SAIHM Competitive Analysis — AI Horizontal Memory Solutions

SAIHM

April 2026

Legal Notice

All comparisons are fact-grounded based on publicly available documentation, published specifications, and verifiable technical claims as of April 2026.

---

1. Market Landscape

1.1 The AI Memory Problem

AI agents lack persistent, cross-session memory infrastructure. Current solutions fall into three categories:

1. **Provider-Managed Memory** — Centralized, vendor-locked memory by AI platform operators (OpenAI Memory, Google Gemini Context)
2. **Vector Database Layer** — General-purpose vector stores repurposed for AI memory (Pinecone, Weaviate, Qdrant, Chroma)
3. **Decentralized AI Memory Protocols** — Purpose-built decentralized memory infrastructure (SAIHM, Recall, MemoryOS)

1.2 Evaluation Criteria

Criterion	Weight	Rationale
Data Sovereignty	High	Agent/user controls data, not platform
Privacy & Encryption	High	End-to-end encryption, zero-knowledge computation
Regulatory Compliance	High	GDPR, EU AI Act, MiCA built-in
Post-Quantum Security	High	Long-term data protection
		Censorship

Decentralization	Medium	resistance, no single point of failure
Cross-Platform	Medium	Works across AI providers and blockchains
Semantic Capabilities	Medium	Encrypted search, knowledge graphs
Economics	Medium	Transparent, predictable pricing
Maturity	Medium	Production readiness, documentation quality

2. Detailed Comparison

2.1 SAIHM vs. Provider-Managed Memory

OpenAI Memory (ChatGPT Memory)

Feature	OpenAI Memory	SAIHM
Storage Location	OpenAI servers (centralized)	Filecoin, Storj, Arweave, IPFS (decentralized)
Encryption	Server-side (provider holds keys)	End-to-end (agent holds keys via sealed GC)
Data Sovereignty	Provider-controlled	Agent-sovereign
GDPR Erasure	Manual request to OpenAI	Cryptographic DEK destruction, Arweave-anchored proof
Cross-Platform	ChatGPT only	Any AI agent on any chain
Post-Quantum	Not documented	NIST FIPS 203/204/205
Audit Trail	Not available externally	Hash-chained audit ledger (Filecoin + Arweave)
Pricing	Bundled with subscription	Pay-per-operation (transparent nCOTI)
Vendor Lock-in	Complete	None

Assessment: OpenAI Memory is convenient for ChatGPT-only workflows but provides no data sovereignty, no cross-platform portability, and no verifiable privacy guarantees. Users trust OpenAI with plaintext memory.

Google Gemini Memory / Context Caching

Feature	Gemini	SAIHM
Architecture	Google Cloud infrastructure	Decentralized GC + multi-tier storage
Privacy Model	Google data policies apply	Zero-knowledge sealed computation
Portability	Google ecosystem only	Universal cross-chain
Regulatory Compliance	Google's compliance posture	Protocol-level GDPR/EU AI Act/MiCA
Cryptographic Erasure	Not specified	DEK destruction with Arweave anchor

Assessment: Similar centralization concerns as OpenAI. Memory is an extension of Google's ecosystem, not an independent infrastructure.

2.2 SAIHM vs. Vector Database Solutions

Pinecone

Feature	Pinecone	SAIHM
Type	Managed vector database (SaaS)	Decentralized memory protocol
Encryption at Rest	AES-256 (provider-managed keys)	AES-256-GCM (agent-managed keys via sealed GC)
Encryption in Compute	No (plaintext during query)	Yes (sealed Garbled Circuit computation)
Data Sovereignty	Pinecone Inc. manages data	Agent-sovereign
GDPR Erasure	Delete API (no cryptographic proof)	DEK destruction + Arweave anchor
Decentralization	None (single vendor)	4 storage providers, on-chain governance
Post-Quantum	No	NIST FIPS 203/204/205
Semantic Operations	Vector similarity search	Encrypted semantic search, GKG, LSA, FHE-PCA
Access Pattern Privacy	No (provider sees queries)	ORAM (oblivious RAM) hides access patterns

Assessment: Pinecone excels at high-throughput vector search but operates as a centralized SaaS with no compute-time encryption, no data sovereignty, and no regulatory compliance infrastructure. Suitable as a complementary cache, not as sovereign memory.

Weaviate / Qdrant / Chroma

Similar limitations to Pinecone: centralized or self-hosted, no encrypted computation, no protocol-level compliance, no post-quantum crypto, no decentralized storage. These are general-purpose vector databases, not AI memory protocols.

2.3 SAIHM vs. Decentralized AI Memory Protocols

Recall (Recall.ai / 3Box Labs)

Feature	Recall	SAIHM
Blockchain	Custom / Ceramic network	COTI V2 Garbled Circuits
Storage	Ceramic + IPFS	Filecoin + Storj + Arweave + IPFS (4-tier)
Encryption Model	Client-side encryption	Sealed GC computation (zero plaintext)
Computation Privacy	No encrypted computation	Full GC-sealed computation
Post-Quantum	Not documented	NIST FIPS 203/204/205
GDPR Erasure	Stream deletion (IPFS immutability challenges)	Cryptographic DEK destruction (data irrecoverable)
Audit Trail	Ceramic stream anchors	Hash-chained ML-DSA signed ledger
Governance	Token-weighted (public votes)	Private garbled-circuit voting
Economics	Token-based	nCOTI with BFSI discount, PDI congestion pricing
Semantic Layer	Basic retrieval	GC-17/18: encrypted LSA, GKG, FHE-PCA, LSH
Cross-Chain	Limited	GC-19: Axelar Amplifier, MPC blind swaps
Reputation System	Not documented	PRS [0-10,000] with 9 sealed decrement types
Conservation Mode	Not documented	Full degraded-operation specification

Assessment: Recall pioneered decentralized AI memory but lacks encrypted computation, post-quantum security, formal regulatory compliance, and the economic sophistication of SAIHM. SAIHM's sealed Garbled Circuit architecture provides a fundamentally stronger privacy guarantee — no component in the system ever accesses plaintext.

MemoryOS

Feature	MemoryOS	SAIHM
Focus	Agent memory management layer	Full-stack decentralized memory infrastructure
Decentralization	Partial (centralized coordinator)	Full (on-chain governance, decentralized storage)
Encryption	Application-level	Protocol-level sealed GC
Regulatory Compliance	Application responsibility	Protocol-embedded (GDPR, EU AI Act, MiCA)
Post-Quantum	No	Yes (NIST FIPS 203/204/205)

Assessment: MemoryOS provides useful memory management abstractions but is not a decentralized protocol. Compliance and security are application-layer concerns rather than protocol invariants.

---

3. Summary Matrix

Capability	OpenAI	Gemini	Pinecone	Recall	MemoryOS
Data Sovereignty	No	No	No	Partial	Partial
E2E Encryption	No	No	At-rest	Client-side	App-level
Encrypted Compute	No	No	No	No	No
Post-Quantum	No	No	No	No	No
GDPR Erasure (Provable)	No	No	No	Partial	No
EU AI Act Compliance	Partial	Partial	No	No	No
Decentralized Storage	No	No	No	Partial	No
Cross-Chain	No	No	No	Limited	No
Semantic (Encrypted)	No	No	No	No	No
Governance	No	No	No	Token	No
Access Pattern Privacy	No	No	No	No	No

Audit Trail	No	No	No	Partial	No

---

4. SAIHM Unique Differentiators

1. **Only protocol with encrypted computation** — Sealed Garbled Circuits ensure zero plaintext exposure at any point in the data lifecycle.
2. **Only protocol with post-quantum cryptography** — NIST FIPS 203/204/205 provides long-term security against quantum computing threats.
3. **Only protocol with provable GDPR erasure** — Cryptographic DEK destruction with Arweave-anchored immutable proof of compliance.
4. **Only protocol with ORAM access pattern privacy** — Tree-ORAM, Path-ORAM, and Fractal-ORAM variants hide which memory shards an agent accesses.
5. **Only protocol with encrypted semantic operations** — FHE-PCA, Garbled Knowledge Graphs, and Latent Space Transcoders operate entirely under encryption.
6. **Only protocol with formal conservation mode** — Structured degraded-operation specification ensures critical functions (reads, erasure, governance) continue during protocol stress.
7. **Most comprehensive regulatory framework** — GDPR, EU AI Act, MiCA, NIST PQC, ISO 27001/27701, ETSI EN 319 401, NIST SP 800-207 all addressed at protocol level.
8. **Only protocol with scope-controlled memory sharing** — Temporary, permanent, and syndicate sharing contracts enable cross-agent collaboration (swarms, enterprise teams, DAOs) while maintaining full encryption and audit trails.
9. **Only protocol with decentralized governance open to all token holders** — On mainnet, any gCOTI holder can propose and vote on protocol parameters via private garbled-circuit voting.
