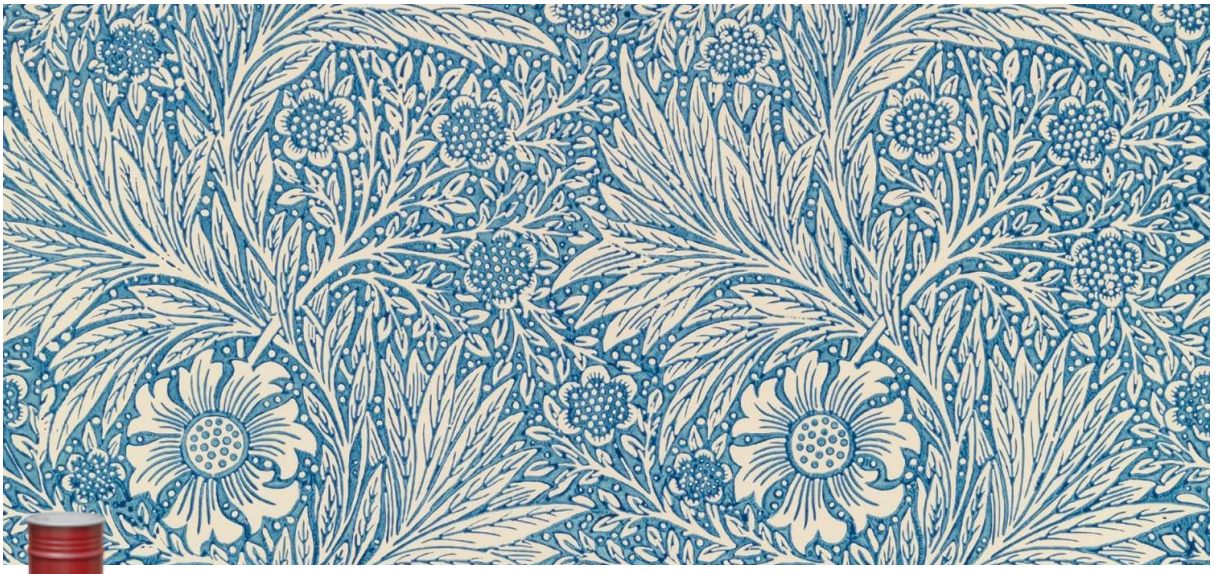

Interactive/Non Interactive-PoRep Gas Cost Comparison

Creator	Luca
Created	@October 18, 2023 6:18 PM
Project	Storage on-boarding

@Luca @Kubuxu

💡 TL;DR: Removing PreCommit makes NI-PoRep and Interactive PoRep gas costs comparable, both for single sectors (where current PoRep is slightly better than NI-PoRep) and for aggregated sector (where NI-PoRep costs are lower than current PoRep ones).

Single Sector

- Considering proof verification only:
  - NI-PoRep with 80 bits of security is ~3.5 times more expensive than current PoRep (114M Vs 34M gas units for proof verification ⇒ difference of 80M gas units).
  - NI-PoRep with 128 bits of security is ~3.6 times more expensive than current PoRep (123M Vs 34M gas units for proof verification ⇒ difference of 89M gas units).
- Considering total gas costs, given that NI-PoRep removes `PreCommit` (and associated gas costs)
  - The difference between NI-PoRep with 80 bits of security and current PoRep goes down to < 27M gas units (114M Vs (34+53)M gas units)
  - The difference between NI-PoRep with 128 bits of security and current PoRep goes down to < 36M gas units (123M Vs (34+53)M gas units)

  Note also that estimated gas cost for `PreCommit` ~53M gas is optimistic (i.e. it is usually higher). This means that the difference between NI-PoRep and current PoRep is probably smaller than estimated in this analysis.

Aggregated Sectors

(i.e. using SnarkPack both for Interactive and NI-PoRep)

- Considering proof verification only
  - NI-PoRep with 80 bits of security when aggregating 6 sectors is 9M gas units more expensive per sector (~1.5x current single proof verification costs).

    - NI-PoRep with 128 bits of security when aggregating 6 sectors is 15M gas units more expensive per sector (~1.9x current single proof verification costs).
- Considering total gas costs, given that NI-PoRep removes `PreCommit` (and associated gas costs), then
    - Current sectors are 2.5x more expensive than NI-PoRep sectors with 80 bits of security (53M + 17M gas units for current sectors, 26M gas units for NI-PoRep sectors).
    - Current sectors are 2.1x more expensive than NI-PoRep sectors with 128 bits of security (53M + 17M gas units for current sectors, 32M gas units for NI-PoRep sectors).

  Note also that estimated gas cost for `PreCommit` ~53M gas is optimistic (i.e. it is usually higher). This means that NI-PoRep is probably performing even better than what this analysis shows, compared with current PoRep.

🌍 Background

PoRep challenges are generated outside Snark Circuits and passed as inputs at verification time. These inputs need to be generated on the spot in order for verification to happen.

With Non Interactive PoRep, the number of challenges is multiplied by a minimum of 8x in order to reach 80 bits of security (wrt to the current 10 we have in PoRep).

These days, 80 bits of security is considered a reasonable parameter, even if for long term security we would recommend to go for 128 buts of security (which would translate in a 12.8x overhead wrt status quo).

📋 Gas cost Analysis: NI-PoRep Vs status quo

We analyze the concrete impact of NI-PoRep proving overhead on gas costs for SPs.

Some aspects to take into account:

- NI-PoRep removes the `PreCommit` step. This means that `PreCommit` gas costs are equal to 0
- We assume we are using SnarkPack to aggregate proofs.
  - Note that today Snarkpack is not really used since, due to how gas is counted for `ProveCommitAggregate`, it is more convenient for SPs to submit single proofs rather than aggregated ones. An overview of this aspect and a proposal for mitigations can be found in Separating proof validation from sector activation (note that this is going to be fixed soon)
- We consider gas costs of a given number of sectors, which proofs get aggregated
- Note that this analysis only considers gas costs associated with verifying proofs on both the Interactive and Non Interactive scenario. We are not considering proving overhead in this doc, but details for 80 and 128 bits of security can be found in 🏗️ NI-PoRep: Proving Overhead Analysis

Useful Resources

- https://docs.google.com/spreadsheets/d/1YxIyvuj1MJka2P7T7KwQj-AXGXBf6KXhFg1SFAtO3Cg/edit#gid=0 is the reference doc for proof fees and gas costs.

  Note that this doc was put together by Kuba, referring to the FVM price list, which was set by empirically testing verification times.

  We'll be using the following values from the aforementioned doc

  - Single proof gas: 49299973 ~ 49M gas units
  - Batch Balancer: 5% of Single proof gas (~2.5M gas units)
  - Proof Submit Charge gas: 34721049 ~34M gas units

  For aggregated proof, gas costs are as follows:

10x **Single Circuit Linear Gas Cost (Single Current PoRep Linear Gas Cost)**
449900

Number of circuits aggregated	Number of Current PoRep aggregated	Gas Cost
≤ 64 = 2^6	6	103994170
≤ 128 = 2^7	12	112356810
≤ 256 = 2^8	25	122912610
≤ 512 = 2^9	51	137559930
≤1024 = 2^10	102	162039100
≤ 2048 = 2^11	204	210960780
≤ 4096 = 2^12	409	318351180
≤ 8192 = 2^13	819	528274980

This means that if we have a number of circuit N which is not a power of two, the total gas cost will be the sum between the gas cost corresponding to $2^{\lceil log_2(N) \rceil}$ and 449900*N

Example: aggregating 6 current PoRep (60 circuits) costs 103994170+ 6*449900, given that $\lceil log_2(34) \rceil = 6$

- **Starboard** is the reference for gas usage of single operations in the Filecoin Network

Single Sector

We compare here gas costs for single sectors, taking into account status quo gas costs and costs for single NI-PoRep sector

C**urrent single sector, no Snarkpack aggregation (not currently used)**

- `PreCommit` ~53 M gas units [approximation obtained by taking *GasUsage/MessageCount* in **Starboard**]
- Snark Verification (10 single snark proofs) at ProveCommit takes ~34M gas units
    - See *Proof Submit Charge gas* in https://docs.google.com/spreadsheets/d/1YxIyvuj1MJka2P7T7KwQj-AXGXBf6KXhFg1SFAtO3Cg/edit#gid=0

NI-PoRep Sectors, 80 bits of security, aggregating sector proofs w/ Snarkpack

- No `PreCommit`

- Snark Verification (80 single snark proofs) at ProveCommit takes ~114M gas units assuming the 80 snark proofs are aggregated with SnarkPack

NI-PoRep Sectors, 128 bits of security, aggregating sector proofs w/ Snarkpack

- No `PreCommit`
- Snark Verification (13 single snark proofs) at ProveCommit takes ~123M gas units assuming the 128 snark proofs are aggregated with SnarkPack

Outcome

- If we consider proof verification only, NI-PoRep proof verification is
  - ~3.5 times more expensive than current PoRep proof verification considering 80 bits of security (114M Vs 34M gas units ⇒ difference of 80M gas units).
  - ~3.6 times more expensive than current PoRep proof verification considering 128 bits of security (123M Vs 34M gas units ⇒ difference of 89M gas units).
- If we consider total gas costs, given that NI-PoRep removes `PreCommit` (and associated gas costs), the difference is goes down to
  - ~27M gas units considering 80 bits of security (114M Vs (34+53)M gas units)
  - ~36M gas units considering 128 bits of security (123M Vs (34+53)M gas units)

Aggregated Sectors

Here we compare gas costs associated with aggregating proofs for multiple sectors. We consider an example of 6 sectors aggregated. Note that differences between interactive and non interactive case would decrease when the number of aggregated sectors increases.

Current Sectors

- `PreCommit` ~53M gas units per sector [approximation obtained by taking `GasUsage/MessageCount` in **Starboard**]
- Snark verification of the aggregation of 6 current sectors (6*10 snark proofs) is

    - Gas cost for 6 current PoRep aggregated + 6* `10x Single Circuit Linear Gas Cost` = 103994170 + 6*449900= 106693570
      ⇒
      17M gas units per sector (without batch balancer).
- Batch balancer is 5% of Single proof gas, which is the 5% of ~49M, resulting in ~2.5M gas units

NI-PoRep Sectors

- No `PreCommit`
- Snark verification of the aggregation of 6 NI-PoRep sectors with 80 bits of security (6*8*10 snark proofs) is
    - Gas cost for 48 current PoRep aggregated + 48* `10x Single Circuit Linear Gas Cost`
      = 137559930 + 48*449900 = 159155130
      ⇒
      26M gas per sector.
- Snark verification of the aggregation of 6 NI-PoRep sectors with 128 bits of security (6*12.8*10 snark proofs) is
    - Gas cost for 77 current PoRep aggregated + 77* `10x Single Circuit Linear Gas Cost`
      = 162039100 + 77*449900 = 196681400
      ⇒ 32
      M gas per sector.

Outcome

- If we consider proof verification only we have
    - NI-PoRep proof verification when aggregating 6 sectors with 80 bits of security is 9M gas units more expensive per sector (~1.5x current single proof verification costs).
    - NI-PoRep proof verification when aggregating 6 sectors with 128 bits of security is 15M gas units more expensive per sector (~1.9x current single proof verification costs).
- If we consider total gas costs, given that NI-PoRep removes `PreCommit` (and associated gas costs), then

- Current sectors are at least 2.5x more expensive than NI-PoRep sectors with 80 bits of security (53M + 17M gas units for current sectors, 26M gas units for NI-PoRep sectors).
- Current sectors are at least 2.1x more expensive than NI-PoRep sectors with 128 bits of security (53M + 17M gas units for current sectors, 32M gas units for NI-PoRep sectors with 128 bits of security).