Introduction

In the landscape of data availability layers (DALs), the optimization of gas costs on the L1 stands as a paramount concern for enhancing operational efficiency. A notable advancement in this pursuit comes with the integration of the newly added EIP4844 point evaluation precompile within data availability networks. This crucial update holds the potential to significantly improve gas costs on Layer 1 (L1) for verification processes, which is particularly advantageous for Rollups. The solution significantly slashes gas costs for verification processes. Unlike the resource-intensive Merkle inclusion proof, which often demands over 100k gas, this innovative approach drastically reduces the overhead to a mere 50k gas. This reduction not only enhances the affordability of smart contract operations but also simplifies their complexity, making them more accessible to developers. By embracing this solution, Rollups can unlock unprecedented efficiencies, marking a pivotal advancement towards a more scalable and cost-effective decentralized ecosystem.

Terms

batch

- list of transactions within a Rollup. Data is not interpreted by the DAL.

versioned_hash

- 1 byte for version: 0x1
- the last 31 bytes of sha256(batch)

Flow

1. Rollup sends batch

to the Data Availability (DA) Network

1. DA network reaches consensus, sends signatures + versioned_hash

to L1DataRootOracle

1. Rollup verifies a batch on L1 by identifying it by batchId
2. Point precompile constituents (versioned_hash | z | y | commitment | proof

) for Data availability verification to L1Verifier

1. L1RollupVerifier

pulls relevant data root from L1DataRootOracle

1. L1RollupVerifier

executes Point evaluation precompile using fetched versioned_hash

and constituents.

Cost implications

Utilizing this approach, Data availability layers can save on proof verification costs, since the Point precompile costs 50k gas as oposed to a Merkle Inclusion Proof (MIP) that costs 100k+ gas.