Nick Clark · Published June 22, 2026 · PDF

Anduril Lattice Mesh: Defense-Grade Mesh, Without Carried Authority

Lattice Mesh is the most visible commercial mesh-networking play in defense, built for the contested, multi-vendor, intermittently connected environments where conventional networking fails. It proves the market: mesh data fabric for autonomy is now a category. But it treats packets as payload, not as carriers of their own routing and governance.

Vendor and Product Reality

Anduril's Lattice is the company's software platform for autonomy and command-and-control, and Lattice Mesh is its data-fabric layer: a way for heterogeneous defense platforms, drones, sensors, ground vehicles, and command nodes from multiple vendors, to share data with one another in a decentralized way, without routing everything through a central server. It is built precisely for the environments where conventional networking fails: contested electromagnetic conditions, intermittent connectivity, and multi-vendor coalitions where no single cloud is reachable or trusted by everyone. Lattice Mesh is the most visible commercial expression of an idea this body of work also holds: that autonomy at the edge needs a decentralized data fabric, not a hub. Its prominence proves the market. Mesh data sharing for autonomy is now a category, and a serious one.

The agreement is genuine and worth stating before the divergence. Both Lattice Mesh and the memory-native protocol reject the central server as the place where coordination happens, and both target the contested, multi-vendor, partition-prone conditions of real operations. The difference is what a packet is permitted to be.

The Architectural Choice: Packets as Payload

In a mesh built on conventional principles, however decentralized, the data unit is payload and the governance lives in the nodes. Routing decisions, access-control rules, and trust state are held in node-resident configuration, and a packet is the thing moved between nodes that hold that configuration. This works well when the nodes are consistently configured and reachable, and it is the architecture that mature mesh fabrics optimize. But it locates authority in the node rather than in the data, which means a packet arriving at a node is governed by whatever that node currently believes, and the consistency of those beliefs across a contested, multi-vendor mesh is exactly what partition and adversary conditions disrupt. The packet carries data; it does not carry the rules for its own handling.

What the Memory-Native Primitive Provides

The memory-native protocol makes the data unit a self-governing operand. Every message carries a governed envelope: an authority-taxonomy field naming the credentialing authority and the scope of the asserted permission; a dynamic-device-hash continuity field anchoring the originating device's credential history without a real-time revocation fetch; a hop-history relay field recording the chain of nodes that handled the message under their own credentials; and a store-and-forward propagation field that preserves freshness, scope, and authority across partition events. A governance class field at a fixed wire offset lets any node locate and act on the message's handling regime before it parses the payload, and an opaque relay is required only to preserve that field bit-for-bit. Routing scope, mutation policy, trust window,

and lineage travel inside the unit, so a receiving node evaluates a message against the authority the originator declared rather than against the node's own possibly-stale configuration, and it does so locally, without a round-trip. The nodes become generic executors of governance the packet carries.

Complementary at the Problem, Divergent at the Wire

Lattice Mesh and the memory-native protocol are fighting the same battle under different doctrine. At the level of the problem, decentralized data sharing for autonomy in contested, multi-vendor environments, they are aligned, and a platform like Lattice is exactly the kind of system that could carry a governed envelope as opaque payload over its existing fabric. At the level of wire-architecture they diverge: node-resident governance over packets-as-payload, versus carried governance in packets-as-operands. The envelope rides above any transport, so the divergence is composable rather than exclusive: a mesh optimized for decentralized delivery can transport self-governing data units and gain per-message carried authority without changing its routing. No relationship, endorsement, or infringement is asserted; the comparison is architectural.

Disclosure Scope

The memory-native protocol, in which the data unit carries a governed envelope encoding authority, scope, device-hash continuity, hop history, and store-and-forward propagation, and in which nodes evaluate carried governance locally without a central authority, is disclosed in the protocol filing (U.S. Application No. 19/366,760, published as US 2026/0052096 A1). This article compares that disclosed mechanism with Anduril's publicly described Lattice Mesh data fabric and positions carried, packet-resident governance as complementary to a decentralized delivery fabric. References to Anduril and Lattice are to public materials and are used for comparison only.

Memory-Native Protocol (/memory-native-protocol)

All 36 steps → (/inventive-steps)

Authority intrinsic to the object. Routing by semantic properties.

PRIMARY TECHNICAL DISCLOSURE

- Memory-Native Networking: A Cognition-Compatible Protocol Substrate (/articles/memory-native-networking-a-cognition-compatible-protocol-substrate)

SECONDARY TECHNICAL

- Protocol-Native Carriers: Agents as the Fundamental Unit of Transmission (/articles/memory-native-protocol/protocol-native-carrier)
- Dynamic Routing Protocol: Memory-Aware Path Selection for Semantic Agents (/articles/memory-native-protocol/dynamic-routing)
- Trust-Weighted Route Scoring: Dynamic Path Selection Through Policy-Defined Trust Thresholds (/articles/memory-native-protocol/trust-weighted-routing)
- Network Health Monitoring System: Signed Health Agents as Distributed Operational Telemetry (/articles/memory-native-protocol/network-health-monitoring)
- Health Agents as Semantic Objects: Operational Metrics That Route Like Any Other Agent (/articles/memory-native-protocol/health-agents)
- Dynamic Indexing Protocol: Entropy-Driven Restructuring of Semantic Flows (/articles/memory-native-protocol/dynamic-indexing)
- Soft-Index Anchors: Ephemeral Index Points Inferred From Agent Lineage (/articles/memory-native-protocol/soft-index-anchors)
- Adaptive Consensus Protocol: Memory-Native Quorum Without Fixed Validator Sets (/articles/memory-native-protocol/adaptive-consensus)
- Trust-Weighted Voting in ACP: Domain-Scoped Votes Accumulated Against Agent Memory (/articles/memory-native-protocol/acp-trust-voting)
- Dynamic Alias Resolution: Zone-Local Semantic Aliases Resolved Through Transport Headers (/articles/memory-native-protocol/alias-resolution)
- Horizontally Composable Protocol Stack: Independent Layers Operating in Parallel (/articles/memory-native-protocol/composable-stack)
- Transport-Layer Agnosticism: One Protocol Stack Above Any Carrier (/articles/memory-native-protocol/transport-agnosticism)

- Federated Semantic Zone Deployment: Heterogeneous Nodes Coordinating Across Trust Boundaries (/articles/memory-native-protocol/federated-zones)
- Health-Triggered Quorum Adjustment: Dynamic Thresholds From Network Stability Signals (/articles/memory-native-protocol/health-triggered-quorum)
- Authority Credential as a First-Class Field on the Wire (/articles/memory-native-protocol/governed-mesh-wire-format)
- Hop-History Relay and Byzantine Custody Chain (/articles/memory-native-protocol/hop-history-relay)
- Dynamic Device Hash Continuity Without CRLs or OCSP (/articles/memory-native-protocol/dynamic-device-hash-continuity)
- Rateless Forward-Error-Correction for Lossy Mesh Media (/articles/memory-native-protocol/rateless-fec-fountain)
- Mobile Store-and-Forward Without Cellular Backhaul (/articles/memory-native-protocol/mobile-store-and-forward)
- Credentialed Firmware and Policy Distribution Through the Mesh (/articles/memory-native-protocol/firmware-via-mesh)

APPLICATIONS · GENERAL

- Edge Computing Without Central Routing Authority (/articles/memory-native-protocol/edge-routing)
- IoT Device Mesh Governance at Scale (/articles/memory-native-protocol/iot-mesh)
- Vehicle-to-Vehicle Communication With Intrinsic Governance (/articles/memory-native-protocol/autonomous-vehicle-networking)
- Military Mesh Networks Without Central Routing Authority (/articles/memory-native-protocol/military-mesh-networks)
- Smart City Infrastructure With Self-Governing Transport (/articles/memory-native-protocol/smart-city-infrastructure)
- Satellite Communication With Delay-Tolerant Governance (/articles/memory-native-protocol/satellite-communication)
- Industrial IoT Protocols With Embedded Authority (/articles/memory-native-protocol/industrial-iot-protocols)
- Healthcare Device Mesh Networking (/articles/memory-native-protocol/healthcare-device-mesh)
- Contested-Mesh Radio for Defense and Public Safety (/articles/memory-native-protocol/contested-mesh-radio)
- Expeditionary Mesh for GNSS-Denied Operations (/articles/memory-native-protocol/expeditionary-mesh)

- Maritime, Agricultural, and Mining Mesh Without Cellular (/articles/memory-native-protocol/maritime-iot-mesh)
- The Mesh Ceiling: Why Packet-as-Payload Networks Plateau (/articles/memory-native-protocol/carried-authority-ceiling)
- The Malicious Host Problem, Reframed: Attribution, Quorum, and Routing Beat a Compromised Node (/articles/memory-native-protocol/malicious-host-contained)
- Beyond Jamming: Autonomy in Space, Deep Disconnection, and Delay-Tolerant Networks (/articles/memory-native-protocol/disconnected-and-interplanetary)

APPLICATIONS · SPECIFIC

- Starlink Built a Satellite Mesh. The Routing Authority Is Still Terrestrial. (/articles/memory-native-protocol/starlink)
- Zigbee Built a Mesh Protocol for IoT. The Messages It Carries Have No Memory. (/articles/memory-native-protocol/zigbee)
- Matter Unified Smart Home Devices. The Protocol Still Separates Data From Authority. (/articles/memory-native-protocol/matter)
- Helium Decentralized Wireless Coverage. The Protocol That Uses It Did Not Follow. (/articles/memory-native-protocol/helium)
- LoRaWAN Solved Long-Range IoT. The Messages Are Still Passive Payloads. (/articles/memory-native-protocol/lorawan)
- Tailscale Made WireGuard Usable. The Coordination Server Still Holds the Authority. (/articles/memory-native-protocol/tailscale)
- QUIC Modernized Transport. The Protocol Carries No Semantic Authority. (/articles/memory-native-protocol/quic-protocol)
- MQTT Connected Billions of IoT Devices. The Broker Still Holds the Authority. (/articles/memory-native-protocol/mqtt)
- CoAP Brought REST to Constrained Devices. The Protocol Carries No Governance Semantics. (/articles/memory-native-protocol/coap)
- gRPC Made Service Communication Type-Safe. The Protocol Carries No Trust Semantics. (/articles/memory-native-protocol/grpc)
- ZeroMQ Eliminated the Broker. Routing Authority Still Lives in Application Code. (/articles/memory-native-protocol/zeromq)
- WireGuard Simplified VPN Tunnels. The Protocol Has No Semantic Routing Layer. (/articles/memory-native-protocol/wireguard)
- Nebula Built Overlay Mesh Networks. The Certificate Authority Is Still Central. (/articles/memory-native-protocol/nebula-mesh)

- Calico Enforces Network Policy at the Kernel Level. Policy Authority Is Still External. (/articles/memory-native-protocol/calico)
- Cilium Made eBPF the Network Data Plane. The Protocol Layer Carries No Governance. (/articles/memory-native-protocol/cilium)
- Weave Net Built a Virtual Network for Containers. The Protocol Carries No Semantic Authority. (/articles/memory-native-protocol/weave-net)
- Persistent Systems Wave Relay Hardens Mesh Without Authority Semantics (/articles/memory-native-protocol/persistent-systems)
- Silvus StreamCaster Solves the Radio Layer, Not the Trust Layer (/articles/memory-native-protocol/silvus-streamcaster)
- Rajant Kinetic Mesh Has Mobility, Lacks Credential Authority (/articles/memory-native-protocol/rajant-kinetic-mesh)
- Trellisware TSM Optimizes Routing, Not Authority Resolution (/articles/memory-native-protocol/trellisware-tsm)
- Autotalks Craton2 Is V2X Silicon Without Governance (/articles/memory-native-protocol/autotalks-craton2)
- Qualcomm 9150 C-V2X Authenticates Messages, Not Behavioral Authority (/articles/memory-native-protocol/qualcomm-9150)
- NXP RoadLink Implements DSRC, Not the Authority Taxonomy (/articles/memory-native-protocol/nxp-roadlink)
- Chroma Vector Database (/articles/memory-native-protocol/chroma-vector-db)
- Milvus Vector Database (/articles/memory-native-protocol/milvus-vector-db)
- Pinecone Vector Database (/articles/memory-native-protocol/pinecone-vector-db)
- Qdrant Vector Database (/articles/memory-native-protocol/qdrant-vector-db)
- Weaviate Vector Database (/articles/memory-native-protocol/weaviate-vector-db)
- **Anduril Lattice Mesh: Defense-Grade Mesh, Without Carried Authority (/articles/memory-native-protocol/anduril-lattice-mesh)**
- Hivemind: Onboard Autonomy Without an Onboard Authority Substrate (/articles/memory-native-protocol/shield-ai-hivemind)

Memory-Native Protocol overview → (/memory-native-protocol)