

# Encounter PoP: security analysis

---

Student: Lucie Hoffmann

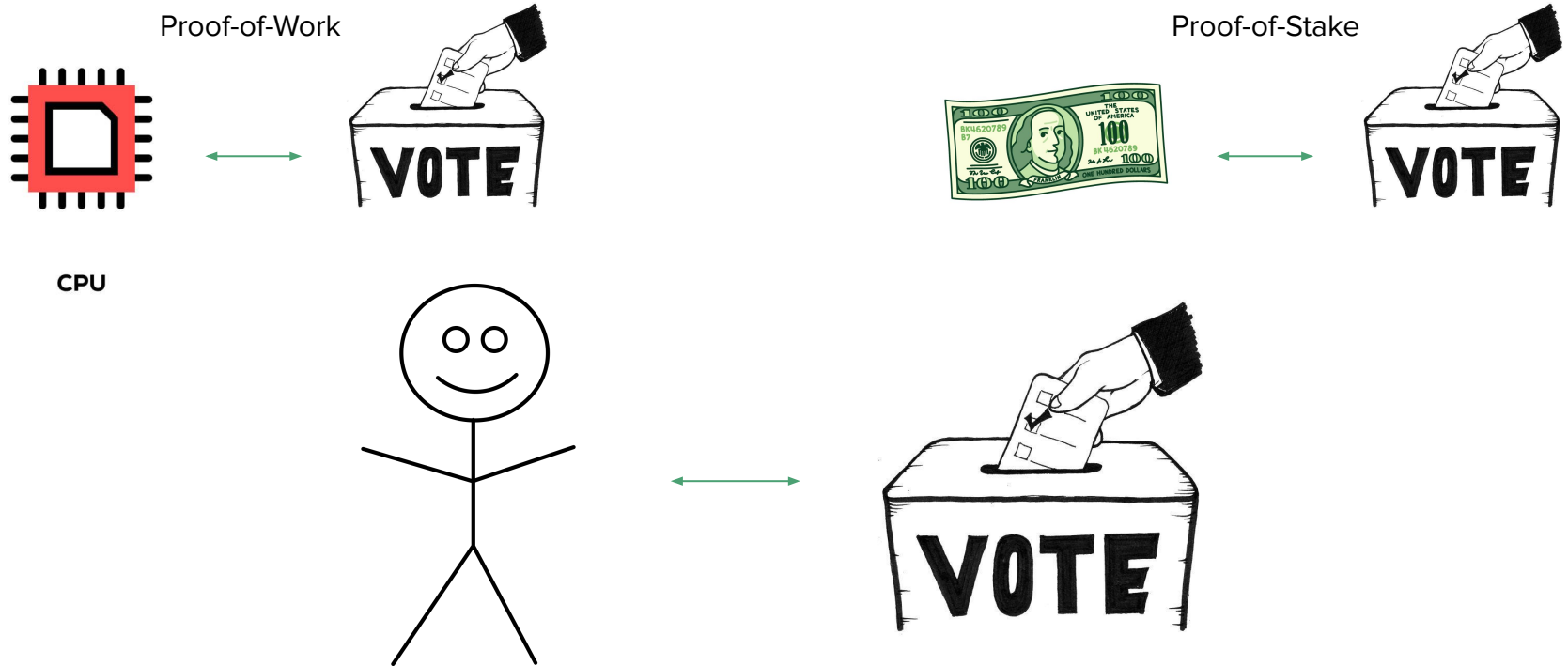
Lab: DEDIS

Supervisors: Prof. Bryan Ford, Louis-Henri Merino, Haoqian Zhang

# Outline

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

# Proof-of-Personhood (PoP)



## Encointer communities

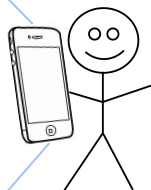
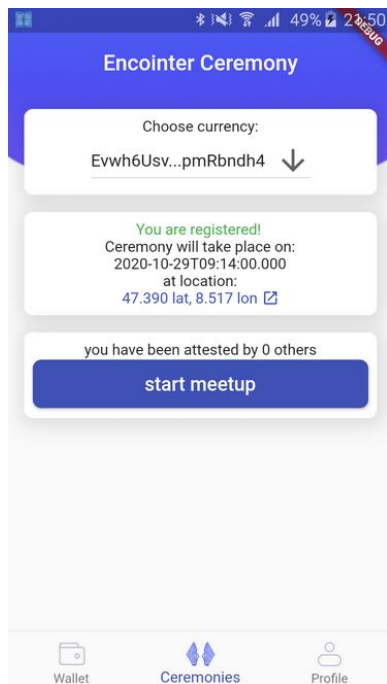
Unique PoP token



Universal Basic Income  
(UBI)

Local currencies

# Encointer



## Ceremony

### Lausanne community - LauzCoin

Meetup at Flon

Meetup at Ouchy

### Montreux community - JazzCoin

Meetup at train station

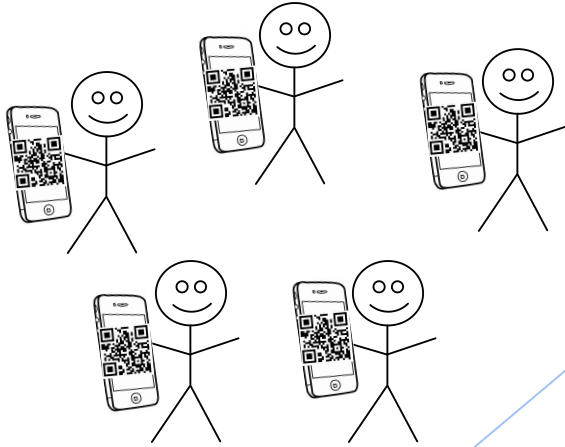
Meetup at lake

### Zürich community - GrüziCoin

Meetup at ETH

Meetup at port

# Encontre



## Ceremony

### Lausanne community - LauzCoin

Meetup at Flon

Meetup at Ouchy

### Montreux community - JazzCoin

Meetup at train station

Meetup at lake

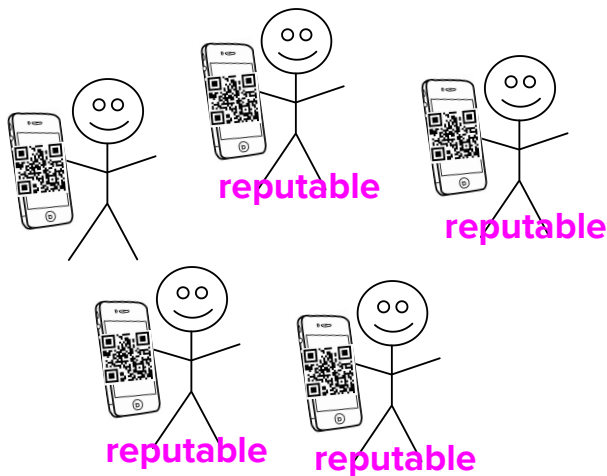
### Zürich community - GrüziCoin

Meetup at ETH

Meetup at port

# Encounter

- Reputation: successfully validated in last ceremony
- Meetup: at least  $\frac{3}{4}$  **reputation**
- Validation condition: attested by **at least all reputables but 2**

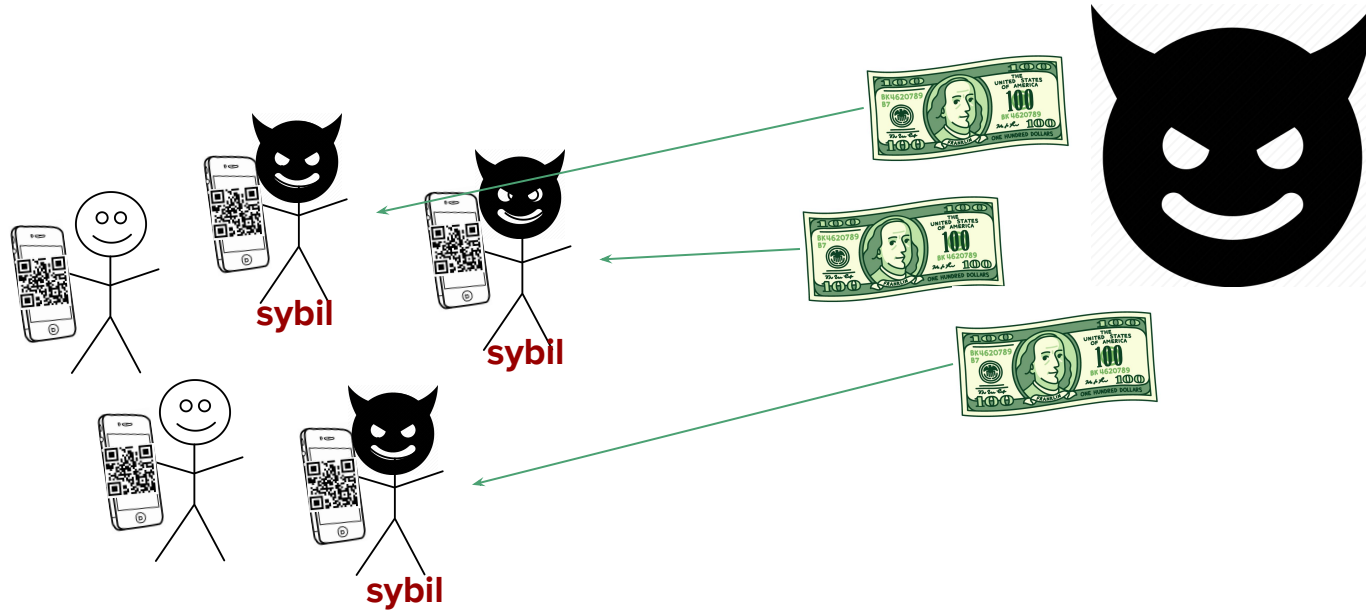


# Outline

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

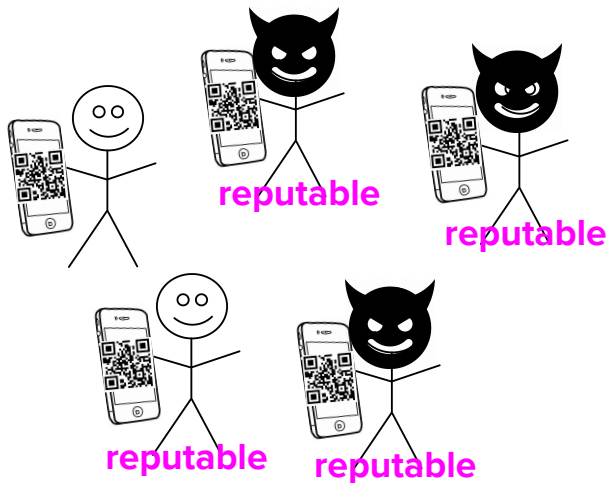


# Sybil attack in Encounter



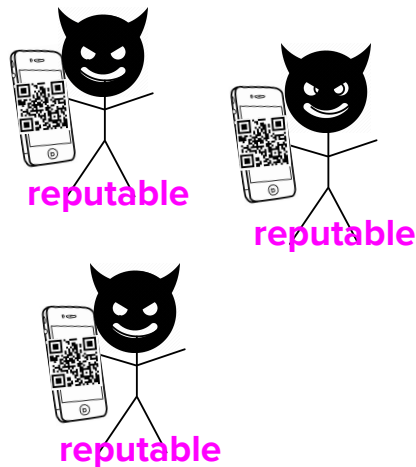
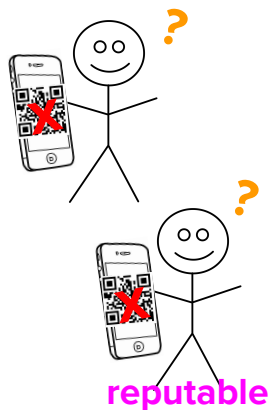
# Sybil attack in Encounter

- Reputation: successfully validated in last ceremony
- Meetup: at least  $\frac{3}{4}$  **reputation**
- Validation condition: attested by **at least all reputables but 2**



# Sybil attack Encounter

- Reputation: successfully validated in last ceremony
- Meetup: at least  $\frac{3}{4}$  **reputation**
- Validation condition: attested by **at least all reputables but 2**

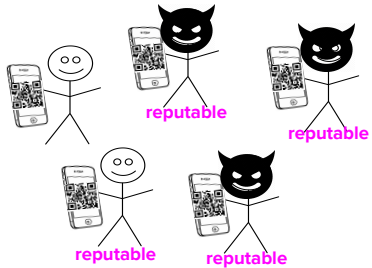


# Outline

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

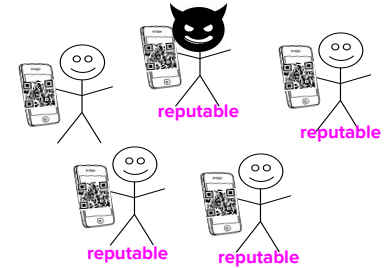
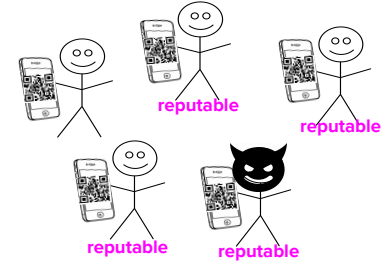
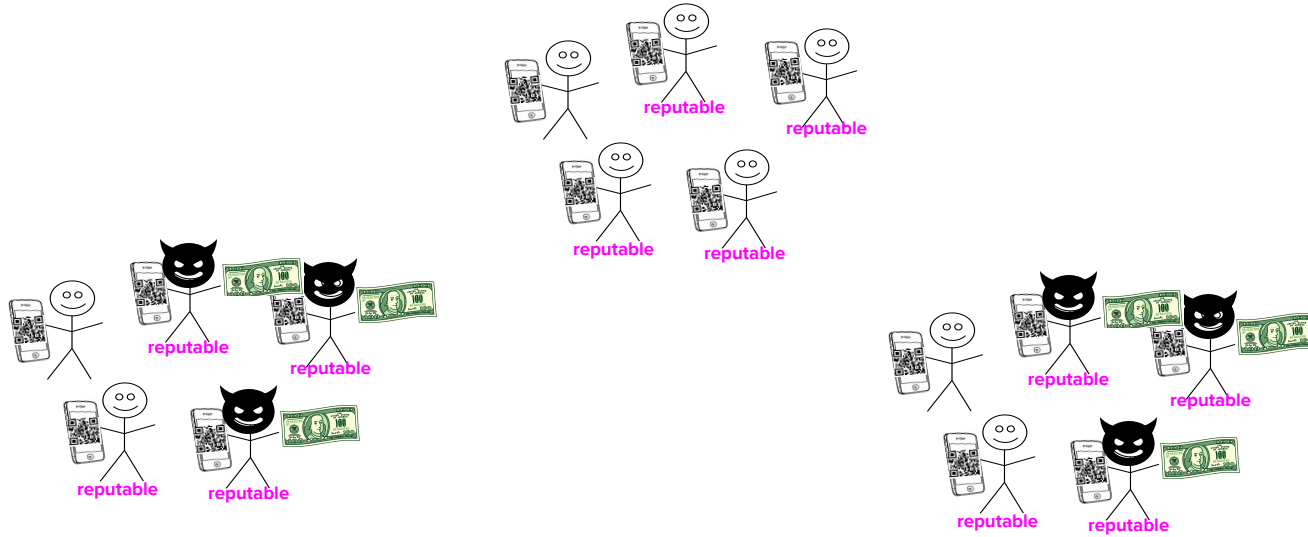
# Can we make profit from Encointer?

- Probability for a meetup to be controlled by sybils



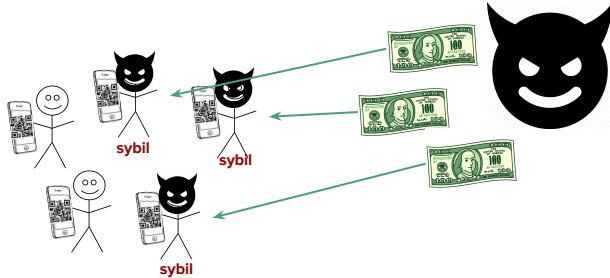
# Can we make profit from Encointer?

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



# Can we make profit from Encounter?

- 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

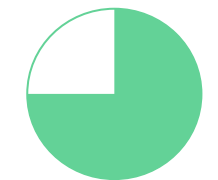


UBI reward =  $R$   
Friction factor =  $f$

Sybil cost =  $R + f \cdot R$

# Probability for a meetup to be controlled

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



$\frac{3}{4}$  reputation

Meetup size

=

$$\left| \frac{\text{\#participants}}{\text{\#meetups}} \right|$$

$$\left| \frac{\text{\#participants}}{12} \right|$$

Need at least

$k$

=

$$\frac{3}{4} * \text{\textit{meetup\_size}} - 2$$

Hypergeometric distribution



# Expected profit for a ceremony

For a meetup:

$$E_{\text{meetup}} = p * \text{profit} - \text{cost} * (1 - p)$$

Probability of success  
=  
Upper bound on probability of controlling a meetup

minimum:  $k * \text{reward}$

maximum:  $(k - 1) * \text{additional\_sybil\_cost}$   
= friction \* reward

The diagram illustrates the formula for the expected profit of a meetup,  $E_{\text{meetup}} = p * \text{profit} - \text{cost} * (1 - p)$ . It includes several annotations: a green arrow points from the text 'Probability of success = Upper bound on probability of controlling a meetup' to the variable  $p$ ; another green arrow points from the text 'minimum:  $k * \text{reward}$ ' to the  $\text{profit}$  term; a third green arrow points from the text 'maximum:  $(k - 1) * \text{additional\_sybil\_cost}$  = friction \* reward' to the  $\text{cost}$  term. The term  $\text{additional\_sybil\_cost}$  in the maximum bound is circled in grey.

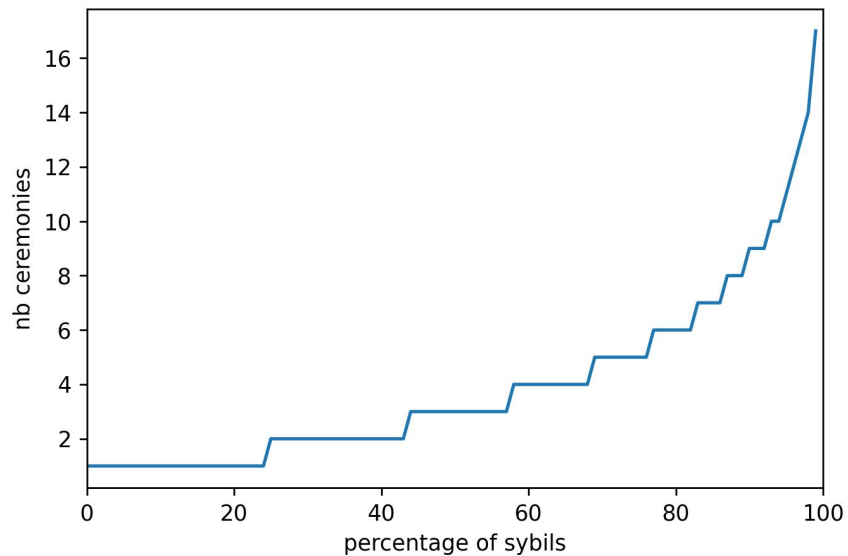
For all meetups:

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

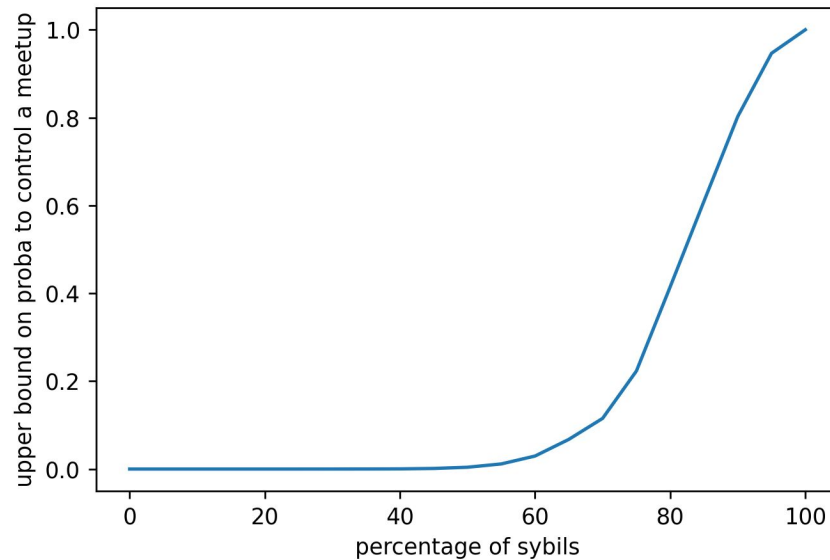
# Outline

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

# Adversary strategy

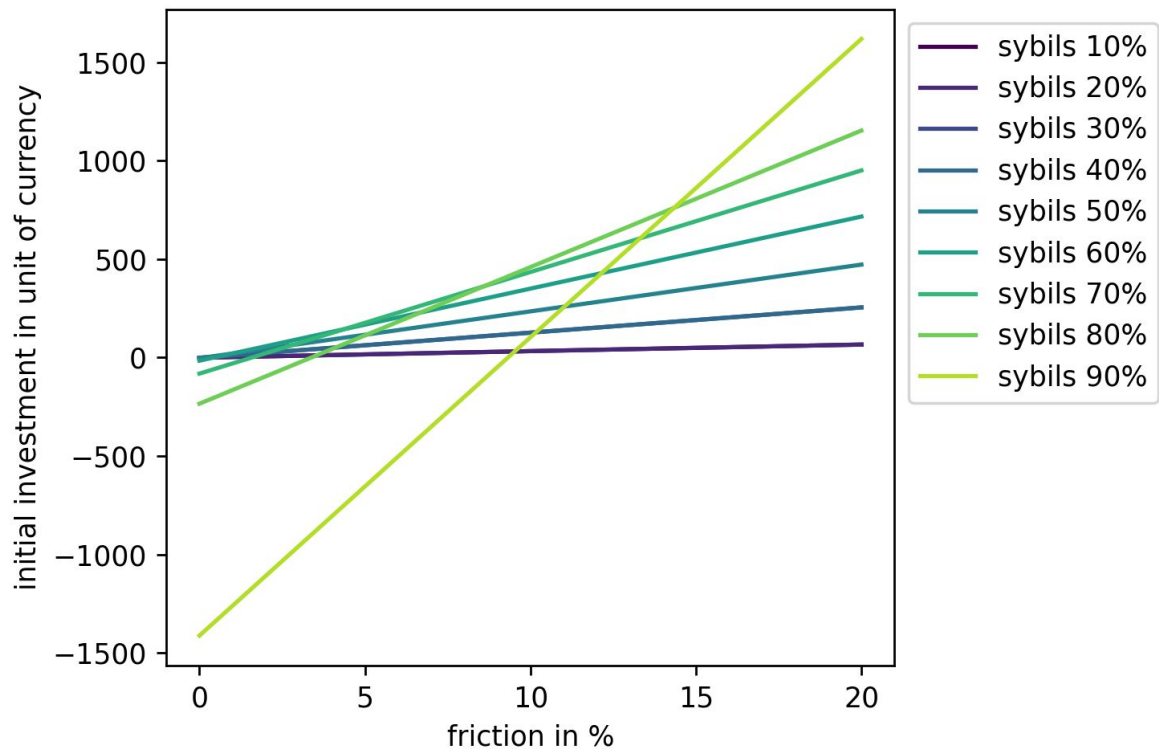


Number of ceremonies to get reputables

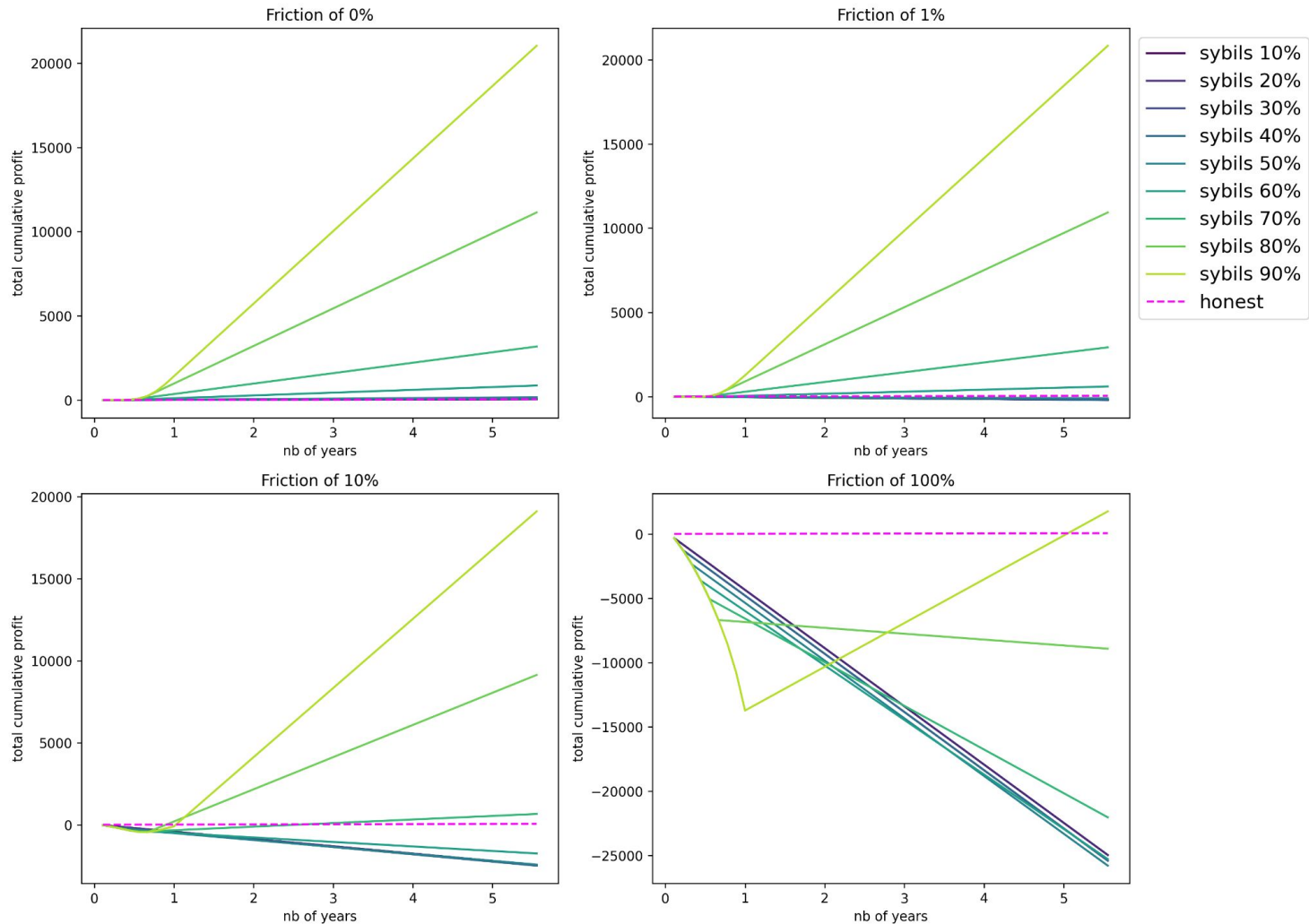


Probability to control a meetup

# Adversary strategy



# Adversary strategy



Can we make  
profit from  
Encointer?

Not impossible, depending on:

- Time resource
- Financial resource

