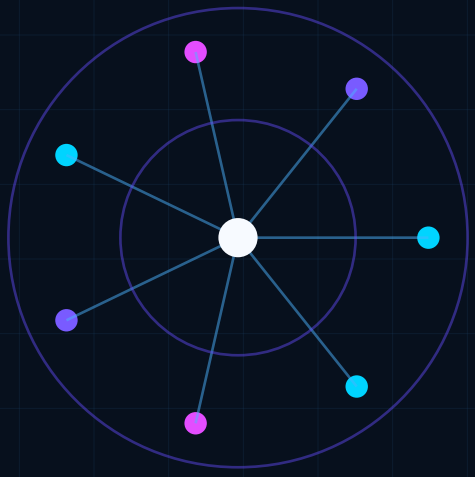
DECENTRALIZED INFRASTRUCTURE

Decentralized Physical Infrastructure Networks (DePIN) Compute Models

Current-source review, evidence-bounded adoption decision, explicit limitations, reproducibility controls, and preserved source research note.



PERMANENT ID	EVIDENCE	ADOPTION	FRESHNESS
RES-025	B-	MONITOR - DO NOT USE FOR ASSE	ACTIVE WATCH

Freshness review: 2026-09-17 / Next scheduled review: 2026-12-16

RESEARCH CONTROL SURFACE

Required Research Fields

Each field remains independently reviewable; evidence strength does not imply production authority.

EVIDENCE GRADE — **B-**

Strength of the retained source set and technical basis.

SOURCE AUTHORITY — **3 registered authorities**

Akash Network Documentation; Helium Documentation; Confidential Computing Consortium

FRESHNESS — **ACTIVE WATCH**

Reviewed 2026-09-17; dynamic sources require event-driven revalidation.

CONFLICTS — **VISIBLE / NOT SILENT**

Differences between specification, vendor behavior, research claims, and reproduced evidence must remain explicit.

LIMITATIONS — **EXPLICIT**

No certification, procurement approval, legal conclusion, or unbounded production claim is created by this report.

REPRODUCIBILITY — **REQUIRED**

Material claims require exact versions, representative data, failure cases, artifacts, and repeatable acceptance criteria.

ADOPTION POSTURE — **MONITOR - DO NOT USE FOR SENSITIVE WORKLOADS**

Monitor DePIN economics and scheduling. Do not place secrets, regulated data, proprietary models, or high-integrity workloads on untrusted nodes without independently verified confidentiality and execution.

REVIEW TRIGGER — **2026-12-16**

Scheduled at 90 days; earlier on material source, vulnerability, implementation, or contradictory-evidence change.

SOURCE AUTHORITY / FRESHNESS

Authority Register and Freshness Delta

Primary-source lineage is preserved; current-source changes are separated from unperformed implementation claims.

AUTHORITY 01

Akash Network Documentation

https://akash.network/docs/

AUTHORITY 02

Helium Documentation

https://docs.helium.com/

AUTHORITY 03

Confidential Computing Consortium

https://confidentialcomputing.io/

2026-09-17 FRESHNESS DELTA

Primary-source register retained and freshness controls advanced to the current review date. No new product or laboratory performance claim is introduced without reproduced evidence.

Freshness policy: scheduled review + immediate review on source supersession, material release, vulnerability, retraction, or contradictory evidence.

Evidence Must Survive Contact With Reality

- Source authority is not implementation evidence. Product behavior, scale, security, interoperability, and operator fit remain environment-specific.
- Conflicting evidence is recorded rather than averaged away. Specification behavior, vendor implementation, preprint results, and production observations are separate evidence classes.
- Quantitative claims are informative until reproduced under documented hardware, software, data, topology, load, and failure conditions.
- Adoption posture is reversible. A stronger source set can coexist with a pilot-only or research-only recommendation when maturity, safety, economics, or operability remain unresolved.

ADOPTION / VALIDATION / REVIEW

Decision Gate and Validation Plan

ADOPTION POSTURE

MONITOR - DO NOT USE FOR SENSITIVE WORKLOADS

Monitor DePIN economics and scheduling. Do not place secrets, regulated data, proprietary models, or high-integrity workloads on untrusted nodes without independently verified confidentiality and execution.

1 / SOURCE	Pin exact versions, publication state, retrieved artifacts, and source hashes.
2 / PROTOTYPE	Demonstrate the core mechanism with representative data and instrumented execution.
3 / FAILURE	Exercise malformed input, dependency loss, stale state, overload, recovery, rollback, and misuse.
4 / BASELINE	Compare against an incumbent, classical, or simpler architecture using the same workload.
5 / ACCEPT	Record acceptance criteria, residual limitations, owner, expiration, and revalidation triggers.

EXPIRATION / REVIEW TRIGGER

Next scheduled review: 2026-12-16 (90-day cadence). Review sooner after material source revision, breaking implementation release, critical vulnerability, retraction, benchmark contradiction, changed workload, or changed legal/safety boundary.

8. Complete Source Research Note

SOURCE-LINEAGE NOTICE

The following material preserves the complete original source note, excluding only the conversational wrapper and outer Markdown fence. Legacy status labels and absolute language are retained for traceability and do not override the candidate status, limitations, or adoption decision in this edition.

Document ID: RES-025 Version: 1.0.0 (Definitive Registry Edition) Status: Published Research Note Classification: Public Organization: Mythos Systems (MYTHOS AI) Owner: Aaron Stovall Effective Date: 2026-07-16 Applies To: Sovereign infrastructure architects, Web3/decentralized compute engineers, and security professionals designing verifiable distributed AI pipelines, zero-trust compute markets, and air-gapped burst-compute environments Companion Standards: MYTHOS-CLD-0009 (DePIN Standard), MYTHOS-EMT-0002 (Sovereign AI), MYTHOS-SEC-0009 (Confidential Computing), MYTHOS-SEC-0010 (FHE & ZKP), MYTHOS-HW-0002 (Trusted Compute)

The architecture of cloud computing has been crippled by monopolistic centralization. Organizations are forced to surrender their proprietary AI weights and data to a handful of centralized cloud providers (AWS, Azure, GCP) to access massive GPU compute. This model destroys data sovereignty, creates single points of failure, and locks organizations into vendor-controlled pricing.

Decentralized Physical Infrastructure Networks (DePIN) offer an alternative: a global, blockchain-validated market of distributed compute nodes. However, naively sending proprietary workloads to anonymous, internet-connected GPUs is a catastrophic security failure. An anonymous node operator can easily exfiltrate model weights or return hallucinated, unexecuted inference results.

This research note defines the architectural dynamics of Sovereign DePIN Compute. It dissects the mechanics of smart-contract Service Level Agreements (SLAs), Proof of Compute (PoC) via Zero-Knowledge Proofs (zk-ML) and Trusted Execution Environments (TEEs), and the cryptographic attestation required to enable highly secure, air-gapped organizations to safely bid on distributed compute. Understanding these dynamics is a prerequisite for building the verifiable, zero-trust decentralized compute fabrics mandated by the Mythos Cloud Standards.

To utilize decentralized compute securely, we must map how a compute workload is advertised, bid upon, executed, and verified on a blockchain.

1.1 The Compute Bidding Protocol (Smart Contracts)

DePIN compute is governed by smart contracts acting as an automated escrow and matching engine.

- The Mechanic: A sovereign organization submits an encrypted compute request (e.g., "Inference for Model X on Encrypted Input Y for Z tokens"). Decentralized node operators stake collateral and bid on the contract. The smart contract automatically matches the bid to the highest-staked, lowest-latency node.
- The SLA Enforcement: If the node fails to return the result within the block time, or if the result fails cryptographic verification, the smart contract automatically slashes the node's staked collateral.

1.2 Proof of Compute (PoC)

A node cannot simply return a JSON payload and claim it ran a 70-billion parameter model. The network must mathematically verify the execution.

- The Mechanic: The node must return the result alongside a cryptographic proof. This is achieved via zk-ML (Zero-Knowledge Machine Learning) or TEE Remote Attestation. The blockchain's consensus layer verifies the proof before releasing the escrowed payment to the node.

1.3 Sybil Resistance & Hardware Attestation

A single attacker could spin up 1,000 virtual nodes to monopolize the network.

- The Mechanic: DePIN networks MUST require Proof of Physical Work (PoPW) or hardware-bound attestation. Nodes must provide a TPM 2.0 or TEE signature proving they are running on physical, unique silicon, preventing virtual Sybil cloning.

While DePIN breaks the cloud monopoly, it introduces severe physical and security constraints that centralized clouds abstract away.

2.1 The Untrusted Node Problem (Model Exfiltration)

An anonymous node operator receives a proprietary AI model to execute. The operator can easily copy the `.safetensors` weights from system RAM and sell them to a competitor.

- The Flaw: Standard API-based compute guarantees data exfiltration if the endpoint is compromised.
- The Mitigation: DePIN compute MUST utilize TEEs (Intel TDX / AMD SEV-SNP). The model is encrypted in transit and only decrypted inside the hardware-isolated enclave. The node operator's host OS and hypervisor cannot read the weights.

2.2 Network Topology and Jitter

Centralized datacenters possess uniform, 400Gbps non-blocking spine-leaf fabrics. DePIN nodes are scattered across the globe on consumer broadband and varied ISPs.

- The Constraint: Distributed training (which requires microsecond All-Reduce synchronization) is physically impossible across a DePIN mesh due to jitter and latency.
- The Mitigation: DePIN compute MUST be restricted to embarrassingly parallel workloads (e.g., batch inference, hyperparameter search, data parallelization) where nodes do not need to synchronize state.

2.3 Economic Volatility (The SLA Stability Problem)

If a DePIN network's native token crashes in value, node operators will instantly turn off their machines to avoid electricity costs, halting global compute mid-workflow.

- The Constraint: Volatile tokenomics cannot guarantee enterprise SLAs.
- The Mitigation: The smart contract SLA MUST be denominated in a stablecoin or dual-token architecture. Furthermore, the compute orchestrator MUST implement checkpointing; if a node drops offline, the durable runtime (Temporal/Clio) seamlessly re-bids the workload to another node without losing state.

The true power of a Mythos-compliant DePIN architecture is realized when highly secure, air-gapped environments (e.g., DoD, classified enterprise) can safely leverage external, decentralized compute without breaching their physical perimeter.

3.1 The Data Diode Bid

An air-gapped organization cannot connect to the public internet to query a DePIN network.

- The Mechanic: The organization utilizes a one-way data diode. The compute request (an FHE-encrypted prompt and a ZK-verification key) is pushed through the diode to a gateway node. The gateway node interacts with the DePIN smart contract, bids on the compute, and waits for the result.
- The Impact: The air-gapped organization leverages global compute power, but the physical network boundary is never breached. The data flowing back through the diode is mathematically verified (ZKP) and encrypted (FHE).

3.2 Fully Homomorphic Encryption (FHE) on DePIN

Even with TEEs, some organizations classify the hardware itself as untrusted.

- The Mechanic: The organization encrypts the prompt and the model using FHE. The DePIN node executes the inference homomorphically. The node never possesses the decryption key.
- The Impact: The compute is mathematically blind. The node returns an encrypted result, which the air-gapped organization decrypts locally. The DePIN node could be owned by a hostile nation-state, and the data would remain perfectly secure.

The fundamental shift of DePIN compute is the transition from "trust the cloud provider" to "trust the math."

- Burst Compute: An organization training a 1-trillion parameter model can burst 50% of the hyperparameter search to a DePIN network, cutting cloud costs by 80% while maintaining cryptographic proof of execution.
- Censorship Resistance: A sovereign AI researcher in a heavily regulated jurisdiction can publish their model to a DePIN network. Because the nodes are decentralized and the smart contracts are autonomous, no single government can force a takedown of the compute.
- Verifiable AI: When an agent retrieves an inference result from a DePIN node, it attaches the ZK-proof or TEE-attestation to its Evidence Bundle. The downstream consumer can mathematically verify that the AI output was generated by the correct, unmodified model on the correct input.

To deploy DePIN compute in production, the Mythos Architecture enforces strict orchestration and verification boundaries.

5.1 The DePIN Routing Gateway

The PANTHEON Nona (Planner) module MUST NOT directly interact with a blockchain RPC.

- The Mitigation: The architecture MUST utilize a DePIN Routing Gateway. Nona proposes a standard tool call. The Gateway intercepts it, formats it into a DePIN smart-contract bid, manages the escrow, verifies the ZK-proof/attestation returned by the node, and passes the result back to Nona. The cognitive loop is completely abstracted from the blockchain mechanics.

5.2 Mandatory Verification Gates

No DePIN compute result enters the active memory graph (Mnemosyne) without passing a verification gate.

- The Mitigation: If the DePIN node returns a result lacking a valid TEE attestation quote or a valid zk-STARK proof, the Routing Gateway instantly drops the result, slashes the node via the smart contract, and re-bids the workload. Zero unverified data touches the core agent state.

5.3 Stable Economic Quorums

To prevent token volatility from crashing the compute pipeline, the Mythos architecture mandates economic abstraction.

- The Mitigation: The organization pre-funds a smart-contract wallet with stablecoin. The DePIN Routing Gateway draws from this pool. The node operators are paid in stablecoin, insulating them from token volatility and ensuring enterprise-grade uptime guarantees.

Decentralized Physical Infrastructure Networks break the centralized cloud monopoly, offering limitless, censorship-resistant compute. However, leveraging anonymous hardware for sovereign AI requires absolute cryptographic enforcement. By combining smart-contract SLAs, TEE hardware isolation, and Zero-Knowledge verifiability, we transform a chaotic mesh of internet-connected GPUs into a mathematically verifiable, zero-trust compute utility. In a Mythos-compliant architecture, the compute provider does not need to be trusted; the math guarantees the result.

```
A centralized cloud is a monopoly; a DePIN mesh is a market.
```

```
An anonymous node is a thief; a TEE enclave is a vault.
A JSON response is a claim; a ZK proof is a settlement.
A volatile token is a risk; a stablecoin SLA is a guarantee.

The compute is decentralized; the verification is absolute.

> Nodes may be anonymous.
> Cryptographic provenance must be absolute.
```

End of Research Note RES-025

9. Source Register

Source	Authority and Status	Freshness Control
Akash Network Documentation https://akash.network/docs/	Primary network documentation Living Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
Helium Documentation https://docs.helium.com/	Primary network documentation Living Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
Confidential Computing Consortium https://confidentialcomputing.io/	Primary industry consortium Living Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.

10. Lineage, Review, and Publication Record

Record	Value
Original source file	RES-025_DePIN_Compute_Models.md
Original source words	1528
Upgrade type	Enterprise research report; source and freshness validation; limitations; adoption decision; reproducibility plan
Generated on	2026-07-22
Current status	Candidate Research Report
Publication authority	Formal Mythos approval not yet recorded
Next review	90 days or event-driven trigger, whichever occurs first