NI-PoRep: Proving Overhead Analysis

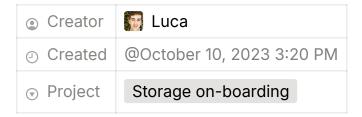|	
⊙ Creator	🧑 Luca
⊙ Created	@October 10, 2023 3:20 PM
⊙ Project	Storage on-boarding

> 💡 TL;DR1: If we consider PC1+PC2+C1+C2 and Storage costs (i.e. not considering maintenance costs), a 128 bits of security NI-PoRep sector is 5% more expensive overall than a Interactive PoRep sector when sector duration is 3y.

🌍 Background

NI-PoRep allows for removing interaction at the cost of augmenting the number of challenges by a factor of 8 or 12.8 (depending on wether we want to achieve 80 or 128 bits of security). See ⭕ Non Interactive PoRep for more details.

The 8x/12.8x number of challenges translates into an 8x/12,8x Snark proving overhead. But how does this proving overhead translates in practice? This is the aim of this doc.

➡️ How to get there

We asked for estimations of realistic numbers for proving setup and we considered the latest Supranational improvements (SupraSeal) to have a sense of how NI-PoRep overhead is affecting per sector PC1+PC2+C1+C2 costs.

📋 Onboarding Cost Analysis: Interactive Vs NI-PoRep

C2 (Pre SupraSeal Improvements, Interactive PoRep)

Hardware

GPU

- 2080 ti ⇒ 20 mins

- 250$ (Capex)

- 2 years ROI

- 150w

- 0.1$/kw

Daily cost and Per Sector cost

Having a proof every 20 mins means having 72 proofs per day.

`energy_cost` = 150w*24*0.1$ = 3.6 kw * 0.1$ = $0.36 per day

`capex_amortization` = 250$ / 24 months ROI = $0.35 per day

We have:

- Daily cost = `energy_cost` + `capex_amortization` = 0.36+0.35 = 0.71$

- Per sector cost = Daily cost/Proofs in a day = 0.71/72 = 0.0099$

C2 (Post SupraSeal Improvements, Interactive PoRep)

We assume SupraSeal improves C2 costs by ~5x. Note that proving is improved by ~8/10x but benchmarks suggest that overall improvement factor is ~ 5x (see SupraSeal C2 benchmarks, first line in the table)

⇒ Per sector cost after SupraSeal improvement = 0.0099/5 = 0.00198$

PC1+PC2+C1

Hardware (SupraSeal Setup)

- 64 core CPU — $5k

- 128 GB of RAM — 500$

- 12 x NVME in RAID 0 + os SSD — $7.2k

⇒ Hardware cost ~ $20k

Overall, we consider

- $20k (Capex)

- 2 years ROI

- 1kw

- 10$c/kw

Considering a PC1+PC2+C1 cycle of 128 sectors in parallel is taking ~6h to complete (estimation from Filmine)

Daily cost and Per Proof cost

Having 128 sectors in ~6h translates into a total of 128*(24/6) = 512 sector/day

`energy_cost` = 1kw*24 = 24 kw * 0.1$ = 2.4$ per day

`capex_amortization` = $20k / 24 months ROI = 800/month/30 = 27.4$ per day.

We have:

Daily cost = `energy_cost` + `capex_amortization` = 2.4$ + 27.4$ = 29.79$ for 512 sectors

Per Sector cost = 29.79/512 = 0.058$ sectors

🌀 PC1+PC2+C1+C2 Recap

Per Sector Cost allocation post SupraSeal Improvement, Interactive PoRep (without considering storage and maintenance costs throughout sector lifetime)

- 0.058$ — PC1/PC2/C1

- 0.00198$ — C2 (improved by 5x)

Given overall 5x Improvement: Total cost per Interactive PoRep sector: 0.058$ + 0.00198$ = 0.05998 [C2 represents ~3.3% of the total cost]

Per Sector Cost allocation post SupraSeal Improvement, NI-PoRep, 5x improvement (without considering storage and maintenance costs throughout sector lifetime)

- 0.058$ — PC1/PC2/C1

- 0.00198 *12.8$ = 0.0253$ — C2 with 128 bits of security

Total cost per NI-PoRep sector:

- 128 bits of security = 0.058 + 0.0253 = 0.0833

Per Sector Cost Comparison Interactive Vs NI-PoRep, C2 improved by 5x (without considering storage and maintenance costs throughout sector lifetime)

- 128 bits of security = 0.058 + 0.0253 = 0.0833 ⇒ 128 bits NI / interactive: 0.0833/0.05998 ⇒ NI is 38.8% more expensive

👷 Storage and Maintenance costs

Sector cost are not only related to PC1 ,PC2, C1, C2. Indeed, storage maintenance costs for sectors need to be taken into consideration.

Storage costs

We consider HDD price. Talking with different manufacturers and tier 3 SPs, we got a quite wide range or price per TiB, spanning for 20$/TiB to 38$/TiB.

For this analysis, we assume a reasonable price accessible to SP/SaaS providers to be something close to 30$/TiB with a 5y warranty.

In this case, daily storage cost per sector would be ~0.000567$, resulting in ~0.206955$ yearly storage cost.

Maintenance costs

SPs need to cover maintenance costs associated to sectors: those have to do with proving over time (i.e. `WindowPost`), but also with facilities, labour cost and so on.
For simplicity we consider this costs to be 0 in this analysis (not that each value greater than 0 would results here into a better outcome values for NI-PoRep)

🌈 Putting everything together

We consider a worst case scenario modeled as follows:

- 128 bits of security. Any lower choice of security parameter would translate into a better outcome for NI-PoRep values

- 3y sector duration. Any longer duration would translate into a better outcome for NI-PoRep values

- Storage cost = 30$/TiB with a 5y warranty, resulting in a daily per sector storage cost of ~0.000567$ (i.e. 0.620$ for 3y). Note that any higher storage cost would translate into a better outcome for NI-PoRep values

- PC1 + PC2 + C1 cost = 0.058$ per sector, post SupraSeal software release, according to the analysis above.

- Current C2 cost for Interactive PoRep sectors = 0.0099$ (i.e. pre SupraSeal software release. See analysis above).

- 5x improvement factor given by SupraSeal software for C2. This results into

  - C2 cost = 0.00198$ for an interactive PoRep sector

  - C2 cost = 0.0253$ for a 128 bits of security NI-PoRep sector

  Note that any higher improvement factor would translate into a better outcome for NI-PoRep values]

- Maintenance costs = 0

Assumptions above result into the following costs for Interactive/NI-Porep sectors

Interactive PoRep Sectors

- 0.620$ = Storage costs for sector lifetime (3y)

- 0.058$ = cost of PC1 + PC2 + C1

- 0.00198$ = cost of C2

Total cost per sector = Storage cost for 3y + PC1 + PC2 + C1 + C2 = 0.620$ + 0.058$ + 0.00198$ = 0.67998$

128 bits of Security NI-PoRep Sectors

- 0.620$ = Storage costs for sector lifetime (3y)

- 0.058$ = cost of PC1 + PC2 + C1

- 0.0253$ = cost of C2

Total cost per sector = Storage cost for 3y + PC1 + PC2 + C1 + C2 = 0.620\$ + 0.058\$ + 0.0253\$ = 0.7033\$

This means that the "per sector" difference between an Interactive PoRep Sector and a 128 bits of security NI-PoRep sector is 0.7033\$ - 0.67998\$ = 0.02332\$

⇒ 128 bitsNI-PoRep sectors are ~3.4% more expensive than an interactive PoRep sector, without considering maintenance costs.