Security analysis of Proof-of-Personhood: Encointer

Master project report

Lucie Hoffmann

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

Decentralized Distributed Systems Laboratory, EPFL

June 11, 2021

1 Abstract

Proof-of-Personhood (PoP), unlike other consensus mechanisms like Proof-of-Work or Proof-of-Stake, is more egalitarian and aims to give any human being a unique and singular token, allowing them to stay anonymous while holding them accountable. Instead of getting a voting power proportional to one's number of CPUs or dollars, PoP gives one vote per human. Encointer's implementation of PoP is still in the development phase and in this report we present how an adversary could make profit from their system based on simplified simulations.

2 Introduction

While Proof-of-Work (PoW) and Proof-of-Stake (PoS) show a re-centralization of voting power, Proof-of-Personhood (PoP) provides the ideal participation rules for a truly distributed permissionless consensus protocol [1]. This concept brings the basis for a more democratic management of online systems and often comes with a Universal Basic Income distributed equally to every human associated to a unique PoP.

There exist several approaches to achieve PoP [2], [3]. An online approach, like the one proposed by Idena [4] (analyzed in more details in Jordi Subira Nieto's report [5]), needs a way to tell human from computers apart. Reverse turing tests aim to accomplish this by relying on "AI-hard" problems impossible to solve for computers but easy for humans. One can also rely on a web of trust, where one obtains a unique digital IDs by being recognized as trustworthy by a group of already trusted humans, or biometric identity, where one proves their uniqueness and humanness by showing a uniquely identifying biometric like their face for example. In this report, we focus on a system mainly based on another mechanism, which is offline: pseudonym parties. These are in-person events where one can get their unique digital ID. It relies on the simple fact that one unique person can only be at one place at a given time [6]. The advantage with this approach is that we do not need to find a way to distinguish a human and a computer because the physical presence at meetings is sufficient.

Encointer is a blockchain of cryptocurrencies proposing such an in-person protocol and designed to give every human being access to a Unique PoP (UPoP) token and an associated amount of Universal Basic Income (UBI) reward [7]. Like any PoP protocol, Encointer is prone to Sybil attacks, where an adversary tries to get more than one unique token and potentially take control of the network as well as make profit from the UBI reward.

We address the question of whether it is possible for an adversary to make profit out of the Encointer protocol, while maintaining more than one Encointer digital identity.

We first present the background of the report in section 3, then describe how Encointer works in section 4. In section 5 we explain our methodology to simulate Encointer and finally give an analysis of our results in section 6.

3 Background

In this section, we present the terms used in the report as well as the mathematical tools used in the analysis.

3.1 Terms used in the report

Universal Basic Income (UBI): small amount of money issued periodically to every human being that should be sufficient to support basic needs [8].

Trusted Execution Environment (TEE): secure piece of hardware providing isolated and secure execution independently from the rest of the system containing and using it.

Minions or sybils: persons that the adversary pays to appear physically at the meetup for validating their sybil IDs.

Friction factor: percentage of the UBI reward defining the cost of a minion for one ceremony. If the friction is 0%, then the adversary has no additional cost since they pay the minion with the UBI reward they get (e.g. for a reward of 1 unit, the cost of a minion is $1 + 1^{*}friction$).

Honests or legitimates: participants following the rules of the protocol, not trying to cheat on anything, going at every Encointer ceremony.

Reputables: users with reputation (see section on Encointer), i.e. that where successfully validated in the previous Encointer ceremony.

3.2 Hypergeometric distribution

Given a population size N, a number of successful objects in the population K, a number of draws n and number of observed successes k, the hypergeometric distribution models the probability of drawing k objects from the success state population in n random draws, without replacement, from the finite population of size N that contains exactly K successful objects. The probability mass function is defined as follows:

$$Pr(X = k) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}$$

Given $p = \frac{K}{N}$ and for $0 < t < n * \frac{K}{N}$, we can define the following tail bound:

$$Pr(X \geq (p + t)n) \leq e^{-2t^2 n}$$

3.3 Linearity property of expectation

For any random variables $X_1, ..., X_n$, which may be inter-dependent, and constants $c_1, ..., c_n$, the following is always true:

$$E(\sum_{i=1}^{n} c_i * X_i) = \sum_{i=1}^{n} (c_i * E(X_i))$$

where $E(.)$ is the expected value.

4 Encointer

In this section, we first introduce Encointer, then we focus on their implementation of PoP and finally we describe what we are interested to analyze.

4.1 Global overview

Encointer aims to give a UBI and a UPoP token to every human willing to participate in their protocol [9]. They enable the creation of local currencies associated to local communities. Any user gets exactly one UPoP for one local currency and should not get any other UPoPs associated to other local currencies. Before diving into the protocol for getting a UPoP, we summarize the structure of Encointer.

Encointer is a so-called parachain of Polkadot [10], which is a relay chain coordinating and connecting multiple blockchains together. These blockchains are called parachains. The role of blocks in the Encointer blockchain is to attest Trusted Execution Environments (TEEs) corresponding to local currencies. Every local currency is bootstrapped with its own TEE. TEEs are used to validate so-called SubtraTEE sidechains [11] that are handling the assignments and validations in the Encointer UPoP protocol as well as maintaining the balance of currencies of the different Encointer communities [7].

4.2 UPoP protocol

In Encointer, a user can get a UPoP associated to a local currency. The protocol for obtaining a UPoP relies on the fact that one person can only be at one place at a time. Users prove their humanness by attending in-person meetings so-called ceremonies.

4.2.1 Protocol steps

Every ceremony for every local currency happen at the same time every 41 days. One ceremony consists of several meetups, i.e. groups of participants to that ceremony. These meetups, regrouping all Encointer local communities, are located all around the globe and meetups corresponding to the same local currency are all located the same region.

At least 24h before the ceremony starts, participants create their registration transaction for ceremony i containing: their one-time public key associated to this ceremony, their optional proof of successful attendance to a past ceremony j for same currency (defines the so-called reputation) and the local currency's id.

Participants are assigned to their meetup 24h before the start of the ceremony. At a meetup, every participant votes on the number of physically present participants via the Encointer mobile app and then broadcast their claim of attendance to all participants within a short time interval (the time delay is attested by the receivers). This claim contains the one-time public key, the ceremony index i, the meetup ID m and the vote.

Then, participants pairwise sign their claims. Every attestation is signed with other participants private keys, associated to them for a given ceremony.

A witnessing phase then lasts until the start of the ceremony + 24h. During this period, every participant sends their collected attestations and individual votes. If successful, the participant has their UPoP token validated and gets their amount of UBI reward.

They also receive a reputation which constitutes a proof of attendance to a specific meetup at a this ceremony. In the current implementation, this reputation is valid until the next ceremony, i.e. if the participant does not attend the next ceremony, they will lose their reputation.

4.2.2 Assumptions and rules

During the ceremony process, any meetup must satisfy the criteria given below.

- The number of participants that met at their last ceremony is minimized.
- The number of participants per meetup is maximized such that it is between 3 and 12.
- No meetup is assigned with more than $\frac{1}{4}$ participants without reputation.
- Meetup locations are randomized.
- No 2 adjacent ceremonies can be attended by one same participant.

During the validation process, we consider only the meetups matching these criteria:

- The set of participants for meetup m should have at least 1 valid attestation from another participant in this same set.

- The set of participants with reputation for meetup m should have at least 1 valid attestation from another participant with reputation in this same set.

Finally, for a successful validation, any participant must satisfy the following rules:

- The successful participant's vote is that of the majority vote of the set of participants with reputation for this meetup m.
- The successful participant has collected at least (number participants with reputation assigned to meetup) - 2 attestations.
- The successful participant has attested between (number participants with reputation assigned to meetup) - 2 and (majority vote on number participants) participants, bounds included.

4.2.3 Threat model

Encointer UPoP security relies on the hypothesis that "a majority of participants with reputation for each ceremony and each meetup is honest and successfully registers their non-empty attested claims to the blockchain in time" [7]. They consider 2 main possible attacks in their threat model: a sybil attack, where the adversary wants to validate more than one UPoP token, and the sabotage attack, where the adversary aims to prevent legitimate participants to get their UPoP token (and associated reward).

4.3 Security

We make two observations on the Encointer rules.

First, if an adversary controls at least 3 reputable IDs in a meetup and do not show up (do not attest others), then no participants of this meetup is successful and they successfully led a sabotage attack.

Second, if an adversary controls at least (number participants with reputation assigned to meetup) - 2 reputable IDs in a meetup, they are successfully validated. In this case, they do not even need to show up in the meetup, vote for their number of IDs assigned to the meetup as the number of participants and no one else except them gets validated in the meetup. This corresponds to a sybil attack and from now on, in this report, we say that, in this case, the adversary controls the meetup.

Focusing on this last threshold conditioning the acquisition of a UPoP and associated UBI reward, we want to analyze how feasible it is for an adversary to make profit out of this reward while growing a sybil network in some Encointer community. In fact, an adversary can achieve a certain percentage of sybils with reputation in an Encointer community by paying or convincing some minions to go validate their IDs in-person. This percentage is defines their chances of having enough sybils assigned to the same meetup. Then they could make profit by leveraging the probability to control a meetup, i.e. have enough sybils assigned to that meetup so that they don't need to show up and pay minions.

To achieve this analysis, we simulated simplified scenarios while gradually adding constraints. First assuming the adversary could have any percentage of sybils with reputation in the network, we focused on estimating the probability for an adversary to mount a successful sybil attack in a single meetup. Then we considered all meetups to observe the potential profit of the adversary in one ceremony. Next, we studied the potential profit the adversary could accumulate over several ceremonies. We finally added a non-null friction factor, to see the effect of the additional cost of a minion on the potential cumulative profit of the adversary, as they are re-investing this profit into minions to grow in the network.

5 Implementation of the analysis

In this section, we describe the choices and assumptions made for every steps of the analysis. We first explain how we computed the probability of controlling a meetup, the associated expected profit. Then we justify the computations for the initial investment of the adversary. Finally we specify the approximations and parameter choices we made in our analysis.

The code for each of these steps can be found in the appendix A of this report.

5.1 Probability for a meetup to be controlled

In this subsection, we explain why we used an upper bound of the hypergeometric distribution to compute the wanted probability as well as what parameters we used.

5.1.1 Hypergeometric distribution

Every meetup is assigned a certain number of participants, which we call n. Given s sybils and h honest participants, we want to know the probability that a given meetup gets enough sybils to be controlled by the adversary. Let us say 'enough' sybils is defined by a number k. Then we are interested in the probability of selecting k sybils in n draws from the set of participants containing s sybils and h honests, without replacement. This is perfectly modelled by the hypergeometric distribution described in the background section.

5.1.2 Tail bound

The probability for a meetup to be controlled corresponds to the probability of having at least k sybils in a given meetup, or said differently, the probability for a meetup to be assigned at least k sybils.

There is no closed-form for such a probability and it is thus hard to compute its exact value, notably with varying parameters such as s or k. Consequently, we use a tail bound on this probability: the one defined in the background section.

This upper bound makes sense in our analysis because it gives us the maximum potential of an adversary to control a meetup, i.e. it gives a good idea of the worst possible case that can happen.

5.1.3 Parameters of computation

The parameter k depends on the meetup size n and the fraction of reputables in this meetup. The meetup size itself depends on the total number of meetups in the ceremony.

First, we define the number of meetups like in the Encointer implementation as the ceiling value of the total number of participants divided by 12 [12].

Then, we compute the meetup size as the floor value of the number of participants divided by the number of meetups: as seen in the Encointer implementation, every meetup will get this floor value of participants, except one which gets the ceiling value.

Finally, we assume for simplicity that every meetup gets $\frac{3}{4}$ reputables and $\frac{1}{4}$ newbies. Again, this helps giving a good idea of the worst case where the number of reputables to be controlled by the adversary in a meetup is minimized, since in the Encointer thresholds the fraction of reputables is actually at least $\frac{3}{4}$ and could thus be more. The parameter k then needs to be defined as (number of reputables in meetup) - 2, i.e. $\frac{3}{4}$*(meetup size) - 2. We take the ceiling value of $\frac{3}{4}$*(meetup size) to make sure k is big enough for controlling the meetup.

The tail bound then corresponds to e^{-2*n*t^2} where $t = \frac{k}{n} - (\frac{s}{s+h})$.

5.2 Expected profit at one ceremony

We first consider the expected profit made in a given meetup using the upper bound on the probability of controlling a meetup, i.e. the probability of success:

$$p * profit - cost * (1 - p)$$

where p is the probability of success, $profit$ is the money gain in case of success and $cost$ is the money loss in case of failure.

For the profit in case of success, we consider its minimum value: the minimum number of sybils needed to control the meetup multiplied by the reward, i.e. $k * reward$. For the cost in case of failure, we consider its maximum value: the maximum number of sybils in a meetup such that they do not control it multiplied by the additional cost of a minion, i.e. $(k-1) * cost$. The additional cost of a minion is simply $friction * reward$. This means we consider the minimum profit an adversary can make in a meetup.

Since the considered probability of success is an upper bound, the obtained result is an upper bound on the minimum expected profit made by the adversary at one meetup, in the worst case scenario.

To get this upper bound for all meetups in the ceremony, we apply the linearity property of expectation.

5.3 Investment over ceremonies

We compute the investment needed to achieve a percentage of sybils in the network as follows: for the first ceremony where the adversary has no sybils with reputation, we consider the cost of adding a third of the legitimate participants in the network (cost depending on the friction). For other ceremonies, we subtract the expected profit made at the ceremony to this cost. For all ceremonies, we also subtract the reward the adversary always get, like any honest participant does.

Note that the expected profit considered here corresponds to the previously computed upper bound on minimum expected profit.

5.4 Other parameters and approximations

5.4.1 Simplified scenario and parameters choices

In our scenario, we assume the number of legitimate participants is stable across all ceremonies and fixed to 1000. This is an arbitrary number representing the initial size of an Encointer community having their own local currency. Choosing a different value would only vary the time and number of ceremonies needed to achieve a percentage of sybils in the network. We think 1000 is already high enough to represent the number of users in such a community.

We also fix the reward to 1 unit of currency: an almost insignificant reward as stated in the Encointer paper to minimize the possibility of making any interesting profit. This reward is constant across ceremonies: this means we do not take into account the devaluation of money as the Encointer network is growing. In the real world though, the adversary's profit is bounded by Encointer community market cap, corresponding to the total value of all the money in the community network.

Finally, when analyzing the effect of non-null friction on the potential profit of the adversary, we consider the first powers of ten to get an order of magnitude.

5.4.2 Approximations

Added to the approximations already stated in this section, we convert the number of ceremonies in years to get a better idea of the time passing as follows: since there is a ceremony every 41 days, we have about $\frac{365}{41}$ or 9 ceremonies per year. So x ceremonies correspond approximately to $\frac{x}{9}$ years.

6 Results

In this section, we present the results obtained at each step of our simulations. We first observe the profit made by the adversary at one ceremony, then we study the profit evolution over several ceremonies without friction and finally we add the friction constraint.

6.1 Control and profit at one ceremony

In this subsection, we focus on one ceremony and assume the adversary already processes a certain percentage of sybils with reputation in the network. We study the probability to control a meetup given this percentage and observe the associated profit in the case where using a minion is at no additional cost than the reward, i.e. the adversary pays the minions with the reward they get for the corresponding sybil IDs. This is the case where the friction is 0%.

As seen in Figure 1, the chance of success starts being interesting for high percentages of sybils only. The adversary needs more than half of the network to start making profit. They might want to create and make a reputation for as many IDs as they can to increase their chances.

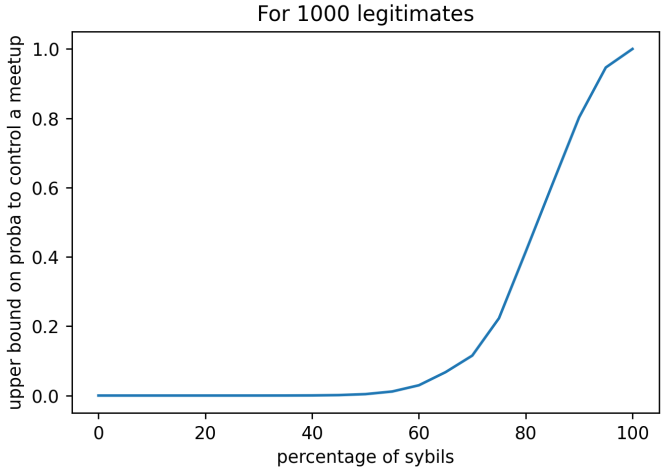

Figure 1: Probability for a given meetup to be controlled by sybils.

As we could have guessed, the minimum expected profit as a function of the sybils percentage, plotted in Figure 2, has the same shape as the probability distribution.

The growth begins exponentially and starts to plateau a bit as the percentage gets closer to 100%: this is logical since the profit is always bounded by number of meetups, which is itself bounded by the number of participants. This means that as the adversary linearly increases their percentage, they increase their profit exponentially.

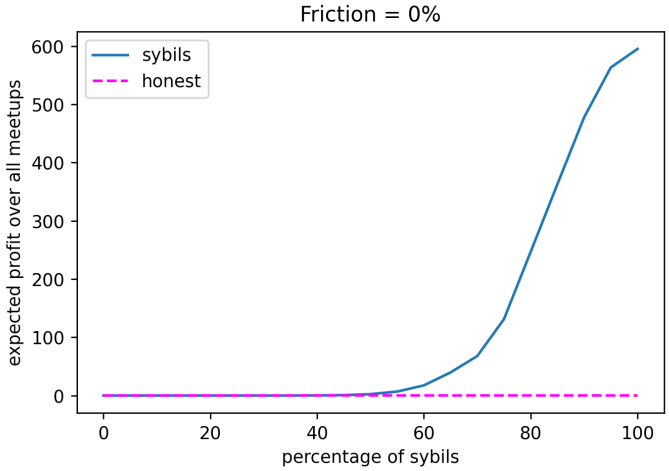

Figure 2: Upper bound on the minimum expected profit made by the adversary (sybils) in all meetups as a function of their percentage of sybils in the network when friction is 0%. The reward received by an honest participant is there as a reference.

6.2 Potential profit when there is no friction

Remaining in the scenario of 0% friction, we now enlarge our vision to several ceremonies. The adversary's investment, in this case, is always going to be 0, regardless of the fraction of sybils they aim to achieve in the network. So they have no financial limit to create as many IDs as needed to make profit. It is only a matter of time before they get the wanted percentage of the network.

In Figure 3, we plot the number of ceremonies needed to achieve every possible percentage of the network. To get a 90% of the network they need 9 ceremonies. Since there is a ceremony every 41 days, they need to wait 369 days, i.e. about 1 year and 3 days to have 90% sybils with reputation participate in a ceremony. They potentially will have made profit before this

period has passed, by maintaining their sybils with reputation while growing their percentage in the network: they start with $\frac{1}{4}$ of the network and a very low chance of controlling any meetup and making profit, then increase their sybil fraction by $\frac{1}{3}$ of the network in the next ceremony, increasing their chance, and so on until getting the wanted percentage (90% in this case).

This means the adversary needs to wait a maximum of one year before making high profit.

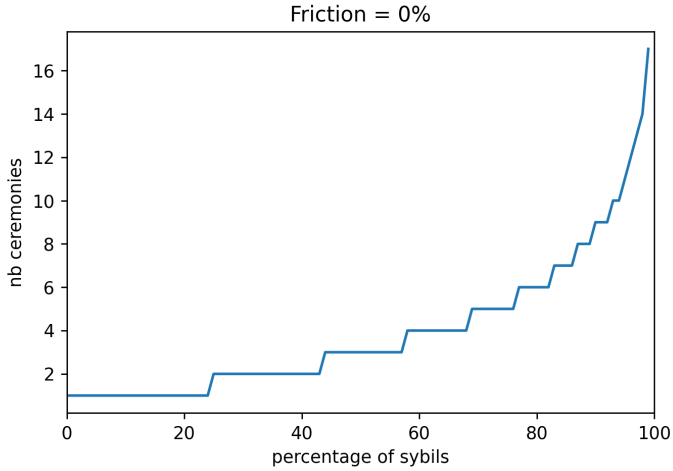

Figure 3: Minimum number of ceremonies to achieve a given fraction of sybils with reputation in the network.

Now, let us compare the profit accumulated over several ceremonies for different percentages of sybils, see Figure 4.

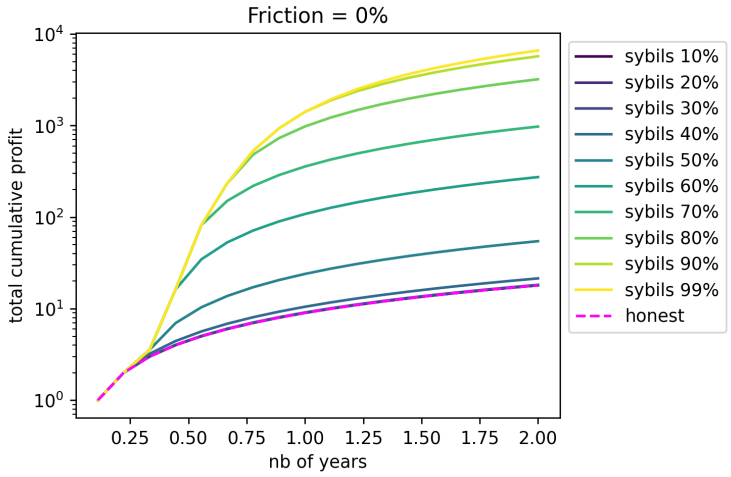

Figure 4: Upper bound on the minimum profit the adversary accumulates across 18 ceremonies in a scenario with fixed amount of legitimate participants and 0% friction.

From 10% to 30%, the profit is about that of an honest participant: the adversary maintains sybil IDs at no cost, gaining as much as an honest participant but making no profit.

With 40% sybils, they start gaining more than an honest participant: they maintain 40% IDs while making some small profit.

For 50% and more sybils, they gain clearly more than an honest participant, making interesting profit while maintaining their sybil IDs. We observe that, for this range of percentage, after less than half a year, the adversary already has made huge profit.

This scenario with 0% friction is clearly advantageous for an adversary willing to wait a rather short time to make an interesting profit at no initial cost, while maintaining several UPoP tokens.

6.3 Potential profit with friction

In the real world, minions may be convinced or charmed by the adversary so that the friction stays at 0%, but they might also want to be paid more than the reward, as a compensation for not getting their UPoP token for example. In this subsection, we study this very case where the friction can be higher than 0% and observe its impact on the adversary's profit.

As can be seen on Figure 5, the friction impacts higher percentages of sybils more badly, due to the substantial initial investment (see Figure 6), which is much higher for high sybils percentages. Note that on Figure 6 the initial investment can be negative: this corresponds to a positive profit the adversary makes while growing their percentage.

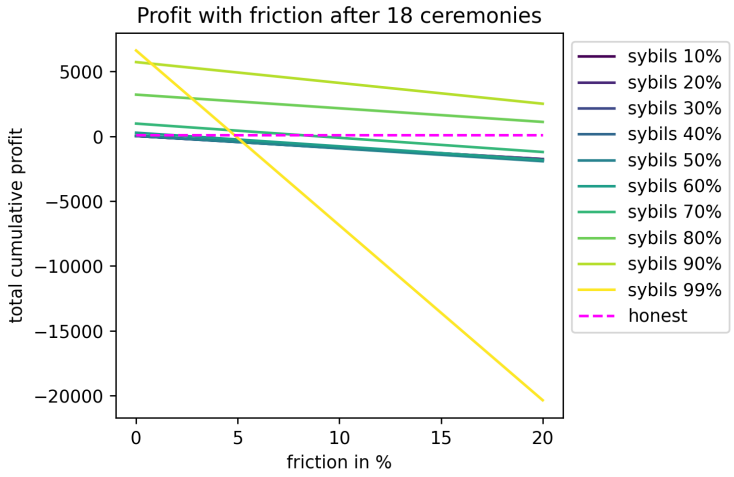

Figure 5: Upper bound on the minimum profit the adversary has accumulates after 18 ceremonies (about 2 years) as a function of the friction factor.

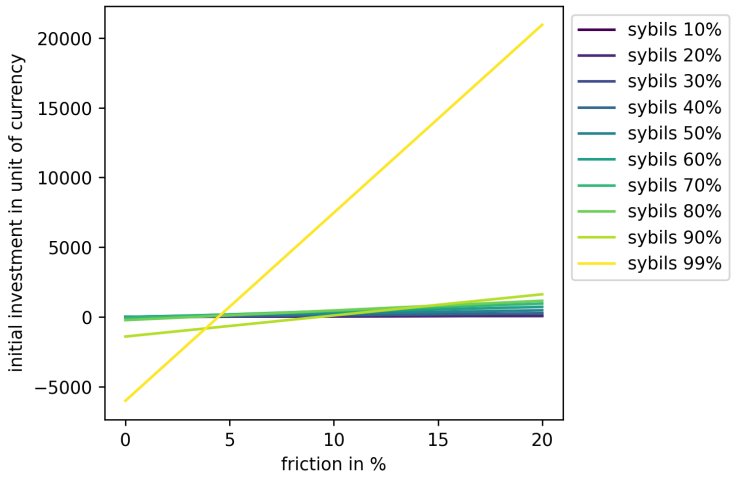

Figure 6: Investment needed to achieve different sybils percentages as a function of the friction factor.

For any non-null friction, we guess from the graphs that the investment increases exponentially as the percentage of sybils increases linearly.

With low friction, high percentages of sybils remain the most interesting ones, but as soon as the friction grows, these high percentages of sybils also become the ones causing the highest loses.

This effect on higher percentages can also be seen in the drop after about 90% of sybils when plotting the maximum friction for which the profit remains non-negative for every possible fractions of sybils in the network after a fixed number of ceremonies. In Figure 7, we plot this

maximum friction after 18 ceremonies (about 2 years), which is enough for making a reputation for up to 99% sybils.

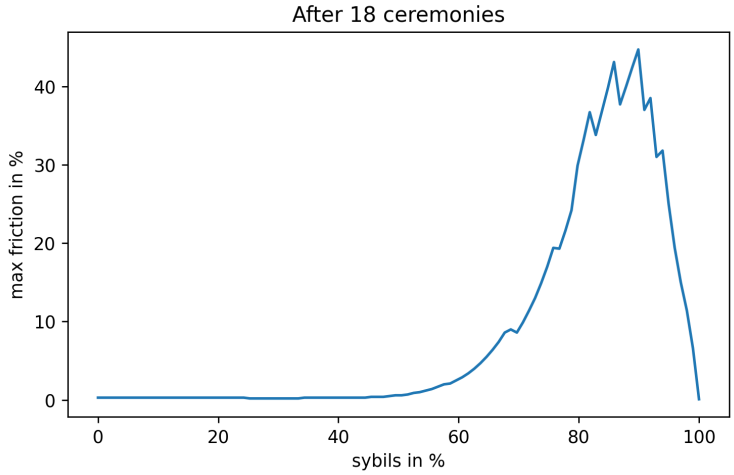

Figure 7: Maximum friction before getting a negative profit as a function of the fraction of sybils.

Of course, the higher the number of ceremonies, the more time given to the adversary to make positive profit, and so the higher the maximum friction threshold.

In our case, the minimum friction that would make no percentage of sybils interesting for profit is about 4.5%, which can be considered already significant. This maximum friction threshold is achieved by a percentage of 90%, which would thus be the most interesting sybils percentage for the adversary.

Now, let us fix different frictions by orders of magnitude, i.e. 0.1%, 1%, 10% and 100% and see their effect on the evolution of profit with respect to different percentages of sybils. See Figure 8.

0.1% friction hardly impacts the profit and in this case any fraction of sybils remains at no cost, except that they get less than an honest participant for percentage of sybils below or equal to 40%. This is because the adversary always gets their reward which is higher than the cost of all minions in this case.

With 1% friction, the adversary starts losing money for a bit more than half a year before making profit for percentages higher or equal to 60%. For these percentages, they never need to invest more than 20 units of currency. For lower percentages, they continuously lose money without making any profit.

With 10% friction, they need to wait about a year before they can make positive profit with sybils percentages of 80% to 90%. For too high percentages like 99%, the initial investment for getting this high percentage of sybils is too high and they need to wait more than 3 years before making positive profit. Similarly for 70% sybils, the adversary needs to wait about 2 and a half years before making positive profit. Percentages below or equal to 60% are never interesting for the adversary in this case: they lose more and more money with time. For percentages greater than 60%, they need to invest up to more than 7000 units of currency before making positive profit.

For a 100% friction, the adversary can hope to make positive profit in about 5 years only with 90% sybils but they would need to invest about 13000 units of currency to achieve this percentage. With 99% the initial investment hurts so bad they would need to wait about 25 years before making positive profit and would need to invest about 125000 units of currency. For any other percentage below 90%, the profit is forever negative, making them lose more and more money with time passing.

So, 0.1% friction has almost no impact on the adversary's profit. 1% friction only impacts permanently percentages strictly below 60% and higher percentages remain interesting regarding the low investment needed. 10% friction impacts permanently percentages strictly below 70% and 100% friction impacts permanently all percentages strictly below 90%. For the two latter friction factors, the substantial investment might make it less interesting for the adversary, de-

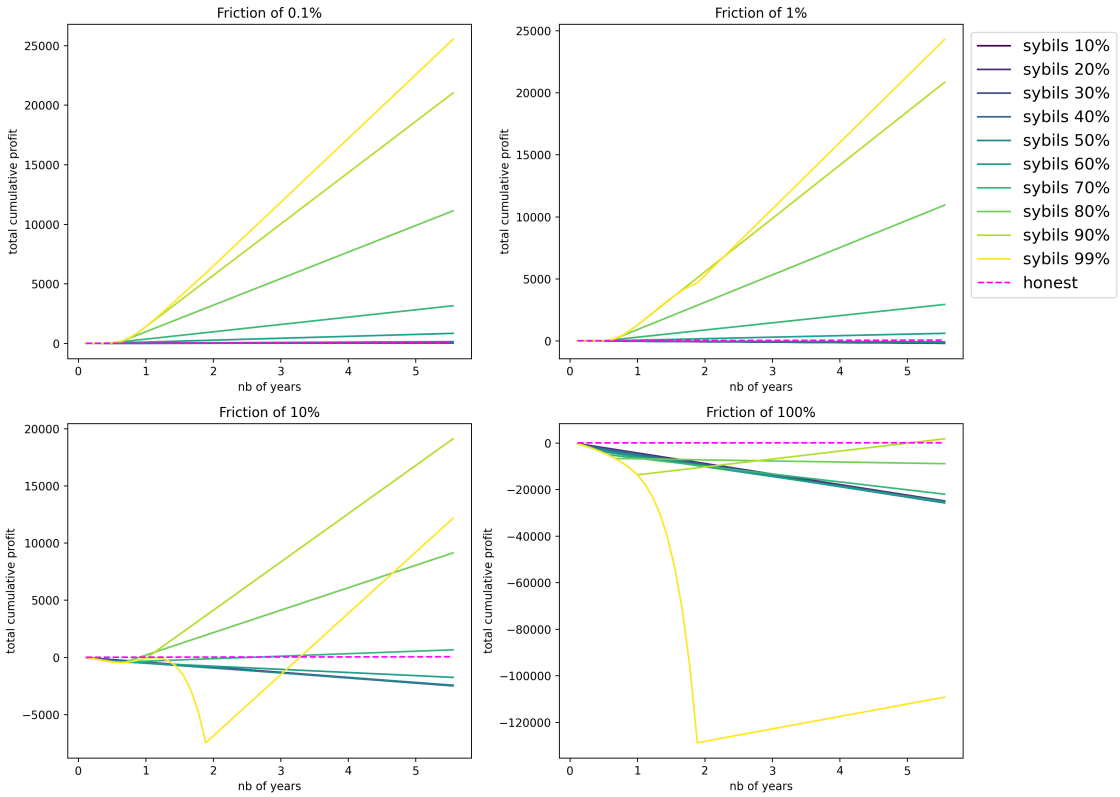

Figure 8: Upper bound on the minimum profit the adversary accumulates across 50 ceremonies for different magnitudes of friction.

pending on their initial resources.

The threat models thus depend on 2 types of adversary resources:

- Time resources: how many years can they wait before making positive and interesting profit?
- Financial resources: how much can they invest before making a positive and interesting profit?

We summarize these last results in the Figure 9. Note that the values are approximated from the study of the graphs.

	Within 1 year	Waiting for 3 years	Waiting for 5 years
0 unit of currency	0.1% and 1% remains interesting when considering profit within 1 year. 10% and 100% friction is definitely not worth it.	Same as for 0 unit of currency.	Same as for 0 unit of currency.
460 units of currency	Same as for 0 unit of currency.	Up to 10% friction remains interesting.	Same as for 3 years.
13000 units of currency	Same as for 0 unit of currency.	Same as for 460 units of currency.	Always profitable regardless of the amount of friction up to 100%.

Figure 9: Table summarizing the adversary's potential depending on their time and financial resources.

6.4 Global interpretations

In this subsection, we question the obtained results in regard of the simplifications and approximations made during the simulations, and interpret their relevance in the real world.

We first note that the adversary can only exchange the currency they gain with other members of the corresponding community against goods and services made available by these members. This means the real value of the profit they make is determined by the value of these goods and services, which might nevertheless still be interesting for the adversary.

More importantly, as said in the approximations, we did not take into account the devaluation of money as the network grows above the community currency market cap. Taking this into account, the profit would still grow but this growth would be much slower than in our simulations. It would grow linearly with the percentage of sybils instead of exponentially.

Another thing we did not consider is the growth of the network independently from sybils. Sybils are not always the only newbies at each ceremony and the adversary might not have a chance to add a number of sybils equal to a third of the network at every ceremony. Added to the fact that the number of legitimates is also likely to grow, this means the adversary's growth will tend to be slower than in our simulations.

However, this potential error in the growth velocity may be compensated because we set the initial number of legitimates in the Encointer community to 1000, which might already be quite high for a local community. In a community with fewer members, the adversary would need less sybils to achieve a high percentage of the network and thus less time.

We also want to note that since we are using an upper bound on the minimum expected profit in the worst case scenario, the actual profit could be less. We believe it still provides a good idea of the potential of an adversary depending on their time and financial resources.

6.5 Mitigations

An adversary bribing minions is not considered in Encointer because it is out of the scope of the protocol. Bribing can always happen in real life, regardless of the protocol used. They also make the hypothesis of the majority of reputables being honest in each meetup. We showed, however, that there exists a case where minions are not needed, allowing them to make profit: this is the case when they control one or more meetups. In this subsection, we give some suggestions to avoid this kind of profit attack.

When the adversary doesn't need to show up at the meetup, legitimate participants in the meetup, if any, will normally show up and won't be able to get validated. These legitimate participants could somehow notify Encointer of the absence of the sybils assigned to their meetup.

Every participant could for example be associated with a count corresponding to their number of absences to meetups. This count would be determined as follows: every participant at a meetup knows which Encointer pseudonym was assigned to their meetup, and knows which one they signed (those corresponding to the participants present at the meetup). For every other participant assigned to the meetup, they vote 0 if the participant was here, 1 otherwise. The final count associated to an Encointer UPoP token is a bitwise OR operation of every count vote, i.e. for every participant it is 1 if at least one other participant voted against them and 0 otherwise.

Since the number of participants that met in the last meetup is minimized, although the adversary might vote 1 for every honest participant in their meetup, an honest participant count will likely be less than the sybils counts. This is because the adversary can only vote against (i.e. vote 1) honest participants when they are assigned to their meetup, so rather rarely vote against the exact same honest participant, except if their percentage in the network is high enough. On the other hand, honest participants will always vote against the adversary when they don't show up, ensuring they get their count incremented every time they manage to control a meetup. As a result, putting a threshold on this count, we can remove from the network any participant with a count above this threshold. This threshold should be set low enough to remove sybils as fast as possible, but not to 1 directly because every one could get removed after the first ceremony. Setting this threshold to 2 would let only 2 ceremonies for an adversary before they get removed, minimizing their percentage in the network as well as their power to remove honest users.

Moreover, although the adversary might want to vote against honest participants, they have no interest in doing this since they would not have anyone to exchange their gain with anymore. The only thing they would achieve would be to break the community and make the associated local currency useless.

We have not tried to implement a simulation of this mitigation though, so there might be caveats we did not identify here. This could be the goal of future works.

7 Conclusion

In this report, we described the Encointer implementation of PoP and analyzed through simplified scenarios how their hypothesis on majority honest reputables could be broken, as well as how an adversary could make profit thanks to this breach. Our results show that making profit is possible when bribing enough distinct minions, depending on how much these minions need to be paid as well as on the adversary's time and financial resources.

A Appendix

In this appendix we show the implementation of the computations used in our simulations. First we show the code for the probability on Figures 10 and 11, then for the expected profit on Figure 12 and finally for the initial investment on Figure 13.

We used the following Python libraries: random, matplotlib, numpy and math. The corresponding Jupyter notebook can be found on the Github of this project: https://github.com/dedis/student_21_pop_security/blob/main/encounter_simulations/Clean_notebook_Encounter_analysis.ipynb.

A.1 Probability

```python
def upper_proba_k(k=3, sybil_fraction=0.1, n_participants=1000):
    n_meetups = math.ceil(n_participants/12)
    meetup_size = math.floor(n_participants/n_meetups)
    t = math.ceil(k/meetup_size) - sybil_fraction
    return math.exp(-2*meetup_size*t**2)
```

Figure 10: Python function to compute the upper bound on the probability to have at least k sybils in a given meetup.

```python
def get_proba_control(sybil_fraction=0.1, n_legitimates=1000):
    n_sybils = math.ceil(sybil_fraction*n_legitimates / (100-sybil_fraction))
    n_participants = n_sybils + n_legitimates
    n_meetups = math.ceil(n_participants/12)
    k = math.ceil((3/4) * (n_participants/n_meetups)) -2
    return upper_proba_k(k, sybil_fraction, n_participants)
```

Figure 11: Python function to compute the upper bound on the probability to control a given meetup.

A.2 Expected profit

```python
def expected_profit(sybil_fraction,n_legitimates,reward,friction):
    n_sybils = math.ceil(sybil_fraction*n_legitimates / (100-sybil_fraction))
    n_participants = n_sybils + n_legitimates
    n_meetups = math.ceil(n_participants/12)
    k = math.ceil((3/4) * (n_participants/n_meetups)) -2
    min_profit = reward*k
    additional_sybil_cost = friction*reward
    max_cost = (k-1)*additional_sybil_cost
    p = get_proba_control(sybil_fraction,n_legitimates)
    return (min_profit*p - max_cost*(1-p)) * n_meetups
```

Figure 12: Python function to compute the upper bound on the minimum expected profit made over all meetups in a ceremony.

A.3 Initial investment

```python
# investment to get a given fraction of sybils in the network
def initial_investment(sybil_fraction, n_legitimates, reward, friction):
    n_previous_participants = n_legitimates
    n_sybils = math.floor(n_previous_participants/3)
    if (sybil_fraction==0):
        n_sybils = 0
    investment = []
    additional_sybil_cost = friction*reward

    prev_inv = n_sybils*additional_sybil_cost-reward
    investment.append(prev_inv)
    n_previous_participants += n_sybils
    curr_sybil_fraction = n_sybils/n_previous_participants

    while curr_sybil_fraction < sybil_fraction:
        add_sybils = math.floor(n_previous_participants/3)
        n_sybils += add_sybils
        n_previous_participants += add_sybils
        profit = expected_profit(curr_sybil_fraction,n_legitimates,reward,additional_sybil_cost) + reward
        prev_inv = prev_inv+add_sybils*additional_sybil_cost - profit
        investment.append(prev_inv)
        curr_sybil_fraction = n_sybils/n_previous_participants

    return investment, len(investment)
```

Figure 13: Python function to compute the initial investment needed to achieve a given percentage of sybils in the community network.

References

[1] P. J. L. G. N. G. Maria Borge, Eleftherios Kokoris-Kogias and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," April 2017. [Online]. Available: https://bford.info/pub/dec/pop-abs/

[2] D. Siddarth, S. Ivliev, S. Siri, and P. Berman, "Who watches the watchmen? a review of subjective approaches for sybil-resistance in proof of personhood protocols," 2020.

[3] B. Ford, "Identity and personhood in digital democracy: Evaluating inclusion, equality, security, and privacy in pseudonym parties and other proofs of personhood," November 2020. [Online]. Available: http://arxiv.org/abs/2011.02412

[4] "IDENA: Proof-of-Person blockchain." [Online]. Available: https://idena.io

[5] J. S. Nieto, "Security of proof-of-personhood: Idena," June 2021.

[6] B. Ford and J. Strauss, "An offline foundation for online accountable pseudonyms," April 2008. [Online]. Available: https://bford.info/pub/net/sybil-abs/

[7] A. Brenzikofer, "Encointer- local community cryptocurrencies with universal basic income," December 2020. [Online]. Available: https://bford.info/pub/net/sybil-abs/

[8] "Universal Basic Income - The Encointer Book." [Online]. Available: https://book.encointer.org/economics-ubi.html

[9] "Encointer – universal basic income in local currencies." [Online]. Available: https://encointer.org/

[10] "Polkadot Wiki." [Online]. Available: https://wiki.polkadot.network/

[11] "Introduction - The substraTEE Book." [Online]. Available: https://www.substratee.com/

[12] "encointer/pallets." [Online]. Available: https://github.com/encointer/pallets