What is claimed is:

1. A computer-implemented method for executing cognition-native semantic agets across distributed and heterogeneous computational environments having a plurality of semantic agents, devices, anchors, and trust zones, the method comprising:
   instantiating a semantic agent having a plurality of fields including an intent field, a context block, a memory field, a policy reference field, a mutation descriptor field, and a lineage field;
   evaluating the policy reference field at runtime prior to any mutation, delegation, or propagation of the agent, wherein agent mutation, delegation, or propagation is deterministically permitted or denied based on validation of policy provided in the policy reference field;
   resolving human-readable aliases to unique identifiers using adaptive indexes governed by anchor-based consensus, wherein semantic agents, devices, anchors, and trust zones are resolved through scoped path-based aliasing and through entropy-derived unique identifier registration and slope-indexed retrieval, wherein resolving human-readable aliases includes slope-indexed pathfinding across anchor nodes, registration of identifiers derived from semantic entropy, and enforcement of propagation constraints based on mutation lineage and policy inheritance;
   routing the agent across a memory-native substrate based on semantic trust scope, contextual relevance, and mutation eligibility;
   resolving agent execution failure or constraint violation by triggering agent mutation events in accordance with mutation descriptors and scoped policy overrides embedded in the agent;
   validating semantic lineage of the agent and agent authenticity through entropy-resolved trust slope verification; and
   recording execution events, mutation histories, and semantic propagation for the agent in the memory field.
2. The method of claim 1, wherein resolution occurs prior to agent or content propagation or execution, and is validatable across decentralized substrates.
3. The method of claim 1, wherein agent mutation, delegation, or propagation is deterministically permitted or denied without reliance on centralized authorization or post-execution filtering.

4. The method of claim 1, further comprising deploying fallback partial agent structures in environments lacking native memory-aware substrates and deferring memory field synchronization until reconnection of the agent to memory-native zones.

5. The method of claim 1, further comprising evaluating policy references prior to intent resolution or mutation execution, with automatic quarantine or rollback on violation to enforce ethical policy constraints at runtime.

6. The method of claim 1, further comprising resolving scoped trust zone aliases and validating zone-specific governance policies prior to agent execution or propagation for semantic zone migration.

7. The method of claim 1, further including gating agent execution decisions by quorum-based consensus validation in scoped semantic zones for mutation-sensitive or ethics-governed behaviors.

8. The method of claim 1, further comprising compiling semantic execution lineage graphs through accumulation of memory-trace records, mutation justification metadata, and signed policy audit trails.

9. A cognition-native semantic execution platform comprising:

   a plurality of memory-bearing semantic agents, each of the plurality of memory-bearing semantic agents including a plurality of fields including an intent field, a context block, a memory field, a policy reference field, a mutation descriptor field, and a lineage field;

   a memory-native substrate configured to route and store the plurality of memory-bearing semantic agents across a plurality of distributed trust zones based on a semantic context policy, a mutation eligibility policy, and a trust-scoped propagation policy;

   a governance layer including one or more cryptographically signed policy objects that define mutation permissions, semantic constraints, and override conditions for behavior of the plurality of memory-bearing semantic agents within scoped trust zones based on content of the plurality of fields of a respective agent;

   a distributed indexing layer comprising a plurality of adaptive indexes configured to map semantic aliases to unique identifiers for one or more of the plurality of agents, content artifacts, devices, and semantic assets of the platform, each adaptive index governed by a plurality of entropy-sensitive anchors configured to validate alias mutations, resolve identifier collisions, register identifiers derived from semantic entropy, enforce mutation

lineage policies, and deterministically resolve routing queries based on semantic scope and substrate locality; and

an entropy-resolved identity layer configured to authenticate lineage of the plurality of memory-bearing semantic agents and validate behavioral trust slopes across execution cycles without persistent static credentials.

10. The platform of claim 9, wherein the memory-native substrate includes a set of instructions that when executed maintains dynamic semantic memory fields that track mutation outcomes, lineage paths, and policy compliance for each of the plurality of memory-bearing semantic agents .

11. The platform of claim 10, wherein the set of instructions that when executed maintains dynamic semantic memory fields that track mutation outcomes, lineage paths, and policy compliance for each of the plurality of memory-bearing semantic agents without reliance on centralized storage architectures.

12. The platform of claim 9, wherein the scoped trust zones and the distributed trust zones include sets of instructions that when executed enforce scoped mutation governance through quorum-based override protocols and zone-specific policy validation.

13. The platform of claim 9, wherein each semantic agent object is configured to persist execution memory across substrate transitions such that semantic continuity is maintained through serialization, fallback scaffolding, or partial agent emulation.

14. The platform of claim 9, wherein mutation descriptors embedded in each of the plurality of memory-bearing semantic agents and cryptographic validation of associated policy references are configured to govern mutation events.

15. The platform of claim 9, wherein the platform includes instructions to authenticate agent identities of the plurality of memory-bearing semantic agents by validating dynamic agent hash (DAH) slopes derived from memory-local entropy and semantic context, and to evaluate device dynamic hash (DDH) slopes for substrate trust validation during agent execution.