What is claimed is:

1. A computer-implemented system for memory-native protocol execution, comprising:

a plurality of agents, wherein each of the plurality of agents includes a unique identifier, a payload, a memory field, a transport header, and a cryptographic signature;

a plurality of distributed nodes, wherein each of the plurality of distributed nodes is configured to transmit and receive any of the plurality of agents; and

a modular protocol stack, wherein the modular protocol stack is configured to be executed at each of the plurality of distributed nodes, and wherein the modular protocol stack includes a routing layer, an indexing layer, and a consensus layer,

wherein behavior within the system of the routing layer, the indexing layer, and the consensus layer is determined by metadata embedded within a received respective one of the plurality of agents,

wherein the memory field of each of the plurality of agents includes verifiable lineage, access logs, and policy references, and wherein the verifiable lineage, the access logs, and the policy references include sets of instructions configured to govern routing, mutation, and consensus behavior for the corresponding one of the plurality of agents.

2. The system of claim 1, wherein each of the plurality of agents is configured to operate as a self-governing protocol operand, and wherein the transport header specifies constraints selected from the group consisting of: trust scope, time-to-live, semantic class, latency sensitivity, and quorum priority.

3. The system of claim 1, wherein each of the plurality of distributed nodes includes a local trust graph derived from prior memory field evaluations and is configured to dynamically score routing candidates during transmission based on the local trust graph.

4. The system of claim 1, wherein the protocol stack includes a network health monitoring system configured to emit health agents comprising congestion metrics, trust volatility, semantic entropy, and cache degradation data, and wherein each node is configured to modify routing or mutation behavior in response to received one or more health agents.

5. The system of claim 1, wherein the protocol stack is configured to be executed over a stateless transport layer selected from the group consisting of: TCP/IP, HTTP, mesh relay, delay-tolerant networking, and WebRTC.

6. The system of claim 4, wherein the one or more health agents include entropy thresholds configured to trigger index splitting or semantic reclassification by the indexing layer.

7. The system of claim 1, wherein the each of the plurality of agents comprises a cognition-compatible payload encoded as a data object, and wherein the protocol stack is configured to execute cognition-layer mutation behavior using memory field constraints and embedded policy.

8. The system of claim 3, wherein each of the plurality of distributed nodes is configured to adjust the local trust graph in response to trace outcomes embedded in received agents.

9. The system of claim 8, wherein each of the plurality of distributed nodes is further configured to update entries in the local trust graph based on data received from health agents emitted by a network health monitoring system and adjust node trust scores based on one or more observed metrics selected from a group consisting of congestion, latency variance, policy violation frequency, and propagation entropy, thereby allowing a dynamic routing protocol (DRP) to re-score candidate transmission paths in -real-time.

10. The system of claim 1, further including a dynamic indexing protocol (DIP) configured to form soft-index containers based solely on entropy anchors computed from agent-resident data, wherein the entropy anchors are statistical functions of mutation divergence trajectory, lineage density, and access-distribution patterns recorded in the memory field of the agent, and to create, split, merge, or promote local index anchors without involving or depending on a dynamic alias system or human-readable alias resolution.

11. The system of claim 1, further including a network health monitoring system is configured to emit health agents that, when received by one of the plurality of nodes, cause such node to execute one or more adjustments to parameters of an adaptive consensus protocol for one or more semantic classes, the adjustments including raising or lowering quorum thresholds, excusing or reinstating specific participations from quorum eligibility, and re-weighting participant votes.

12. The system of claim 1, wherein each of the plurality of agents is a semantic agent having a structure with an intent field and a cognition-compatible payload, and wherein the structure is configured to be modified in response to policy references or execution context stored in the memory field.

13. The system of claim 1, wherein each of the plurality of agents includes a reference to a policy agent, the policy agent comprising quorum rules, mutation eligibility criteria, and role definitions referred to when governing execution behavior.

14. A computer-implemented method for distributed memory-native communication, comprising:

receiving an agent at a node, the agent comprising a unique identifier, an access log, a payload, a memory field, a transport header, and a signature;

verifying the signature of the agent and parsing the transport header and the memory field;

determining routing eligibility and mutation scope of the agent by evaluating the access log and policy references of the agent;

executing one or more protocol stack layers based on content contained in the memory field;

appending a trace log to the memory field; and

forwarding, after appending the trace log, the agent to one or more eligible nodes, wherein the one or more eligible nodes is determined by assessing dynamic routing protocol and one or more memory field constraints, for mutation execution or resolution.

15. The method of claim 14, wherein determining routing eligibility includes scoring candidate paths based on trust scores derived from access log outcomes recorded in prior agents.

16. The method of claim 14, further including triggering a consensus operation when the memory field indicates a proposed mutation, and evaluating trust-weighted votes cast by participating nodes cast according to a policy agent referenced in the memory field.

17. The method of claim 14, further including restricting and authorizing read, write, or mutation behavior based on policy references contained in the memory field without reliance on external session state.

18. The method of claim 14, wherein the agent is a semantic agent having a structure with an intent field and a cognition-compatible payload, further including modifying the structure in response to policy references or execution context stored in the memory field.

19. The method of claim 14, wherein the agent includes a reference to a policy agent, the policy agent including quorum rules, mutation eligibility criteria, and role definitions, further including governing execution behavior of the agent based on the quorum rules, mutation eligibility criteria, and role definitions.

20. The method of claim 14, wherein evaluating the access log includes identifying the most recent execution history associated with neighboring nodes, including success rates, policy violation frequency, and node responsiveness.