
Rensselaer

why not change the world?®

# Account Recovery in Decentralized Applications

Yanlin Zhu, Lirong Xia, Oshani Seneviratne

# Overview

- Motivation
- Account Recovery Process
- Methodology

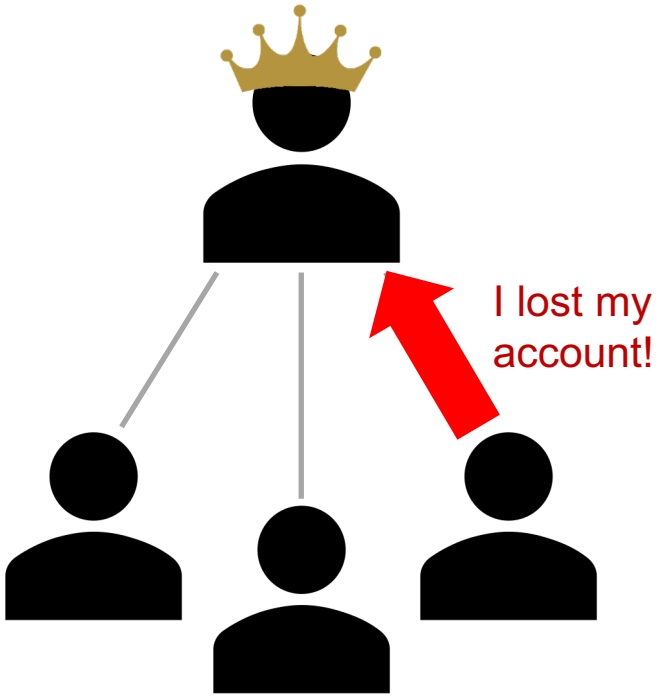
# Hyperledger

- A **permissioned** distributed ledger network

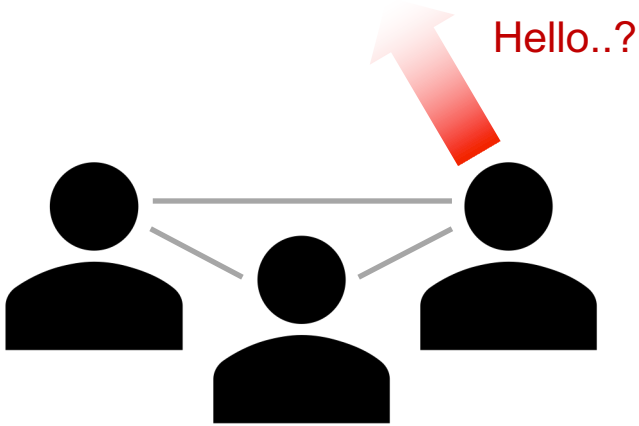
# Hyperledger

- Smart Contract / Chaincode
- Transaction
- Asset

# Motivation




Centralized




Decentralized

# Basic Idea

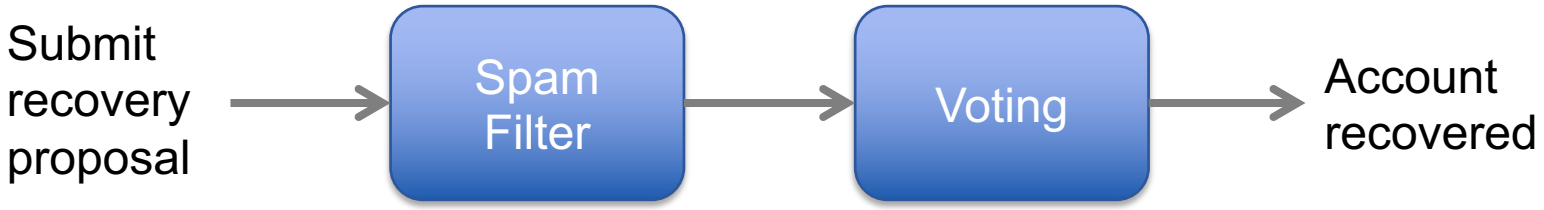
*Public Ledger*
*A sent B 1000 coins*


Account owner

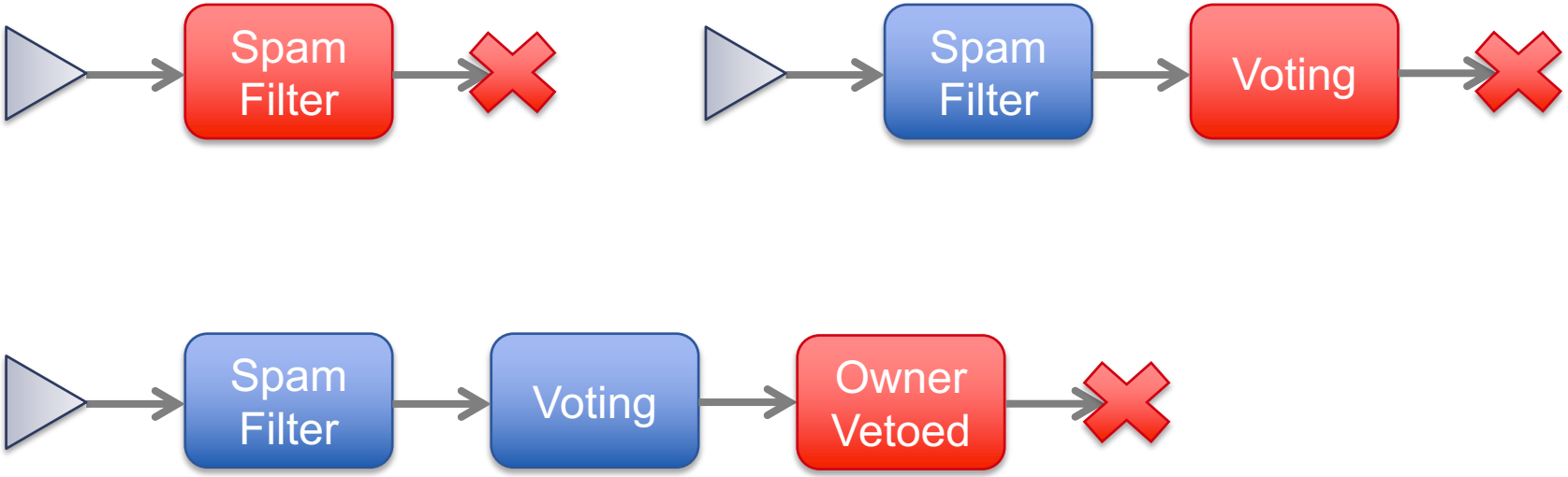

Trade partner


Other users

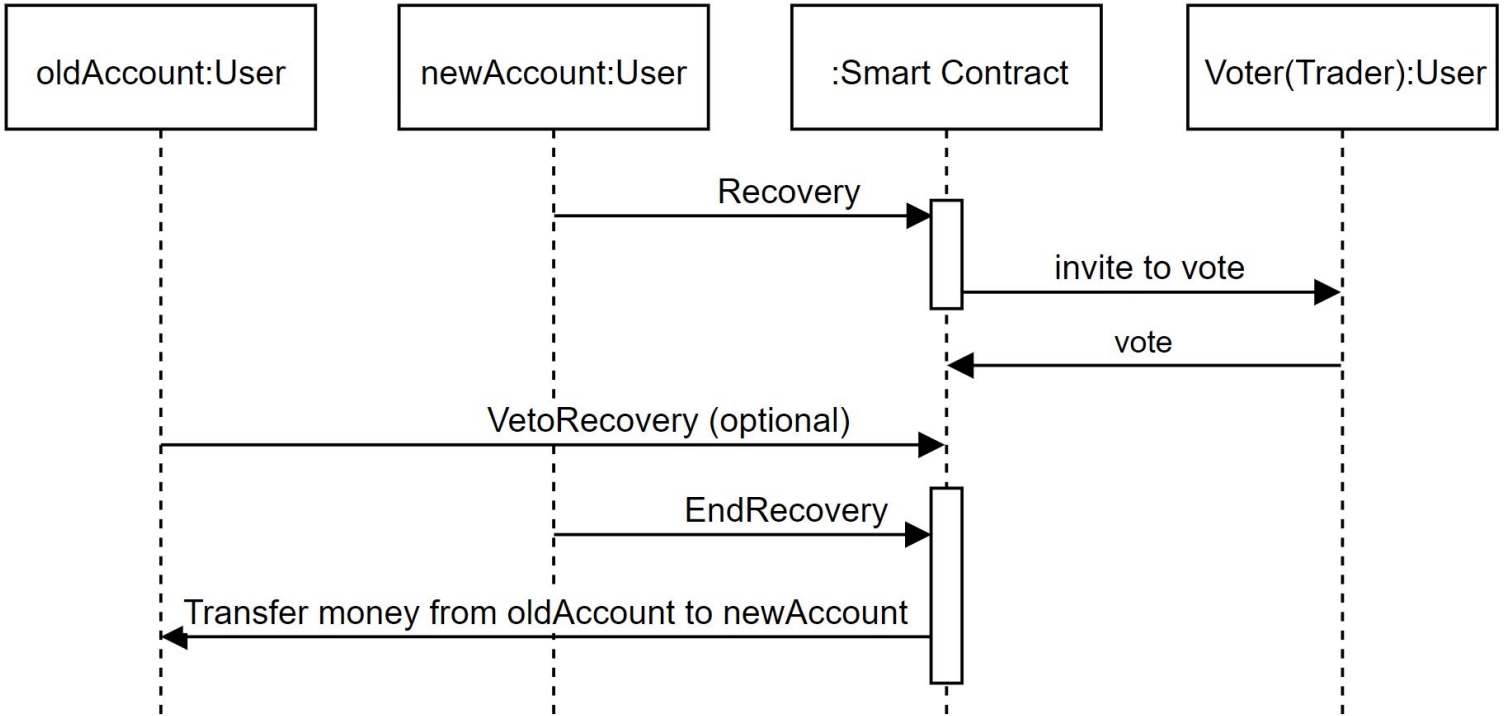
# Account Recovery Process



# Account Recovery Process



# Account Recovery Process

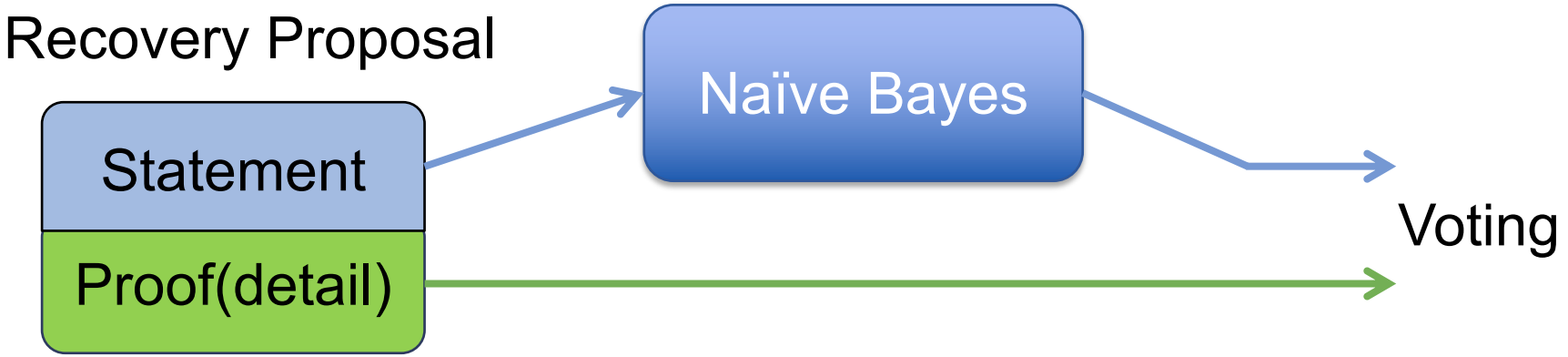


# Potential Attacks

- 51% Attack as a trader

- Social engineering

# Spam Filter





```
{
  "$class": "org.example.basic.Proposal",
  "proposalID": "Recovery-user0-1",
  "statementOS": "I just realized that I lost my account.",
  "detail": "{'6317648c119084ddbd7b317b6e753f7d1a513d641510003068dd4c7b6f983b9
  "newAccount": "user6",
  "oldAccount": "user0",
  "detailpoll": "Poll-Recovery-user0-1",
  "stage": "Concluded",
  "votingReward": 100,
  "owner": "resource:org.example.basic.User#user0"
}
```

```
{
  "$class": "org.example.basic.NBclassifier",
  "nbclassifierID": "recoveryClassifier",
  "jsondata": "{'categories':{'spam':true,'ham':true},'docCount':
{'spam':214,'ham':214},'totalDocuments':428,'feature':
{'the':true,'chicago':true,'hotel':true,'i':true,'a':true,'great':
true,'of':true,'my':true,'was':true,'for':true,'stay':true,'at':tr
ue,'in':true,'is':true,'to':true,'as':true,'it':true,'and':true,'h
ad':true,'from':true,'very':true,'staff':true,'with':true,'rooms':
true,'room':true,'would':true,'not':true,'there':true,'were':true,
'so':true,'that':true,'all':true,'':true,'num=0':true,'second-
person=0%':true,'stayed':true,'this':true,'have':true,'our':true,'
we':true,'they':true,'location':true,'but':true,'on':true,'t':true
,'are':true,'you':true},'featureSize':47,'wordCount':
{'spam':12126,'ham':12627},'wordFrequencyCount':{'spam':
```

# Voting

- C: correct vote reward
- W: incorrect vote reward
- t: cost of time

$$Reward_{Authentic} = \frac{\sum_{n=v_c}^{v_r} \binom{v_r}{n}}{2^{v_r}} * C + \frac{\sum_{n=0}^{v_c-1} \binom{v_r}{n}}{2^{v_r}} * W - t$$

$$Reward_{Random} = \frac{1}{2}\left(\frac{\sum_{n=v_c}^{v_r} \binom{v_r}{n}}{2^{v_r}} * C + \frac{\sum_{n=0}^{v_c-1} \binom{v_r}{n}}{2^{v_r}} * W\right) + \frac{1}{2}\left(\frac{\sum_{n=0}^{v_c} \binom{v_r}{n}}{2^{v_r}} * C + \frac{\sum_{n=v_c+1}^{v_r} \binom{v_r}{n}}{2^{v_r}} * W\right)$$

# Short Demo

## User Asset before the recovery

user0


```
{
  "$class": "org.example.basic.User",
  "userId": "user0",
  "name": "Alice",
  "pubKey": "768979afacd26b9ec601d77092fc16a0f74706a5d3acfac5a218763fe72c875712
  "aCoin": 1000,
```


Show All

user1


```
{
  "$class": "org.example.basic.User",
  "userId": "user1",
  "name": "Bob",
  "pubKey": "6317648c119084ddbd7b317b6e753f7d1a513d64151003068dd4c7b6f983b99282
  "aCoin": 1000,
```


Show All

user2


```
{
  "$class": "org.example.basic.User",
  "userId": "user2",
  "name": "Chloe",
  "pubKey": "7ba7111744d808dbb11fd70150b6107de61acc9b073f52ee9b79b92912d81db2f5
  "aCoin": 1000,
```


Show All

user3


```
{
  "$class": "org.example.basic.User",
  "userId": "user3",
```


## User ACoin amount

- Alice: 1000 — Original Account
- Bob: 1000
- Chloe: 1000
- David: 1000
- Ethan: 1000
- Frank: 1000

Voters

- Alice (new): 200 — Recovery Initiator

# Short Demo

## Prepare to submit **Recovery** transaction

Write Proof

Write proof for
6317648c119084ddbd7b317b6e753f7d1a513d64151003068dd4c7b6f983b992821c49a4ea25bd43e674ae9567870698c40586286dc89f935d58eba0d

I bought car from Bob

Write proof for
7ba7111744d808dbb11fd70150b6107de61acc9b073f52ee9b79b92912d81db2f5a1755d9a777c80595de46c0aa1644db302fb07db9cf2e9d9356cdcb

I sold an apartment to Chloe

Write proof for
b1972cdbf5e7ea805faaa8eee277caae778c8630943bdcbdcef37b81b7eed85fa1de9d9e9fc23cca45b98e0f22bf1920d578994c50ec43c6c6f5c2485

I ate at David's restaurant

Write proof for
479a84cdced9015dd2e75f820173d1f1c8fc9869a54fb5a1409bfe7ddc502ae836d47fb8aadcdc8d2b6351272aceee7e98fe26059895ba9d548c24628

I paid my debt to Ethan

Write proof for
9302c7fa0c7a4f746c6430f2151e80cf0891c5d004560cedfc7c76bfbc24b6526d8fc7d60829e6926deec64182a7f086bcf3f25d03cc4ed33cb77b531

I worked for Frank as a home teacher

Submit recovery proof

Encrypted result below: (submit in the "detail" field in the proposal)

{'6317648c119084ddbd7b317b6e753f7d1a513d64151003068dd4c7b6f983b992821c49a4ea25bd43e674ae9567870698c40586286dc89f935d58eba0d5759ce1':'3d58ab346dbcda37eded6279602e78003604a1d2df4ba0d5c778d29de7732b0e945a02fc6827a51e6c75caa40d9d9e9be9b9187edc4ad0801b128dc58d725457','7ba7111744d808dbb11fd70150b6107de61acc9b073f52ee9b79b92912d81db2f5a1755d9a777c80595de46c0aa1644db302fb07db9cf2e9d9356cdcb7fdf70b':'4d5540d9289b1795574897d030019b401d53595e3a4732e1105c8cee250653c6876b05d21b55e0332a9b3098ade2ea6d4e9b90bbb24098575495d6b4c9e1399b','b1972cdbf5e7ea805faaa8eee277caae778c8630943bdcbdcef37b81b7eed85fa1de9d9e9fc23cca45b98e0f22bf1920d578994c50ec43c6c6f5c24859bb1479':'ab95a5c6a29f9b30ec163e6a04b38229856e98324252f0f787821a3c4d4e75a4612084e033128ee601991a3f8ba75a6323ae8ff0346bcd810af2d7d53a3fe3a9','479a84cdced9015dd2e75f820173d1f1c8fc9869a54fb5a1409bfe7ddc502ae836d47fb8aadcdc8d2b6351272aceee7e98fe26059895ba9d548c24628e121af1':'1d79c58ea097273246476e1c806b052b68dc75f73c102992676838389b7d52df610521fcc0699914a8cfa37ff30f5911b8232b246a5db55c8a955c7d2dff3baa','9302c7fa0c7a4f746c6430f2151e80cf0891c5d004560cedfc7c76bfbc24b6526d8fc7d60829e6926deec64182a7f086bcf3f25d03cc4ed33cb77b53148d02f5':'42f0e3f848a850c47505861fef64f6a038e20d2c33387ae6b938997a3dc29cdd9bff963d2a724606ce367fb7a061eed729aecf418fc44825f61f2fd73d875b29'}

## User ACoin amount

- Alice: 1000 — Original Account
- Bob: 1000
- Chloe: 1000
- David: 1000 — Voters
- Ethan: 1000
- Frank: 1000
- Alice (new): 0 — Recovery Initiator

# Short Demo

## After the Recovery transaction is submitted

Recovery-user0-1


```
{
  "$class": "org.example.basic.Proposal",
  "proposalID": "Recovery-user0-1",
  "statementOS": "I just realized that I lost my account.",
  "detail": "{'6317648c119084ddbd7b317b6e753f7d1a513d64151003068dd4c7b6f983b9
  "newAccount": "user6",
  "oldAccount": "user0",
  "detailpoll": "Poll-Recovery-user0-1",
  "stage": "Voting",
  "votingReward": 100,
  "owner": "resource:org.example.basic.User#user0"
}
```


Collapse

Recovery Proposal created in Asset

## User ACoin amount

- Alice: 1000 — Original Account
- Bob: 1000
- Chloe: 1000
- David: 1000 — Voters
- Ethan: 1000
- Frank: 1000
- Alice (new): 0 — Recovery Initiator

# Short Demo

## Voter vote based on decrypted proof

Paste the "detail" field in the proposal in the textbox

{'6317648c119084ddbd7b317b6e753f7d1a513d64151003068dd4c7b6f983b992821c49a4ea25bd43e674ae9567870698c40586286dc89f935d58eba0d5759ce1':'3d58ab346dbcda37eded6279602e78003604a1d2df4ba0d5c778d29de7732b0e945a02fc6827a51e6c75caa40d9d9e9be9b9187edc4ad0801b128dc58d725457','7ba7111744d808dbb11fd70150b6107de61acc9b073f52ee9b79b92912d81db2f5a1755d9a777c80595de46c0aa1644db302fb07db9cf2e9d9356cdcb7fdf70b':'4d5540d9289b1795574897d030019b401d53595e3a4732e1105c8cee250653c6876b05d21b55e0332a9b3098ade2ea6d4e9b90bbb24098575495d6b4c9e1399b','b1972cdbf5e7ea805faaa8eee277caae778c8630943bdcbdcef37b81b7eed85fa1de9d9e9fc23cca45b98e0f22bf1920d578994c50ec43c6c6f5c24859bb1479':'ab95a5c6a29f9b30ec163e6a04b38229856e98324252f0f787821a3c4d4e75a4612084e033128ee601991a3f8ba75a6323ae8ff0346bcd810af2d7d53a3fe3a9','479a84cdced9015dd2e75f820173d1f1c8fc9869a54fb5a1409bfe7ddc502ae836d47fb8aadcdc8d2b6351272aceee7e98fe26059895ba9d548c24628e121af1':'1d79c58ea097273246476e1c806b052b68dc75f73c102992676838389b7d52df610521fcc0699914a8cfa37ff30f5911b8232b246a5db55c8a955c7d2dff3baa','9302c7fa0c7a4f746c6430f2151e80cf0891c5d004560cedfc7c76bfbc24b6526d8fc7d60829e6926deec64182a7f086bcf3f25d03cc4ed33cb77b53148d02f5':'42f0e3f848a850c47505861fef64f6a038e20d2c33387ae6b938997a3dc29cdd9bff963d2a724606ce367fb7a061eed729aecf418fc44825f61f2fd73d875b29'}

Enter your complete RSA key information below to decrypt

n: 6317648c119084ddbd

e: 10001

d: dceb8a7fbda9369027a

p: c542a13db8a66dfbef4

q: 80993d21b23d28d49e

Decrypt the proof

The decrypted proof for you is

I bought car from Bob

VT-Recovery-user0-1-0


```
{
  "$class": "org.example.basic.VoteToken",
  "votetokenID": "VT-Recovery-user0-1-0",
  "response": "",
  "poll": "resource:org.example.basic.Poll#Poll-Recovery-
  "creator": "resource:org.example.basic.User#user6",
  "voter": "resource:org.example.basic.User#user1",
  "owner": "resource:org.example.basic.User#user1"
}
```


VT-Recovery-user0-1-0


```
{
  "$class": "org.example.basic.VoteToken",
  "votetokenID": "VT-Recovery-user0-1-0",
  "response": "True",
  "poll": "resource:org.example.basic.Poll#Poll-Recovery-
  "creator": "resource:org.example.basic.User#user6",
  "voter": "resource:org.example.basic.User#user1",
  "owner": "resource:org.example.basic.User#user6"
}
```


Collapse

# Short Demo

## **User** Asset after the recovery

user0


```
{
  "$class": "org.example.basic.User",
  "userId": "user0",
  "name": "Alice",
  "pubKey": "768979afacd26b9ec601d77092fc16a0f74706a5d3acfac5a218763fe72c8757
  "aCoin": 0,
```


Show All

user1


```
{
  "$class": "org.example.basic.User",
  "userId": "user1",
  "name": "Bob",
  "pubKey": "6317648c119084ddbd7b317b6e753f7d1a513d64151003068dd4c7b6f983b992
  "aCoin": 1025,
```


Show All

user2


```
{
  "$class": "org.example.basic.User",
  "userId": "user2",
  "name": "Chloe",
  "pubKey": "7ba7111744d808dbb11fd70150b6107de61acc9b073f52ee9b79b92912d81db2
  "aCoin": 1000,
```


Show All

user3

{

## User ACoin amount

- Alice (old): 0
- Bob: 1025, voted True
- Chloe: 1000, voted False
- David: 1025, voted True
- Ethan: 1025, voted True
- Frank: 1025, voted True
- Alice (new): 1100

# Related Works

- Lee et al. (2017)
  - A Robust Identity Recovery Scheme for the Ethereum Blockchain Platform
- Maram et al. (2019)
  - CHURP: Dynamic-Committee Proactive Secret Sharing

# Conclusion

- Contribution
  - A new method for account recovery
    - Voting by previous trade partners
    - Solution is decentralized
    - No action required before recovery
- Future Work
  - Account clustering
  - Other platform

# Questions?

- Project website and Github repo:
  - https://rpi-scales.github.io/account-recovery/