Nick Clark · Published April 25, 2026 · PDF

IOTA (Tangle) alternative: agent-carried trust without a shared ledger

IOTA and its Tangle are built to give machine-to-machine networks a feeless, DAG-based distributed ledger for recording value and data. That model answers a specific question: how do many participants converge on one agreed ledger. A different question is how a message can carry its own verifiable history, policy, and routing rules so that no shared ledger is needed at all. That is the axis addressed by the Memory-Native Protocol, disclosed in United States Patent Application 19/366,760.

What IOTA (Tangle) Does

IOTA is a distributed ledger project designed for the Internet of Things and machine-to-machine settings. Its distinguishing data structure is the Tangle, a directed acyclic graph in which each new transaction references and approves prior transactions, rather than the linear chain of blocks used by conventional blockchains. This DAG design is intended to remove the separation between users and validators, so that participants who submit transactions also help confirm earlier ones.

IOTA is well known for two goals in particular. First, it targets feeless transactions, which makes it attractive for very small or very frequent transfers of value and data among devices. Second, it aims for scalability that improves rather than degrades as more participants join, since more submitters can mean more approvals. The project has invested substantial engineering effort in moving away from its early reliance on a network Coordinator toward a more fully decentralized consensus, a direction the IOTA community has described under the Coordicide and IOTA 2.0 programs.

These are real strengths for their intended purpose. A feeless, DAG-structured ledger is a thoughtful answer to the problem of recording value and data among many devices without the fee and throughput friction of classic chains. Nothing here is a criticism of IOTA. The point of this comparison is that the Tangle and the Memory-Native Protocol answer structurally different questions, and it is worth being precise about which question each one solves.

The Architectural Axis

The axis is where authoritative state lives.

IOTA, like other distributed ledger technologies, is organized around a shared record. The Tangle is a common structure that participants extend and, over time, converge upon. Confirmation is a property of the graph as a whole: a transaction gains weight and finality because other participants reference and approve it within the shared DAG. Value comes precisely from the fact that everyone is, in the end, talking about the same ledger. That is what makes it a ledger.

The Memory-Native Protocol addresses a different axis. It is not trying to be a better shared ledger; it is asking whether a shared ledger is required at all for a message to carry verifiable trust. In many distributed settings, particularly federated, delay-tolerant, or cross-organizational ones, the constraint is not that participants disagree about a ledger, but that there is no single ledger they can all reach, synchronize with, or agree to be governed by. Different domains bring their own policies and trust models, connectivity is intermittent, and there may be no shared infrastructure to converge on in the first place.

This is a difference in structure, not a defect in either approach. IOTA optimizes convergence on a common record. The disclosed approach optimizes the message so that convergence on a common record is not a precondition for verifiable behavior.

How the Disclosed Approach Differs

In the Memory-Native Protocol, the unit of transmission and execution is a memory-bearing agent rather than a ledger entry. Each agent carries a unique identifier, a payload, a transport header, a cryptographic signature, and an append-only memory field. The memory field holds a signed lineage record, access logs, and references to policy agents that govern what mutations, routing, and consensus participation are permitted. Every entry in the memory field is individually signed by the contributing node and hash-chained, so the history and its ordering are verifiable by any node that receives the agent, using only what the agent carries.

Because the trust context travels inside the message, the protocol stack at each node acts on agent-resident data. The dynamic routing protocol chooses next hops from trust scores, access history, and policy-aligned propagation boundaries embedded in the agent, rather than from global routing tables. The adaptive consensus protocol is the sharpest contrast with a ledger model: it lets nodes evaluate a mutation proposal carried by an agent without relying on centralized coordination or globally synchronized state. As the specification puts it, consensus can be entirely scoped to the identity, memory, and mutation context of a single agent, with each node evaluating its own eligibility, voting weight, and policy alignment from the agent's embedded policy references. There is no fixed validator set and no persistent governance registry required; quorum is dynamically scoped per proposal.

The specification is explicit about the federated case. The substrate can operate across administrative boundaries without requiring shared infrastructure or synchronized ledgers, with each domain defining its own policies and trust models while behavioral compliance is enforced through agent-carried rules and verifiable metadata. It is also explicit about the delay-tolerant case: because each agent carries all necessary context, including policy, mutation proposal, quorum metadata, and routing constraints, agents can propagate and be validated even after long delays, which suits environments with intermittent connectivity or no centralized coordination. This is a store-carry-forward posture in which the message remains authoritative regardless of whether any common ledger is reachable.

Where They Fit Together

These are complementary more often than they are rivals. If an application needs a canonical, shared record of value or data that many parties treat as the single source of truth, a distributed ledger such as IOTA is a natural fit, and its feeless, DAG-based design is well suited to high-frequency device traffic. The Memory-Native Protocol does not attempt to replace that role and does not itself define a settlement ledger.

Conversely, where the need is to move governed, self-describing messages across trust domains that will not, or cannot, share one ledger, the disclosed substrate provides per-message trust, policy, and consensus that do not depend on global convergence. One can imagine the two composed: agents governed by the disclosed protocol could reference a ledger such as IOTA for the specific facts that genuinely warrant a shared, canonical record, while routing, policy enforcement, and scoped mutation validation for the message itself remain agent-carried. The substrate is transport-agnostic and can run over existing networks, so integration with ledger-backed systems does not require replacing either side.

Boundary Conditions

Honesty about limits cuts both ways. The disclosed approach deliberately does not provide a single global ledger or global finality; when an application's core requirement is that all participants agree on one canonical record, agent-scoped consensus is not a substitute for a ledger, and a system like IOTA is the more appropriate tool. Agent-carried trust also shifts responsibility onto policy definition and key management: the guarantees are only as good as the embedded policy references, the signatures, and the trust scoping that the deploying organization configures.

The Memory-Native Protocol is described in a patent application. It sets out an architecture and worked examples rather than a benchmarked, generally available product, and this article makes no performance claims for it beyond what the specification describes as mechanisms. Statements here about IOTA reflect widely known, architecture-level characteristics of the project as generally described by its community; readers evaluating IOTA for a specific use should consult IOTA's own current documentation, since a live project's design continues to evolve.

Disclosure Scope

The invention described on this page is disclosed in United States Patent Application 19/366,760, and every statement about what the invention does, including the agent structure, the dynamic routing protocol, the adaptive consensus protocol, the append-only signed memory field, and operation without shared infrastructure or synchronized ledgers, is drawn from that specification. References to IOTA and the Tangle, and to the broader distributed-ledger market, are provided as external context to locate the invention on a shared-ledger-versus-agent-carried axis; they are not characterizations of the filing and are not claims of the application. Nothing here asserts that IOTA or the Tangle suffers any defect, and no comparison is intended to disparage that project or attribute to it any limitation beyond the ordinary architectural fact that a distributed ledger is organized around a shared, convergent record.

Memory-Native Protocol (/memory-native-protocol) All 40 steps → (/inventive-steps)

Authority intrinsic to the object. Routing by semantic properties.

U.S. 19/366,760 (/patents/19-366760)

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)

- The Agent Is the Wire Format: A Self-Contained Unit on the Network (/articles/memory-native-protocol/governed-mesh-wire-format)
- Hop-History Relay and In-Band Chain of Custody (/articles/memory-native-protocol/hop-history-relay)
- Mobile Store-and-Forward Without Cellular Backhaul (/articles/memory-native-protocol/mobile-store-and-forward)

APPLICATIONS · GENERAL

- A Memory-Native Coordination Fabric for Multi-Agent AI Orchestration (/articles/memory-native-protocol/multi-agent-orchestration-fabric)
- Edge Routing Without a Central Control Plane: Compliance-Grade Routing Authority at the Edge (/articles/memory-native-protocol/edge-routing)
- Broker-Free IoT Device Mesh Governance at Scale (/articles/memory-native-protocol/iot-mesh)
- V2V Communication Without Roadside Infrastructure: Memory-Native Trust for Autonomous Vehicles (/articles/memory-native-protocol/autonomous-vehicle-networking)
- Military Mesh Networks Without Central Routing Authority (/articles/memory-native-protocol/military-mesh-networks)
- Decentralized Smart City Infrastructure Without a Central Control Platform (/articles/memory-native-protocol/smart-city-infrastructure)
- Delay-Tolerant Satellite Routing Governance for LEO Constellations (/articles/memory-native-protocol/satellite-communication)
- Industrial IoT Protocols Without Broker-Centralized Authority: A Memory-Native Substrate for Credentialed OT Telemetry (/articles/memory-native-protocol/industrial-iot-protocols)
- Healthcare Device Mesh Networking for Fault-Tolerant Clinical Data (/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 IoT Mesh Without Cellular Backhaul (/articles/memory-native-protocol/maritime-iot-mesh)
- Why Mesh Networks Stall in Contested, Multi-Vendor Deployments: Node-Resident Governance and the Carried-Authority Fix (/articles/memory-native-protocol/carried-authority-ceiling)
- How to Contain a Compromised Node in a Distributed Network Without Trusting It (/articles/memory-native-protocol/malicious-host-contained)
- Delay-Tolerant and Interplanetary Autonomy: Carrying Authority When There Is No Link Home (/articles/memory-native-protocol/disconnected-and-interplanetary)

APPLICATIONS · SPECIFIC

- Starlink Alternative for Governed Mesh Routing: Why Satellite Handover Authority Stays Terrestrial (/articles/memory-native-protocol/starlink)
- Zigbee vs Governed IoT Messaging: Why the Mesh Routes Frames but Carries No Authority (/articles/memory-native-protocol/zigbee)
- Does Matter Let Governance Travel With the Message? (/articles/memory-native-protocol/matter)
- Helium Alternative for Governed IoT Transport: Decentralized Coverage Plus Message-Borne Governance (/articles/memory-native-protocol/helium)
- LoRaWAN Alternative for Governed IoT: Memory-Native Messages vs Passive Payloads (/articles/memory-native-protocol/lorawan)
- Beyond the Tailscale Coordination Server: Governed Mesh Networking Where Authority Travels With the Packet (/articles/memory-native-protocol/tailscale)
- QUIC vs Content-Scoped Authority: A Memory-Native Protocol Layer Above QUIC (/articles/memory-native-protocol/quic-protocol)
- MQTT vs Memory-Native Protocol: Where IoT Messaging Authority Should Live (/articles/memory-native-protocol/mqtt)
- CoAP Brought REST to Constrained Devices. The Protocol Carries No Governance Semantics. (/articles/memory-native-protocol/coap)
- gRPC Alternative for Governed Agent Execution: Where the Memory-Native Protocol Fits (/articles/memory-native-protocol/grpc)
- ZeroMQ vs Memory-Native Protocol: Brokerless Sockets Without Carried Authority (/articles/memory-native-protocol/zeromq)
- WireGuard vs Memory-Native Protocol: Governed Payloads Above the Tunnel (/articles/memory-native-protocol/wireguard)
- Nebula vs a memory-native protocol: does the mesh still depend on a central certificate authority? (/articles/memory-native-protocol/nebula-mesh)
- Calico Enforces Network Policy at the Kernel. A Governed Alternative Carries Policy in the Packet. (/articles/memory-native-protocol/calico)
- Cilium vs Memory-Native Protocol: Where Governance Lives in the Stack (/articles/memory-native-protocol/cilium)
- Weave Net Alternative for Governed Agent Execution: Where the Memory-Native Protocol Fits (/articles/memory-native-protocol/weave-net)
- Persistent Systems Wave Relay vs Protocol-Native Authority Semantics (/articles/memory-native-protocol/persistent-systems)
- Does Silvus StreamCaster Provide a Payload Governance Layer? (/articles/memory-native-protocol/silvus-streamcaster)

- Rajant Kinetic Mesh and Payload-Level Governance: A Memory-Native Layer Above the Link (/articles/memory-native-protocol/rajant-kinetic-mesh)
- TrellisWare TSM vs Governed Observation Admissibility: Routing Is Not Authority Resolution (/articles/memory-native-protocol/trellisware-tsm)
- Autotalks Craton2 vs Governed V2X: The Authority Layer Above the Chipset (/articles/memory-native-protocol/autotalks-craton2)
- Qualcomm 9150 C-V2X vs Memory-Native Behavioral Authority (/articles/memory-native-protocol/qualcomm-9150)
- Does NXP RoadLink Govern What a V2X Message Is Authorized to Do? (/articles/memory-native-protocol/nxp-roadlink)
- Chroma Vector Database vs a Governed Memory-Native Substrate (/articles/memory-native-protocol/chroma-vector-db)
- Milvus Alternative: Governed Agent Memory Beyond the Vector Database (/articles/memory-native-protocol/milvus-vector-db)
- Pinecone Alternative for Governed Agent Memory (/articles/memory-native-protocol/pinecone-vector-db)
- Qdrant Alternative: Governed, Portable AI Memory Beyond the Vector Database (/articles/memory-native-protocol/qdrant-vector-db)
- Weaviate Alternative for Governed Vector Memory: The Memory-Native Protocol (/articles/memory-native-protocol/weaviate-vector-db)
- Anduril Lattice Mesh vs Carried Governance: A Memory-Native Protocol Comparison (/articles/memory-native-protocol/anduril-lattice-mesh)
- Shield AI Hivemind vs Governed Team Coordination: The Authority Layer Above Onboard Autonomy (/articles/memory-native-protocol/shield-ai-hivemind)
- Bundle Protocol v7 / DTN (NASA ION) vs a memory-native protocol: where do trust, policy, and consensus live? (/articles/memory-native-protocol/bundle-protocol-dtn)
- **IOTA (Tangle) alternative: agent-carried trust without a shared ledger (/articles/memory-native-protocol/iota-tangle)**
- Model Context Protocol (MCP) vs a memory-native protocol: where trust, lineage, and policy live (/articles/memory-native-protocol/model-context-protocol)

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