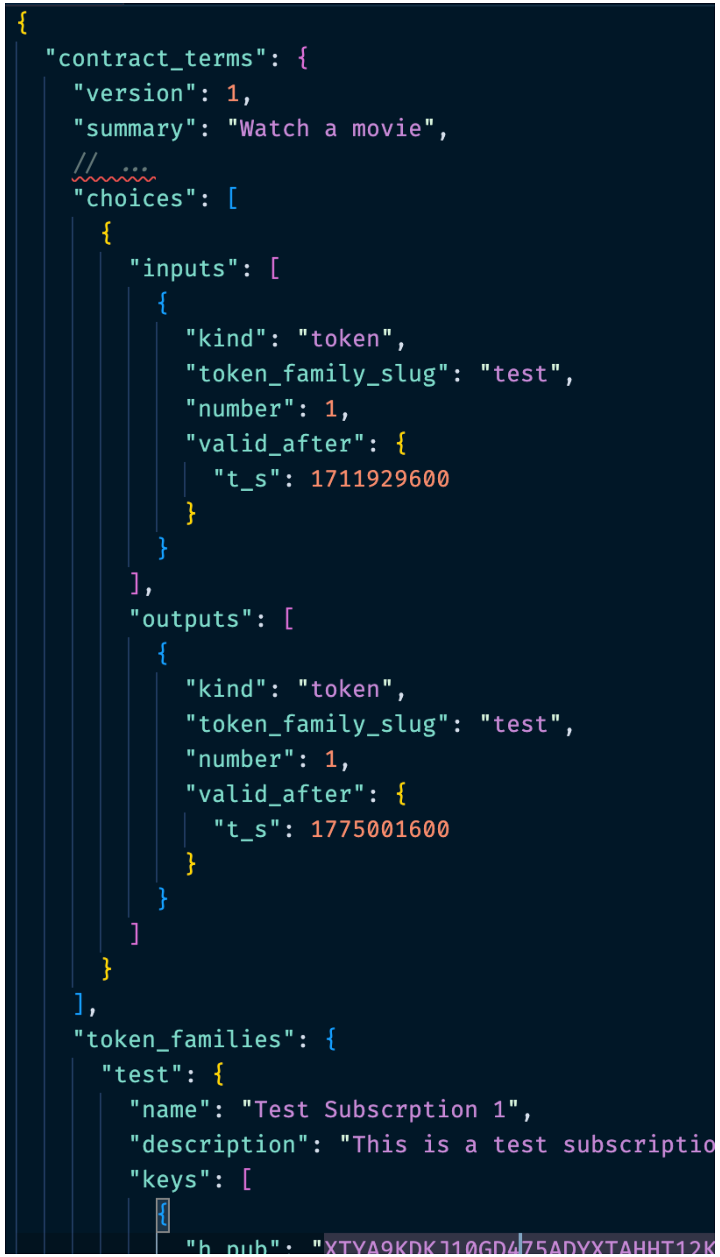
Solution

- What is a token?
  - Key pair generated by wallet (token use key)
  - Issue signature made by merchant (with token issue key)
  - Single-use (merchant remembers)
- What is a token envelope?
  - Blinded hash of token use public key
  - Wallet must remember blinding secret
- Blind signatures
  - Carbon paper lined envelope
- Contract terms
  - Choices (multi currency, sell-ups, discounts, subscriptions, ...)
  - Issue public keys of token families

Solution

0. Wallet claims order

- POST /orders/<ORDER_ID>/claim
  - Provide *nonce* and *token* in body
  - Contract terms in response

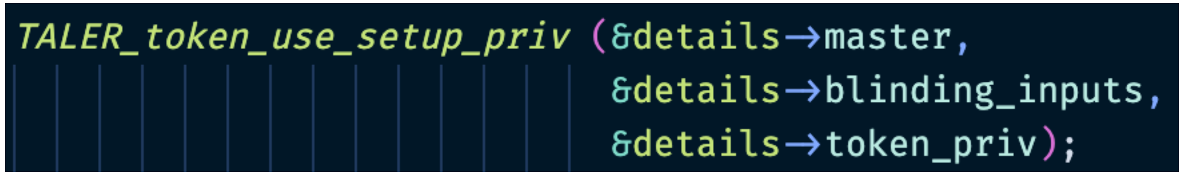


```
{
  "contract_terms": {
    "version": 1,
    "summary": "Watch a movie",
    // ...
    "choices": [
      {
        "inputs": [
          {
            "kind": "token",
            "token_family_slug": "test",
            "number": 1,
            "valid_after": {
              "t_s": 1711929600
            }
          }
        ],
        "outputs": [
          {
            "kind": "token",
            "token_family_slug": "test",
            "number": 1,
            "valid_after": {
              "t_s": 1775001600
            }
          }
        ]
      }
    ],
    "token_families": {
      "test": {
        "name": "Test Subscrption 1",
        "description": "This is a test subscriptio
        "keys": [
          {
            "h_pub": "XTYA9KDKJ10GD475ADYXTAHHT12K
```

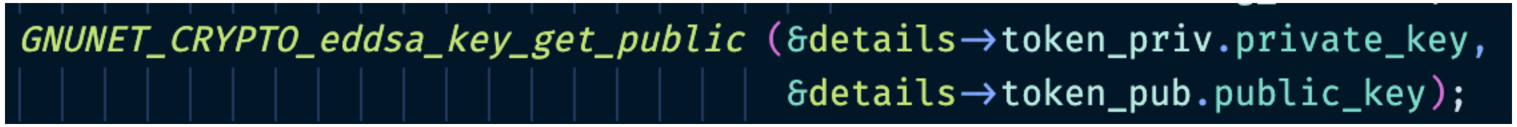
Solution

1. Wallet prepares token envelope

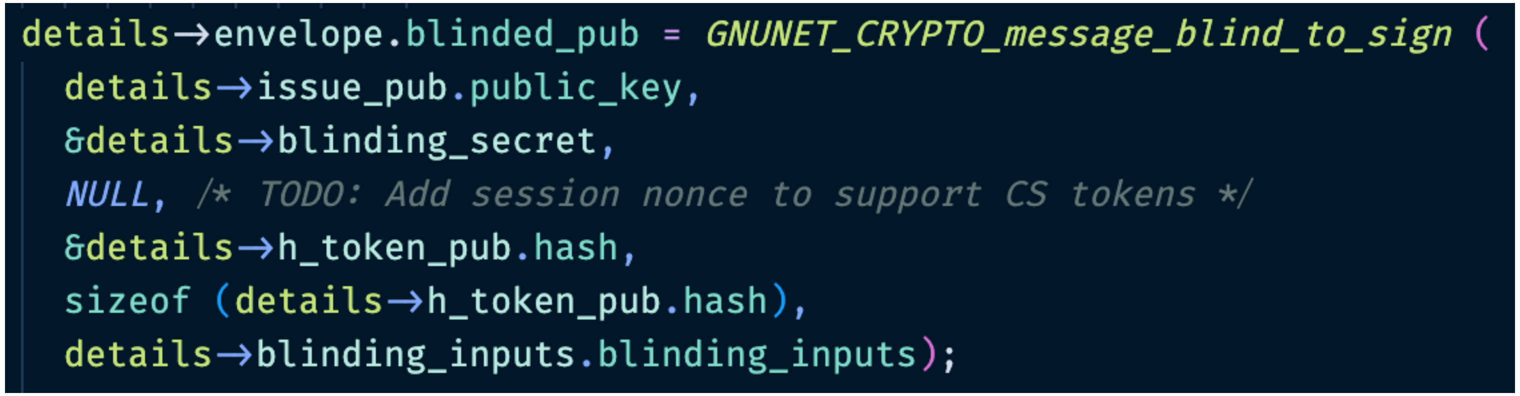
- Generate key pair
- Hash, then blind public key
    - Token issue public key from contract terms



```
TALER_token_use_setup_priv (&details->master,
                            &details->blinding_inputs,
                            &details->token_priv);
```



```
GNUNET_CRYPTO_eddsa_key_get_public (&details->token_priv.private_key,
                                    &details->token_pub.public_key);
```

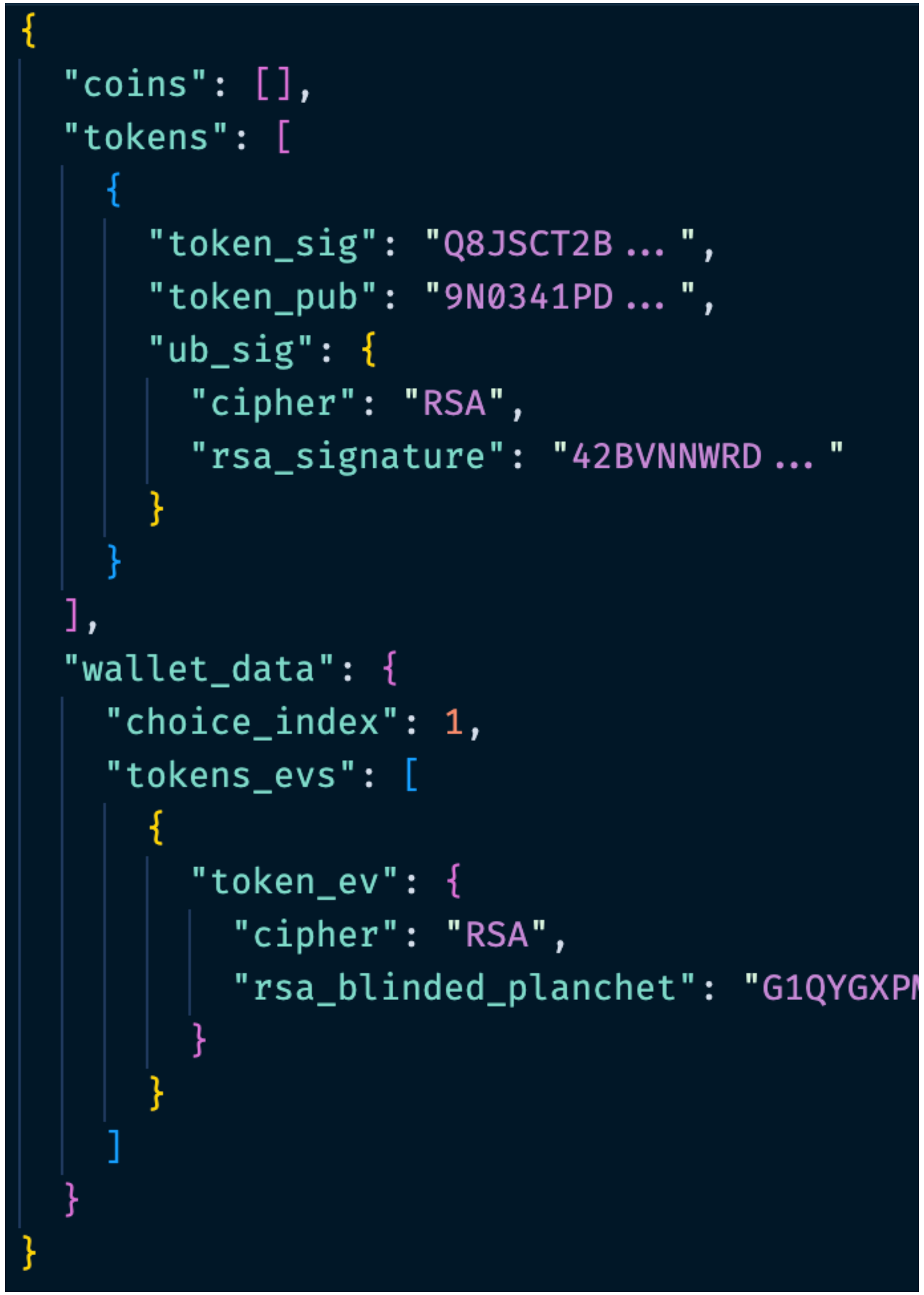


```
details->envelope.blinded_pub = GNUNET_CRYPTO_message_blind_to_sign (
  details->issue_pub.public_key,
  &details->blinding_secret,
  NULL, /* TODO: Add session nonce to support CS tokens */
  &details->h_token_pub.hash,
  sizeof (details->h_token_pub.hash),
  details->blinding_inputs.blinding_inputs);
```

Solution

2. Transmit token + token envelope to merchant

- Sign contract terms with token use private key
  - Token use signature
  - Includes token envelope (commitment)
- POST /orders/<ORDER_ID>/pay
  - Provide *choice_index*, *tokens_evs*, *tokens*

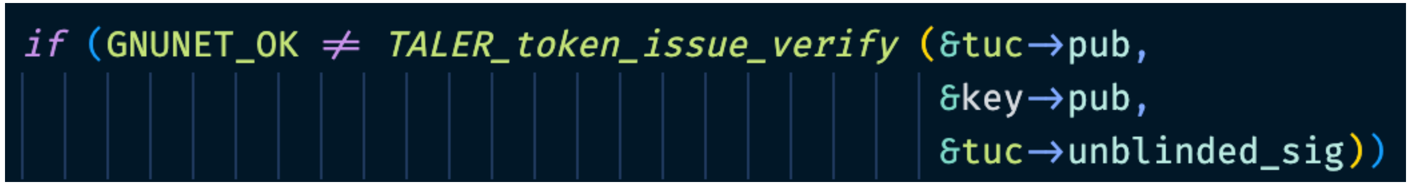


```json
{
  "coins": [],
  "tokens": [
    {
      "token_sig": "Q8JSCT2B...",
      "token_pub": "9N0341PD...",
      "ub_sig": {
        "cipher": "RSA",
        "rsa_signature": "42BVNNWRD..."
      }
    }
  ],
  "wallet_data": {
    "choice_index": 1,
    "tokens_evs": [
      {
        "token_ev": {
          "cipher": "RSA",
          "rsa_blinded_planchet": "G1QYGXP
        }
      }
    ]
  }
}
```

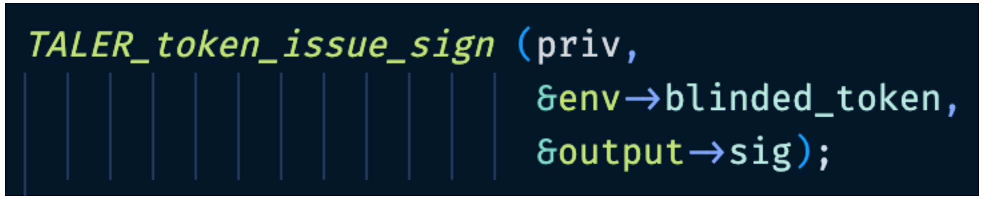
Solution

3. Verify tokens + sign token envelope

- Merchant verifies provided input token
  - For selected choice
- Signs provided token envelopes



```
if (GNUNET_OK != TALER_token_issue_verify (&tuc->pub,
                                           &key->pub,
                                           &tuc->unblinded_sig))
```

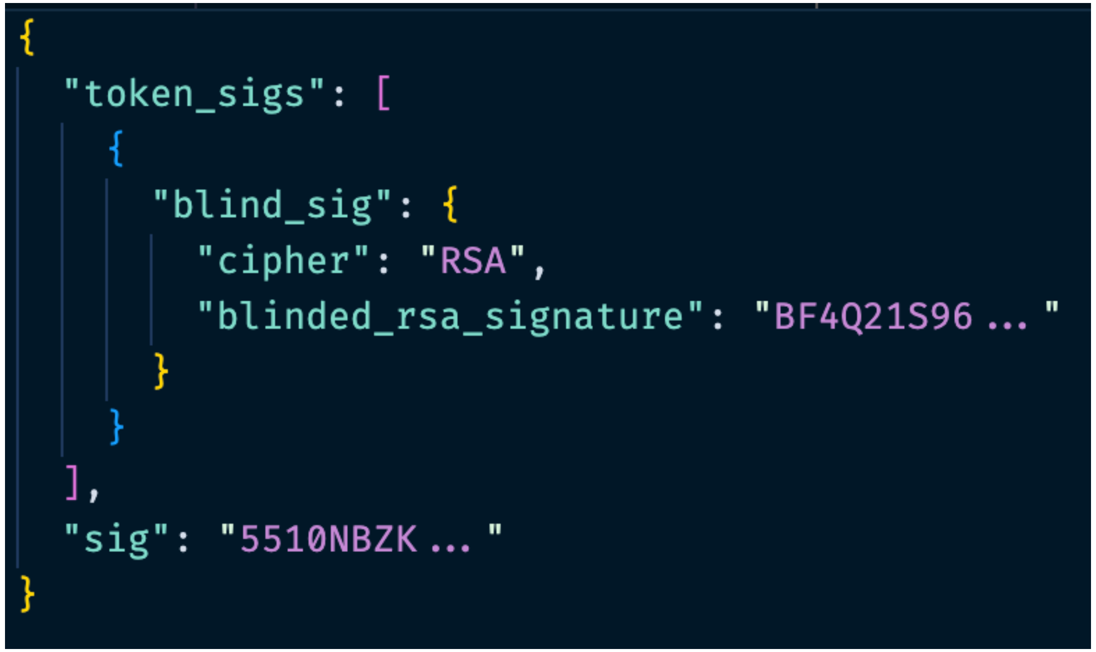


```
TALER_token_issue_sign (priv,
                        &env->blinded_token,
                        &output->sig);
```

Solution

4. Respond with signed token envelopes

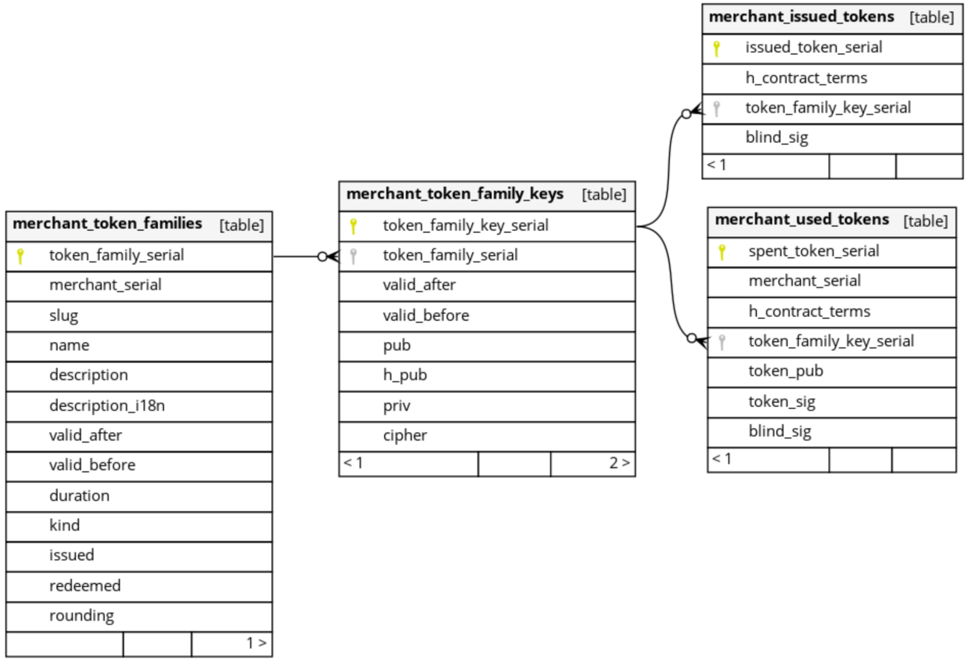
- POST /orders/<ORDER_ID>/pay
  - Blindly signed, fresh tokens in response



```
{
  "token_sigs": [
    {
      "blind_sig": {
        "cipher": "RSA",
        "blinded_rsa_signature": "BF4Q21S96 ... "
      }
    }
  ],
  "sig": "5510NBZK ... "
}
```

Database

- Added four new tables
  - merchant_token_families
    - Represents a subscription or discount
  - merchant_token_family_keys
    - Represents a subscription period
    - <u>Defines the anonymity set</u>
  - merchant_issued_tokens
    - Blindly (!) signed token envelopes
  - merchant_used_tokens
    - Prevent double spending



merchant_token_families [table]
token_family_serial
merchant_serial
slug
name
description
description_i18n
valid_after
valid_before
duration
kind
issued
redeemed
rounding
1 >

merchant_token_family_keys [table]
token_family_key_serial
token_family_serial
valid_after
valid_before
pub
h_pub
priv
cipher
< 1
2 >

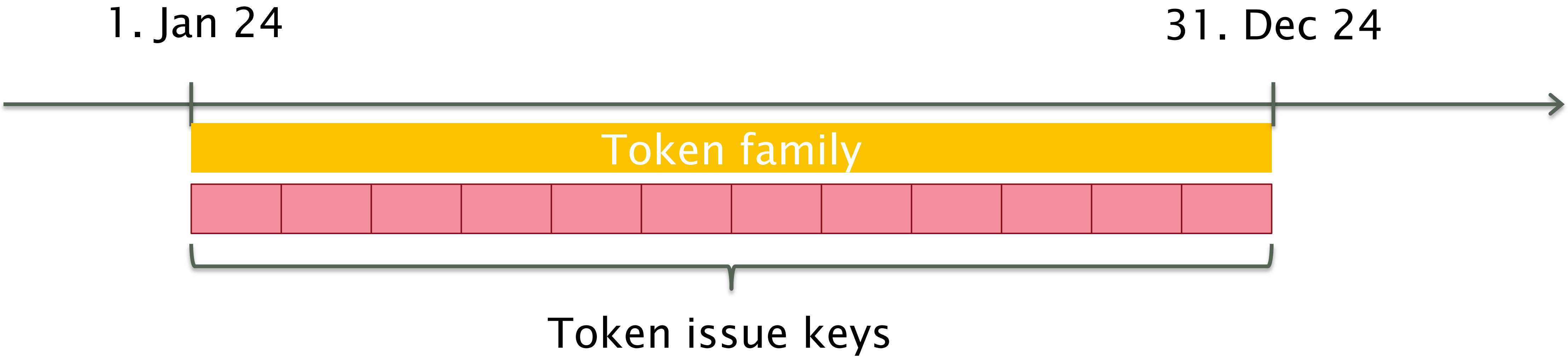
merchant_issued_tokens [table]
issued_token_serial
h_contract_terms
token_family_key_serial
blind_sig
< 1

merchant_used_tokens [table]
spent_token_serial
merchant_serial
h_contract_terms
token_family_key_serial
token_pub
token_sig
blind_sig
< 1

Generated by SchemaSpy

Anonymity set

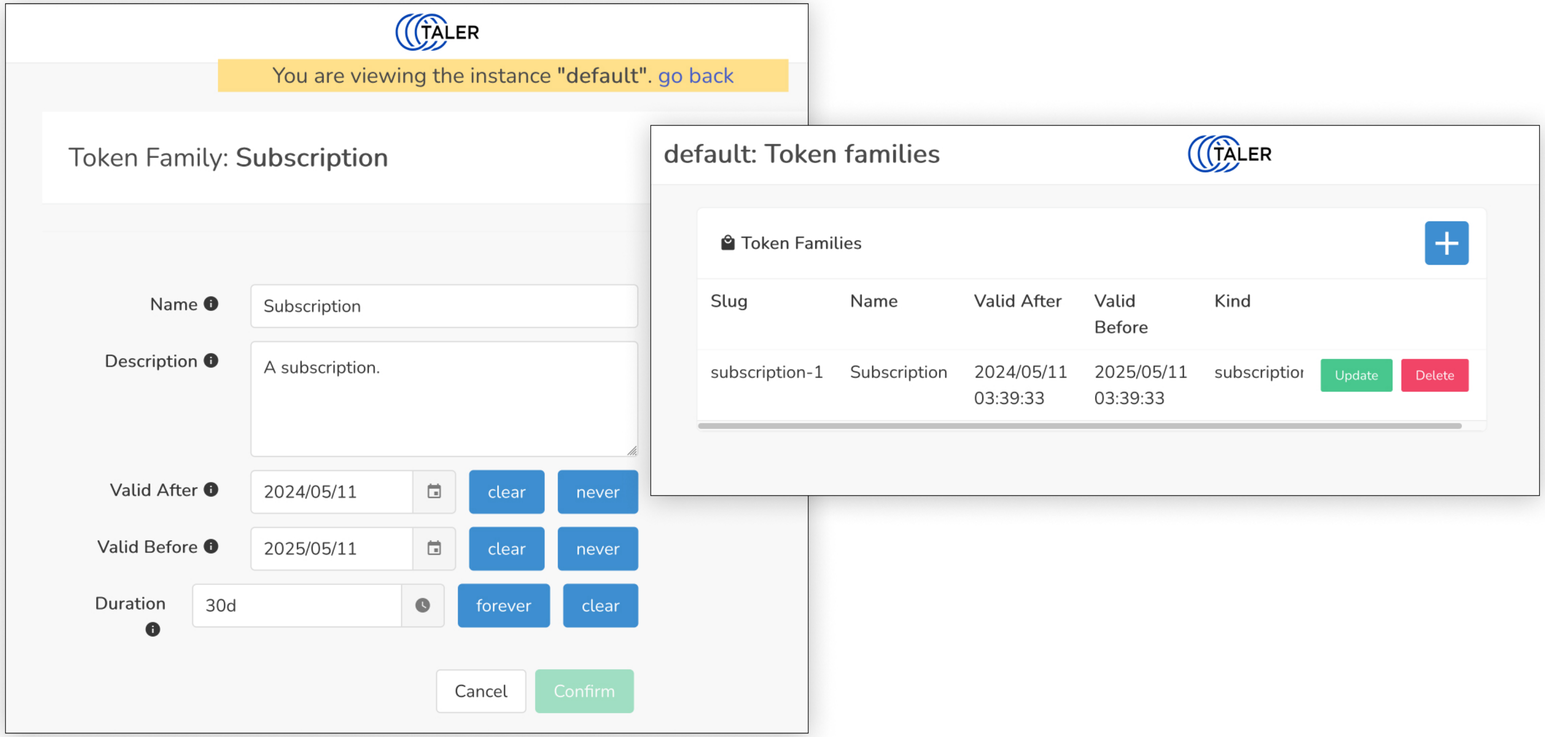
- The size of the anonymity set determines the degree of anonymity
- Tokens are anonymous within the set of all tokens signed by the same token family key
  - Rounding of token start date



Management UI

Aka. Merchant Backoffice UI

- For merchant staff, to manage…
  - …token families
  - …orders
  - etc



You are viewing the instance "default". go back

Token Family: **Subscription**

Name: Subscription

Description: A subscription.

Valid After: 2024/05/11

Valid Before: 2025/05/11

Duration: 30d

default: Token families

Token Families

Slug	Name	Valid After	Valid Before	Kind		
subscription-1	Subscription	2024/05/11 03:39:33	2025/05/11 03:39:33	subscriptioı	Update	Delete

Other use cases

- Loyalty programs
  - Coop Supercard
  - Migros Cumulus
- Memberships
  - ~~Student card~~
- Multi-entry ticketing
  - Festival, concerts, …
- Event deposit system
- Unlinkable gifts
  - 100% discount code

Limitations (design compromises)

- Subscription backups
  - Due to unlinkability
- Termination of single subscription and free trials
  - Due to anonymity
- Browser fingerprinting
  - Use privacy enhancing browser (settings)
- Anonymity set size
  - ASS authority

Future work

- Wallet integration
  - Backups (?)
- ASS authority
- Other ciphers
  - Verifiable credentials

Conclusion

- Not all goals achieved
  - Limited time
  - More complexity than originally planned for (as always...)
- Well-documented solution
  - Thesis, video, poster, one-pager, docs.taler.net
- Implementation in merchant
- API test that emulate wallet

Outlook

- Internet is heavily reliant on advertising
  - Journalism as well
- Many more things can be tokenized
  - Stocks, index funds, securities, …
- Multi-input-multi-output contracts are flexible and powerful
  - Dividends, voting tokens, …
- A (very) small piece in a much larger puzzle aimed at reshaping the digital economy

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Discussion & questions

Thank you for your attention and efforts during my bachelor thesis project.