AIONET — Executive Summary

Hardware-Anchored Finality with PoM & PoD

AIONET Research

August 18, 2025

TL;DR AIONET is an AI-native L1 that anchors consensus in physical memory behavior. **Proof of Memory (PoM)** validates blocks by measuring high-speed HBM-DRAM operations. **Proof of Drift (PoD)** scores validator health from entropy/drift fingerprints to resist spoofing/cloning. Finality is the max of a compute/bandwidth term and a network/coordination term, yielding **sub-2s target finality** with **ultra-low fees**. As HBM bandwidth scales, compute time shrinks; PoD keeps identity honest over time.

Model (concise)

Effective throughput:

$$\Theta_{\text{mem}} = B \cdot N \cdot P \cdot \eta \cdot V, \qquad T_{\text{compute}} = \frac{D}{\Theta_{\text{mem}}}.$$

Network term:

$$T_{\text{network}} = R \cdot \text{RTT} + \Delta.$$

Finality:

$$T_{\text{final}} \approx \max\big(T_{\text{compute}} + \delta_{\text{PoD}},\ T_{\text{network}}\big).$$

Why it scales

- **Physics bounded:** HBM bandwidth growth reduces T_{compute}.
- **Security via behavior:** PoD's entropy/drift fingerprinting ties weight to honest hardware.
- **Composable:** Works under standard mempool/committee plumbing; batching & zk options.

Illustrative HBM trend

HBM Gen	Bandwidth/stack	Channels (N)	PoM compute time (indicative)
HBM3e	1.2 TB/s to 1.4 TB/s	8–16	$\sim$1.5 s to 2.0 s
HBM4	2 TB/s to 3 TB/s	16–32	$\sim$0.8 s to 1.2 s
HBM8*	$\geq$4 TB/s (proj.)	32–64+	$<$ 0.3 s (theoretical)

Threat model highlights

Hardware spoofing/cloning resisted by PoD similarity thresholds; replay checked by signed PoM/PoD commitments; byzantine tolerance with anomaly scoring. Optional zk bindings enable succinct cross-chain proofs.

Read more

- Final derivations and threat model: Full_Finality_Analysis.pdf
- Science & Vision: AIONET_Science_and_Vision.pdf

Figures are indicative targets; real performance depends on network conditions and implementation.