Encointer PoP: security analysis

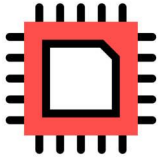
Student: Lucie Hoffmann
Lab: DEDIS
Supervisors: Prof. Bryan Ford, Louis-Henri Merino, Haoqian Zhang

Outline

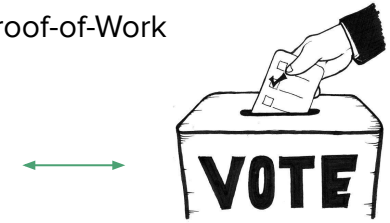
- Proof-of-Personhood (PoP)
- Encointer
- Problematic of this project
- Results

Proof-of-Personhood (PoP)

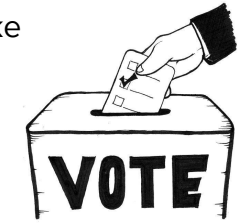
Proof-of-Work

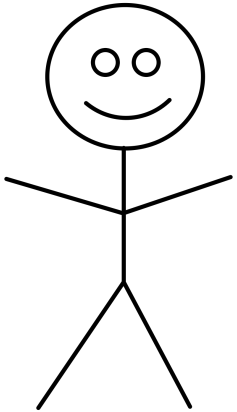


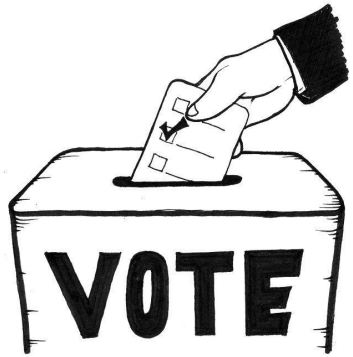
CPU



Proof-of-Stake







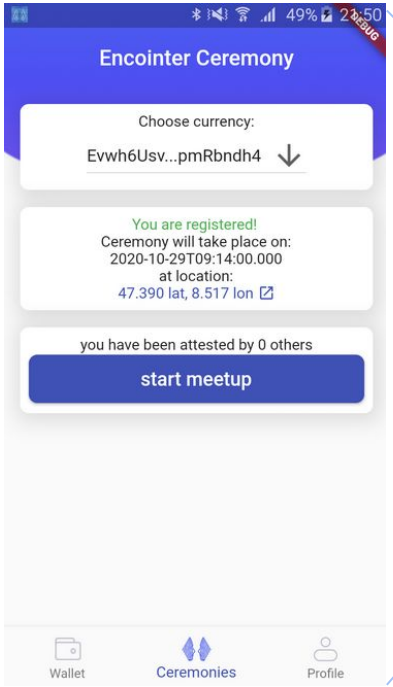
Encointer communities

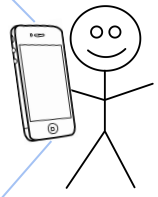
Unique PoP token

Universal Basic Income (UBI)

Local currencies

Encointer





Ceremony

Lausanne community - LauzCoin

- Meetup at Flon
- Meetup at Ouchy

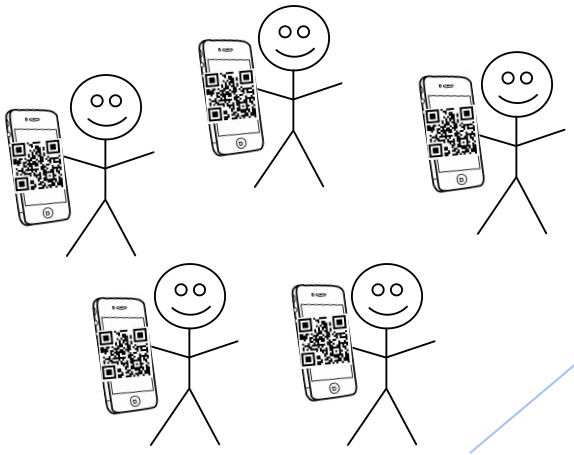
Montreux community - JazzCoin

- Meetup at train station
- Meetup at lake

Zürich community - GrüziCoin

- Meetup at ETH
- Meetup at port

Encointer



Ceremony

Lausanne community - LauzCoin

- Meetup at Flon
- Meetup at Ouchy

Montreux community - JazzCoin

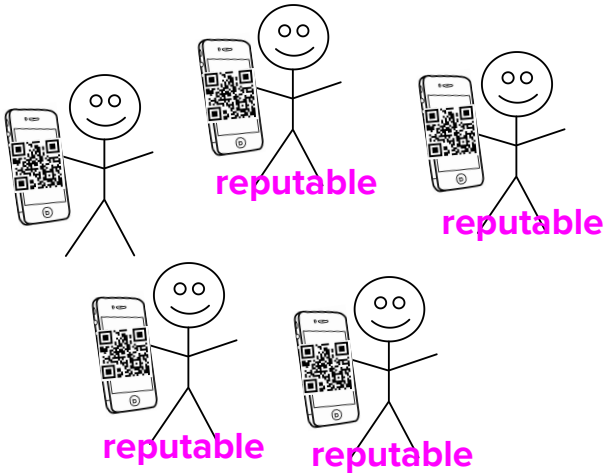
- Meetup at train station
- Meetup at lake

Zürich community - GrüziCoin

- Meetup at ETH
- Meetup at port

Encointer

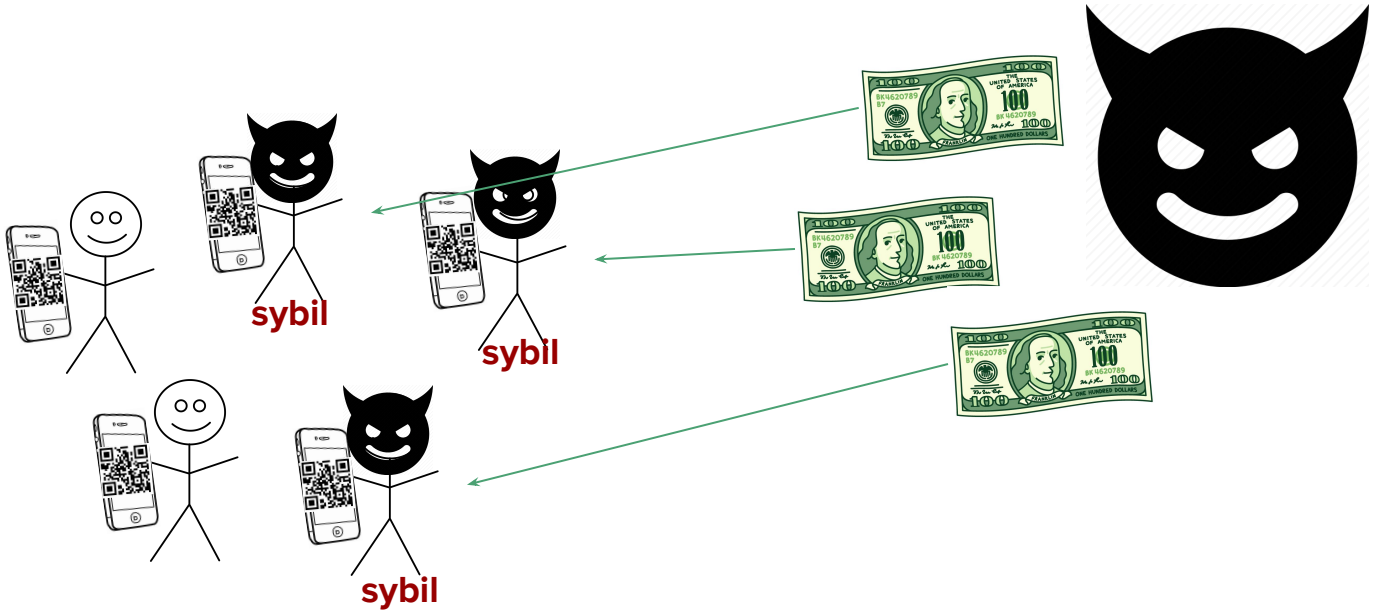
- Reputation: successfully validated in last ceremony
- Meetup: at least ¾ **reputation**
- Validation condition: attested by **at least all reputables but 2**



Outline

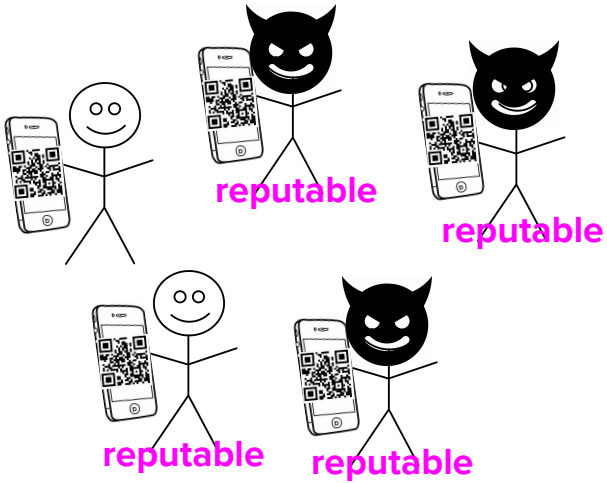
- PoP: great idea
- Encointer: unique PoP token + UBI reward
- Problematic of this project
  - Is sybil attack possible?
- Results

Sybil attack in Encointer



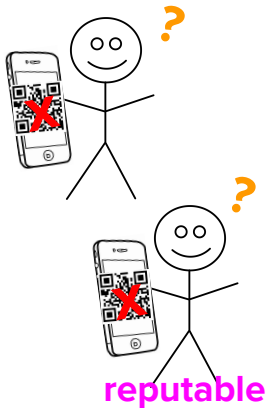
Sybil attack in Encointer

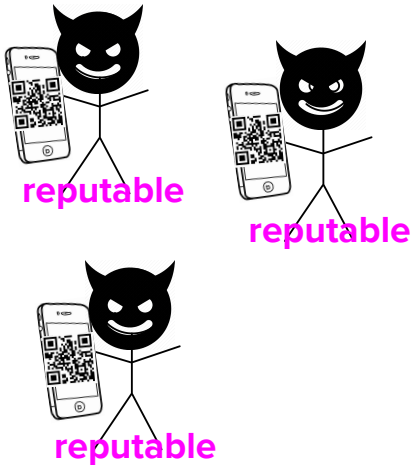
- Reputation: successfully validated in last ceremony
- Meetup: at least ¾ **reputation**
- Validation condition: attested by **at least all reputables but 2**



Sybil attack Encointer

- Reputation: successfully validated in last ceremony
- Meetup: at least ¾ **reputation**
- Validation condition: attested by **at least all reputables but 2**



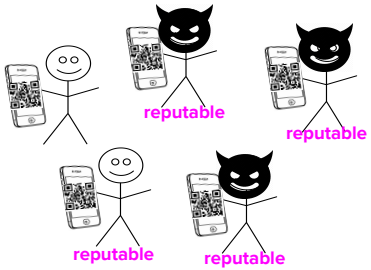


Outline

- PoP: great idea
- Encointer: unique PoP token + UBI reward
- Problematic of this project
  - Is sybil attack possible?
  - Can we make profit from Encointer?
- Results

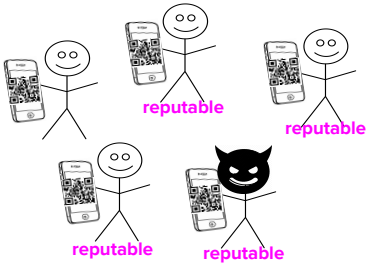
Can we make profit from Encointer?

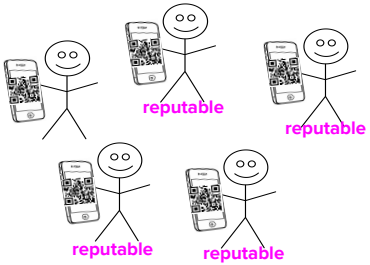
- Probability for a meetup to be controlled by sybils

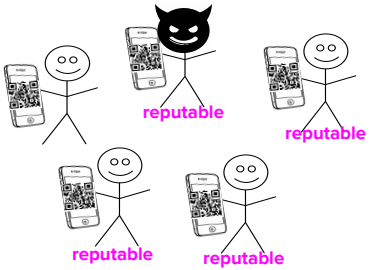


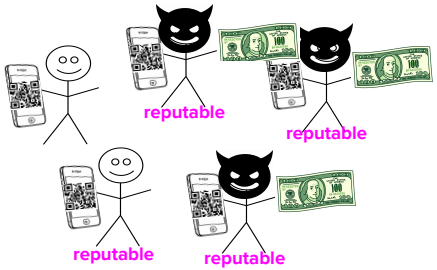
Can we make profit from Encointer?

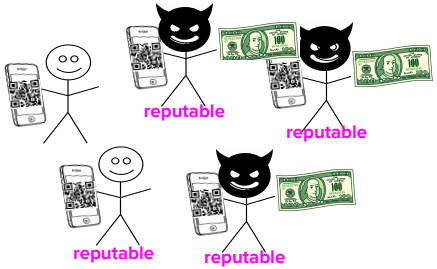
- Probability for a meetup to be controlled by sybils
- Expected profit for a ceremony





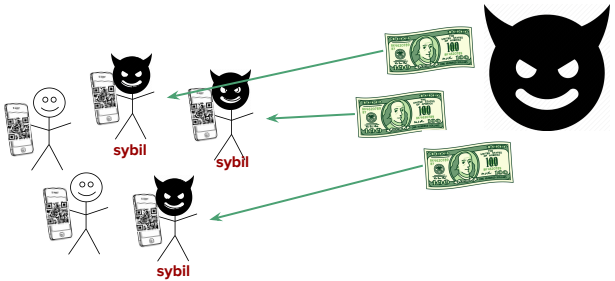






Can we make profit from Encointer?

- Probability for a meetup to be controlled by sybils
- Expected profit for a ceremony
- Evolution of profit over time (several ceremonies)
- Add non-null friction constraint

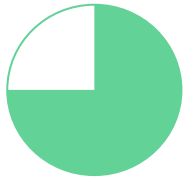


UBI reward = R
Friction factor = f

Sybil cost = R + f*R

Probability for a meetup to be controlled

- Probability to have **at least all reputables but 2** being sybils in a meetup



¾ reputation

Meetup size

=

$$\left\lfloor \frac{\#participants}{\#meetups} \right\rfloor$$

$$\left\lfloor \frac{\#participants}{12} \right\rfloor$$

Need at least

k

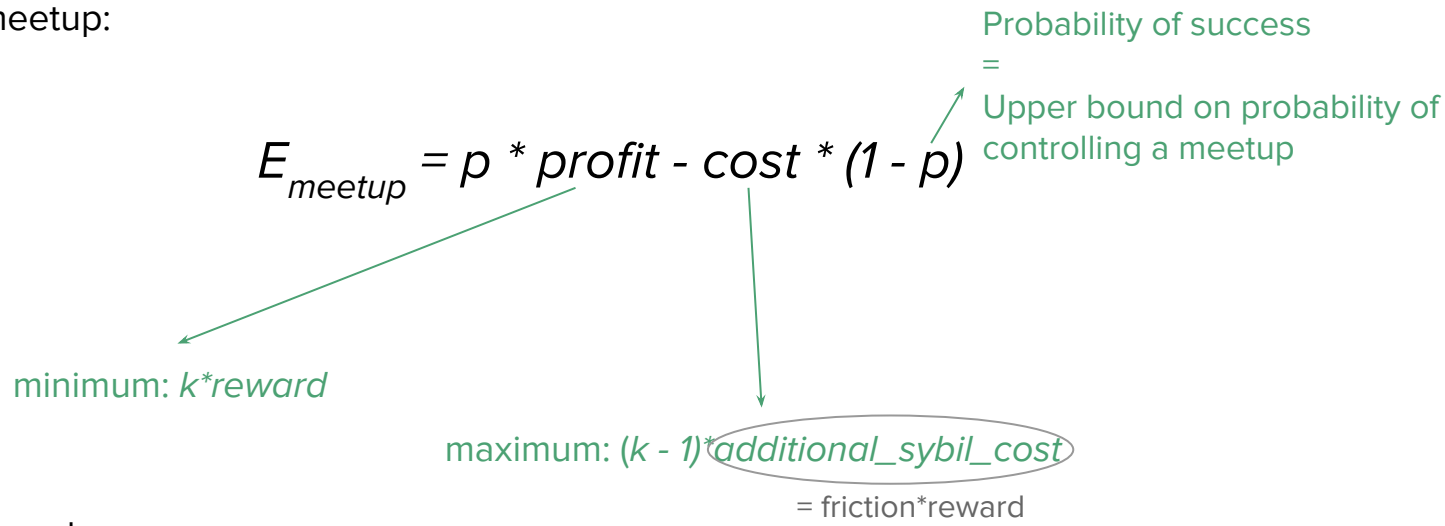
=

¾ * meetup_size - 2

Hypergeometric distribution

Expected profit for a ceremony

For a meetup:



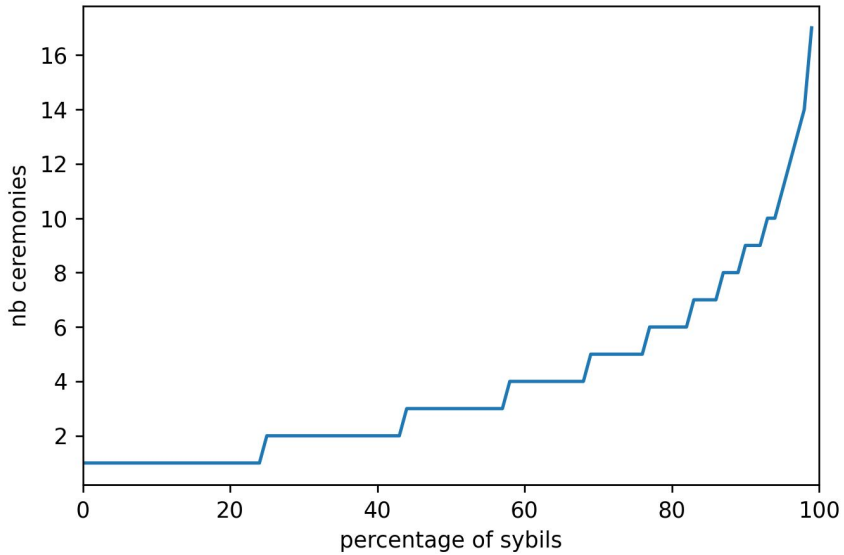
For all meetups:

$$E_{ceremony} = \#meetups * E_{meetup}$$

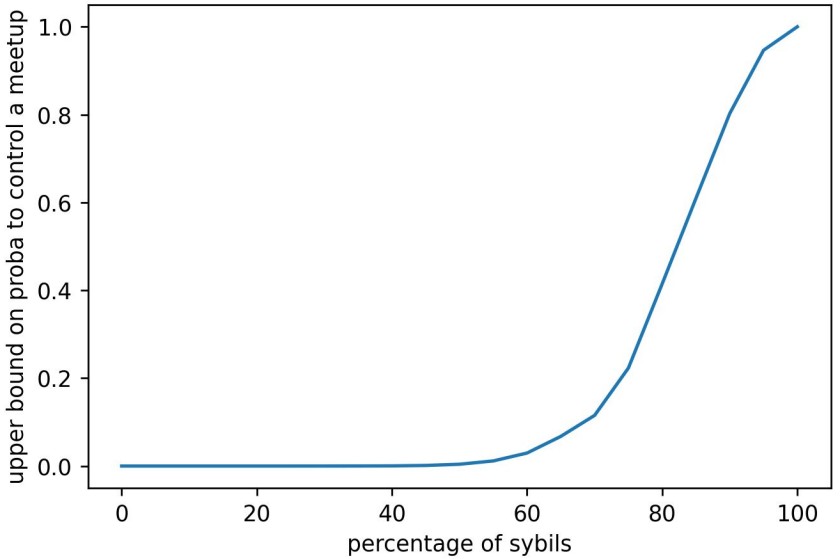
Outline

- PoP: great idea
- Encointer: unique PoP token + UBI reward
- Can we make profit from Encointer?
  - Methodology
- Results

Adversary strategy

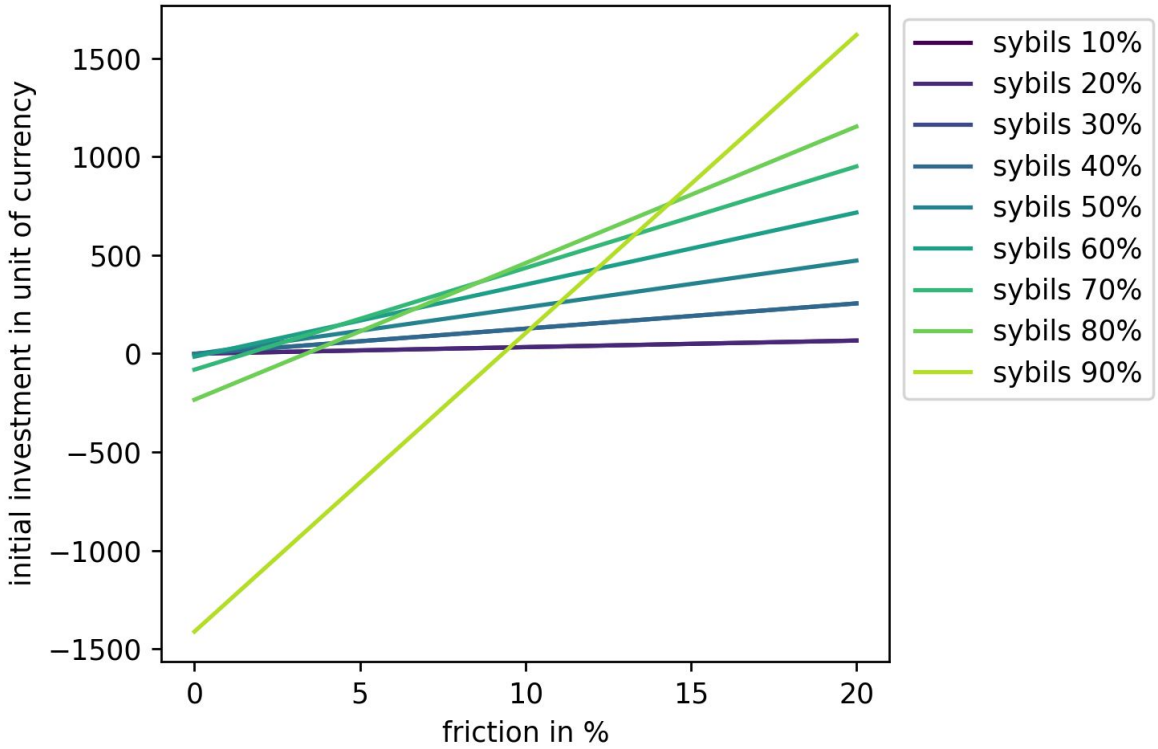


Number of ceremonies to get reputables

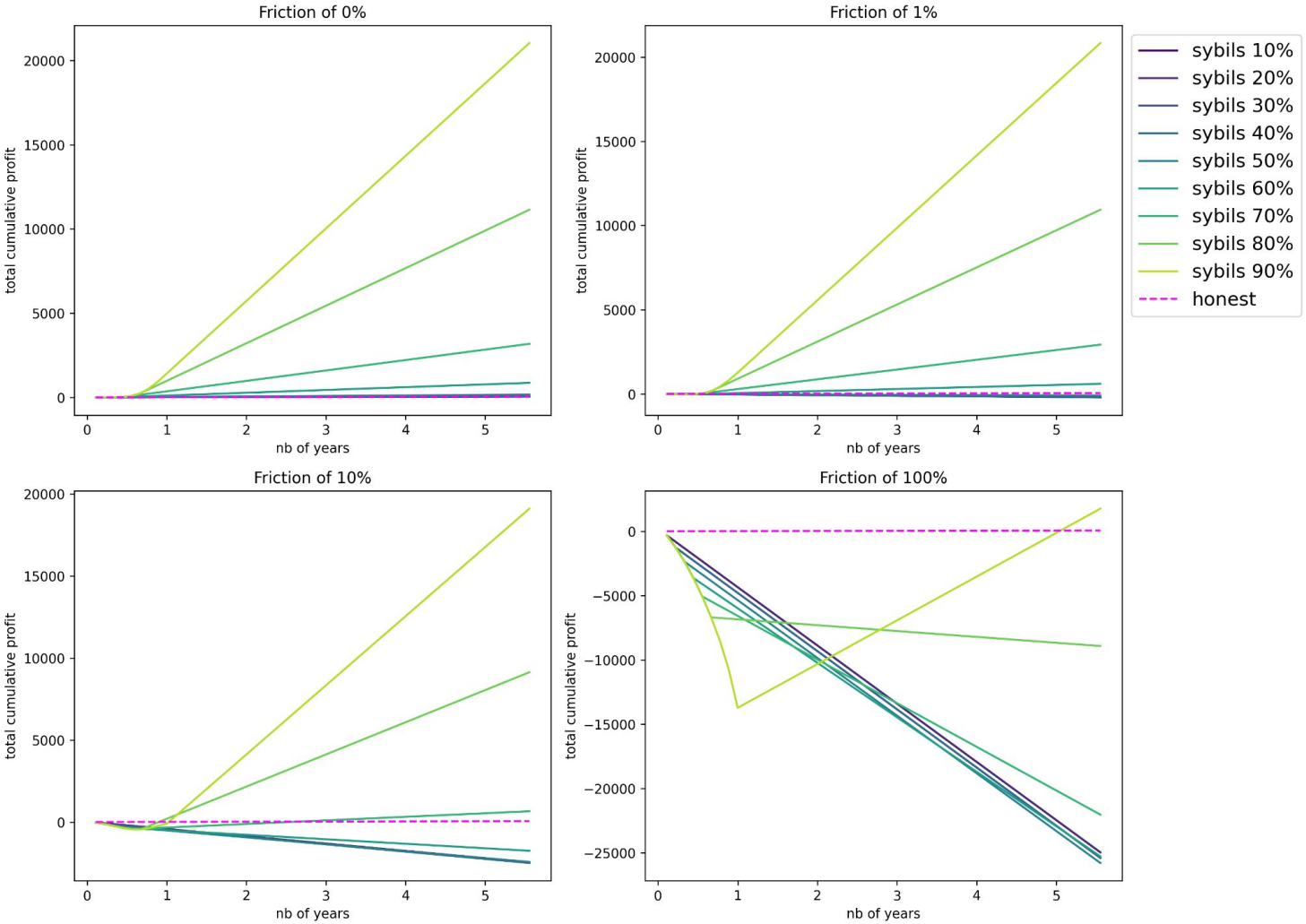


Probability to control a meetup

Adversary strategy



Adversary strategy



Can we make profit from Encointer?

Not impossible, depending on:

- Time resource
- Financial resource