

# Potential Risks (and mitigations) due to interaction removal

One point to take into account when dealing with NI-PoRep, compared with the status quo, is that a malicious party willing to take over the network could potentially keep accumulating sectors locally adding them to the network all in a sudden.


This could in theory allow for an attack which can not be detected in advance which would result in taking over the entire network.

## Why not today?

Such an attack is (in theory) doable today as well. An adversary can add sector until she gets a percentage of the network power which allows for taking over the network. Nevertheless, such a growth in power would be noticed over time, given that each sector, before being added to the network, needs to be precommitted.

## Does NI-PoRep open the door to Network takeover? TL;DR: NO.

It is true that with NI-PoRep and the associated removal of `PreCommit` this traceability of sectors that will be added to the network is not possible anymore. Nevertheless, this is not an issue, for multiple reasons:

- Accumulating sectors and suddenly post them onchain is not the best way to attack the network.
  - NI-PoRep removes `PreCommit` and PCD, but keeps IP as it is today. This means that adding EiBs of sectors results in a massive costs both in terms of hardware and pledge. Latest analysis from CryptoNet lab show that network today is mostly secured by pledge, and this is not going to change with NI-PoRep. See  [\[2023Q3\] Consensus Security: summary\\_doc](#) and related analysis

- Given the point above, cost-wise the best strategy for an adversary willing to takeover the network is actually to bribe and take control of existing sectors for a window of time rather than paying both hardware and pledge cost for adding a massive amount of sectors which need to be maintained later on.

We are not concerned that accumulating sectors and suddenly post them onchain is a real venue for an attack in order to take over the network.

We are convinced that NI-PoRep does not augment the risk of such an attack with respect of today.

### What if we are still concerned this is an issue?

If we are still concerned that too many sectors are added all in a sudden without any possibility of "early detection" we could take one of the following paths:

- Add **NI-Timestamp** message, a light pre-commit-like step in which we timestamp sectors which were sealed in the last 900 epochs (Proposed mitigation, if we are convinced this is a real issue)
  - **Pros:** this would both mitigate the aforementioned issue and the anchorage of sectors to the chain
  - **Cons:**
    - this solution would re-introduce a sort of pre-commit step, even if way lighter than today.
    - No PCD required for **NI-Timestamp** could lead to malicious SP spamming the network with light-precommit messages that do not translate into actual sector added to the network
  - **TODOs:** estimate gas costs
- Add a **NI-PreliminaryProof** message, with which an SP need to pre-validate a sector by submitting a valid proof for it. This preliminary proof does not lead to sector activation (we'd still wait the first WindowPost). Note that this would mitigate the spamming issue mentioned above.
  - **Pros:** Prevents **NI-Timestamp** messages spamming the network
  - **Cons:** Additional gas costs for the preliminary proof
- Bound the per day percentage of NI-PoRep Sector added

- **Pros:** Practically making takeover using NI-PoRep unfeasible by design
- **Cons:** Not great from the product perspective. Moreover, it introduces potential coordination issues (what happens to added sector which exceed the cap?)
- Hardcode the maximum number of sectors which can be added with a single NI-PoRep
  - **Pros:** easy change
  - **Cons:** It does not really enforce security against the aforementioned attack in practice (what if a malicious SP adds plenty of NI-PoRep? each one is bounded, but the total is not).
- Limit the number of sectors added for each NI-PoRep to `Max_NI-Sectors` in order to mitigate the potential issue mentioned above and re-establish an early detection mechanism. This limitation should take into account that we want NI-PoRep to unlock SN improvements at full potential. this would translate in having `Max_NI-Sectors`  $\geq$  maximum number of sectors which can be sealed in parallel.
  - Note that `Max_NI-Sectors` does not really limit the total number of sector an SP can add, but only the nuemr of sector which can be added in a single NI-PoRep iteration (i.e. a malicious SP can run multiple NI-PoRep iteration and overcome the limit)