ANALYTICAL REVIEW

Intellectual Property & Technology Licensing Review

U.S. Patent No. 12,147,562 B1

Artificial Intelligence-Enhanced Ledger Computing Environment

AIRIL: AI-Assisted Runtime Integrity Layer

A structured review of the inventive concept, system architecture, cryptographic design, claim analysis, and licensing considerations.

Romella Janene

Inventor | Romella Janene (El Kharzazi)

EXECUTIVE SUMMARY

This Analytical Review evaluates U.S. Patent No. 12,147,562 B1 and explains why the claimed architecture establishes a new category of enterprise integrity infrastructure. The invention, referred to here as AIRIL — the AI-Assisted Runtime Integrity Layer — yields a practical model we call the Capsule Ledger: a sealed, VM-bound ledger instance that combines dual encryption, AI-assisted hashing, and recursive validation. The patent protects a specific orchestration of components and a 15-step method that together deliver enterprise-grade auditability, known user accountability, cryptographic agility for post-quantum readiness, and ledger portability as a transferable asset.

For a technology organization evaluating strategic adoption or licensing, the essential conclusions are these. First, the inventive value is architectural and procedural; the claims protect a reproducible orchestration rather than a single cryptographic primitive. Second, the Capsule Ledger model maps directly to enterprise needs: regulated audit trails, controlled provenance, and secure handoffs. Third, the architecture is crypto-agnostic and supports migration paths to post-quantum cryptography without changing the Capsule Ledger boundary. Fourth, the patent claims are precise and defensible, providing a strong basis for licensing to cloud providers, device ecosystems, financial institutions, healthcare organizations, and defense contractors. This document is intended to support commercial diligence and internal decision making. A confidential technical appendix is available under NDA and an Implementation Flight Pack is available to licensees under negotiated terms. See the Supporting Materials section near the end of this review.

INTRO

AIRIL is an architectural class: a runtime integrity layer that is sovereign, VM-bound, and AI-assisted. The Capsule Ledger is the user-friendly abstraction: a sealed capsule that contains ledger data, metadata, audit logs, AI hashing logic, and ephemeral key material. The Capsule Ledger enforces integrity inside the runtime boundary rather than relying on distributed consensus.

The following sections examine the inventive concept, system architecture, business abstraction, technical protections, quantum readiness, comparative positioning, legal claims, and recommended next steps for a prospective licensee.

1. THE INVENTIVE CONCEPT

AIRIL is an architectural class: a runtime integrity layer that is sovereign, VM-bound, and AI-assisted. The Capsule Ledger is the user-friendly abstraction: a sealed capsule that contains ledger data, metadata, audit logs, AI hashing logic, and ephemeral key material. The Capsule Ledger enforces integrity inside the runtime boundary rather than relying on distributed consensus.

The patent claims a specific combination of components and interactions. The architecture ties together a Virtual Machine Environment, a Key Management Server that creates a Primary Encryption Key with algorithmic assistance, a Host that creates Data Encryption Keys and performs envelope encryption, an Artificial Intelligence Server that generates partial hashes and assists key creation, an in-VM Artificial Intelligence Engine that completes final hashes and orchestrates analytics, and a Stable Ledger Server that stores the canonical master copy. The novelty is the orchestration: the sequence of interactions that produces a sealed, self-validating ledger instance. This orchestration departs from prior art that relies on network consensus and external validators.

The practical consequence is a ledger that is simultaneously sealed, auditable, and portable. Unlike distributed ledgers that represent shared state across many nodes, a Capsule Ledger is a discrete asset that can be exported, transferred, or archived with a signed manifest and a verification routine. That capability is commercially significant for regulated handoffs such as loan portfolio transfers, clinical trial dataset sales, and contractor transitions for mission-critical systems.

2. SYSTEM ARCHITECTURE HIGH LEVEL

The architecture is intentionally modular and designed for enterprise deployment. Each component has a clear role and a constrained trust boundary.

The User Client initiates sessions and submits transactions. The Host hypervisor acts as a gateway and creates Data Encryption Keys, holding the Primary Encryption Key in memory only for the session duration. The Central Server brokers Key IDs and coordinates session setup. The Key Management Server is the root of trust and creates the Primary Encryption Key with algorithmic assistance. The Artificial Intelligence Server provides heavy compute for partial hashes and analytics. The Virtual Machine Environment is the encrypted runtime container that houses the Capsule Ledger. The Artificial Intelligence Engine is a lightweight in-VM agent that completes final hashes and formats analytics. The Stable Ledger Server is the permanent repository for the canonical master copy and metadata.

Two workflows are central to the invention. The first is session initiation, a 15-step handshake that establishes ephemeral key custody and encrypts the VME. The second is transaction posting, in which the AIE requests a partial hash from the AIS, combines the returned partial hash with transaction content to produce the final hash, and posts the transaction to the VME and the SLS. These workflows enforce separation of duties and minimize persistent exposure of sensitive keys.

The security posture is defense in depth. Runtime encryption of the VME protects active data. Entropic floating hashing provides transaction-level tamper evidence. Separation of duties prevents any single component from holding both persistent PEK and Key ID. Operationally critical components such as the Central Server and the AIS require enterprise-grade availability, clustering, and monitoring.

3. THE CAPSULE LEDGER ABSTRACTION BUSINESS VIEW

A Capsule Ledger is a sealed, self-contained ledger instance that is sovereign, self-validating, AI-native, and portable. It is sovereign because it lives inside an encrypted VM boundary. It is self-validating because recursive revalidation provides tamper evidence whenever the ledger is accessed. It is AI-native because AI participates in key creation, hashing, and analytics. It is portable because the ledger can be exported and transferred as a discrete asset with a signed manifest and a verification routine.

For enterprise buyers the Capsule Ledger model is immediately actionable. It supports scenarios such as the transfer of a loan portfolio with an auditable ledger attached, clinical trial data

handoffs that preserve regulatory audit trails, and satellite command logs that remain verifiable across contractor transitions. These are not hypothetical advantages; they are concrete commercial differentiators relative to distributed ledgers that represent shared state rather than a single transferable asset.

From an integration perspective, the Capsule Ledger maps to existing enterprise patterns. The VME can be instantiated on cloud infrastructure or on premises. The AIS can be co-located with existing analytics clusters or provided as a managed service. The SLS can be implemented as a hardened object store with signed manifests. For a device and services ecosystem such as Apple, the Capsule Ledger can be scoped to device provenance, secure telemetry, and cross-service audit trails while preserving user privacy through known user credentials and selective disclosure.

4. DUAL-LAYER ENCRYPTION AND AI ASSISTED HASHING TECHNICAL SUMMARY

The architecture uses two complementary protection layers. The first layer secures the runtime environment. The Host creates Data Encryption Keys that are envelope encrypted with the Primary Encryption Key. The PEK is created by the KMS with AIS assistance and is present in Host memory only for the session duration. This design minimizes persistent exposure of the PEK and confines active data to the VME.

The second layer secures transactions through entropic floating hashing. The AIS generates a partial hash that the AIE combines with transaction content to produce the final hash. The AI-generated entropy is content-dependent and ephemeral. This approach increases unpredictability and tamper evidence at the transaction level while enabling analytics to be integrated into the integrity process.

Determinism and auditability are essential. For reproducible validation the system must record AI model versions, seeds, and any non-deterministic parameters. Implementations must include model provenance and versioning so that a final hash can be recomputed for verification. These governance artifacts are part of the technical appendix and are required for regulatory acceptance in clinical, financial, and defense contexts.

5. QUANTUM READINESS AND CRYPTOGRAPHIC AGILITY

A material advantage of the architecture is cryptographic agility. The PEK and DEK lifecycle and the transaction hashing process are designed to be algorithm-agnostic. Implementations can use classical symmetric encryption for bulk data while adopting hybrid key encapsulation mechanisms for key exchange. During a migration period hybrid signatures that combine

classical and PQC primitives can be used to preserve continuity. The AIS is a natural orchestrator for hybrid key generation and migration because it can coordinate key material and algorithm selection without changing the Capsule Ledger boundary.

For enterprise buyers this reduces migration risk. Data that must remain verifiable for decades benefits from a ledger architecture that can transition to PQC primitives without rearchitecting the runtime boundary. The AIS role in orchestrating cryptographic transitions is a practical advantage for organizations that must meet long-term integrity requirements.

6. COMPARATIVE ANALYSIS

The following analysis summarizes the high-level differences between AIRIL Capsule Ledger and representative ledger families across six key attributes. Each attribute is examined as a subsection with the position of each ledger family noted.

GOVERNANCE

Governance refers to the control model that determines who can participate and how decisions are made.

- AIRIL Capsule Ledger: Centralized and permissioned
- Public Blockchain: Decentralized
- Hashgraph: Permissioned
- DAGs: Distributed
- Corda: Permissioned

VALIDATION

Validation describes the mechanism by which transactions or state changes are confirmed as legitimate.

- AIRIL Capsule Ledger: Internal and recursive
- Public Blockchain: Network consensus
- Hashgraph: Virtual voting
- DAGs: Parallel validation
- Corda: Notary services

IDENTITY

Identity indicates how participants are represented and authenticated within the system.

- AIRIL Capsule Ledger: Known user credentials

- Public Blockchain: Pseudonymous
- Hashgraph: Node identities
- DAGs: Node identities
- Corda: Legal identities

ENCRYPTION MODEL

Encryption model covers the layers of cryptographic protection applied to data at rest and in transit.

- AIRIL Capsule Ledger: Dual layer and AI assisted hashing
- Public Blockchain: Single layer hashing
- Hashgraph: Single layer hashing
- DAGs: Single layer hashing
- Corda: Transaction privacy controls

ENERGY PROFILE

Energy profile reflects the computational and power cost of operating the network or runtime.

- AIRIL Capsule Ledger: Low
- Public Blockchain: High for PoW
- Hashgraph: Low
- DAGs: Low
- Corda: Low

LEDGER TRANSFERABILITY

Ledger transferability describes whether the ledger can be exported and transferred as a discrete, self-contained asset.

- AIRIL Capsule Ledger: Portable sealed asset
- Public Blockchain: Shared distributed state
- Hashgraph: Shared state
- DAGs: Shared state
- Corda: Shared state

This comparison highlights three practical contrasts. First, AIRIL enforces integrity inside a sovereign runtime rather than by network consensus. Second, AIRIL supports ledger portability as a discrete asset, enabling M&A-style transfers and regulated handoffs. Third, AIRIL integrates AI into cryptographic orchestration and analytics, enabling content-aware hashing and continuous integrity monitoring.

7. LEGAL CLAIM ANALYSIS

Claim 1 recites a 15-step method that covers session initiation, KMS-AIS interaction, PEK creation, DEK generation, AIE-AIS partial hashing, final hash creation, posting, and presentation. The claim is specific and sequential. This specificity is a strength for enforcement because the all-elements rule simplifies infringement analysis. A competitor must implement substantially the same sequence to infringe.

Claim 2 enumerates the component constellation and their interactions. It protects the inventive combination rather than a single element. Enforcement will focus on systems that replicate the same functional roles. Evidence of functional equivalence will be central in any dispute. For licensing and enforcement readiness maintain implementation artifacts, architecture diagrams, and logs that demonstrate the claimed orchestration.

The patent distinguishes itself from blockchain and other DLT prior art by rejecting external validators and by integrating AI into key creation and hashing. The prosecution record should be preserved to support novelty and non-obviousness arguments.

8. STRENGTHS AND LIMITATIONS

The architecture aligns with enterprise requirements for governance, auditability, and long-term integrity. The Capsule Ledger model is a clear commercial narrative that resonates with regulated buyers. The patent's method and system claims create a defensible intellectual property position that supports licensing.

Limitations and risks are operational and implementation related. The architecture centralizes trust in operator components and requires enterprise-grade availability and monitoring. AI-assisted hashing introduces latency that implementers must benchmark. Ledger transfers may trigger data privacy and export control obligations that licensees must manage. These considerations are material but addressable through standard enterprise controls and contractual protections.

9. GAPS AND RECOMMENDED NEXT STEPS

The patent and the materials provided establish the architectural novelty and legal basis for licensing. The following gaps should be addressed during diligence or under a license.

- Performance metrics such as latency, throughput, and concurrency benchmarks are not provided.
- High availability and failover design for critical servers is not specified.
- Deterministic AI governance details such as model versioning and seed management are not documented.
- A PQC mapping to specific candidate algorithms is not included.

The next recommended steps for a prospective licensee are concise. Request the confidential technical appendix under NDA for detailed sequence diagrams, and PQC mapping. If the organization proceeds toward licensing, negotiate access to the Implementation Flight Pack as part of the license. Engage technical teams to map Capsule Ledger integration to existing systems and to define performance targets for any commercial deployment.

10. SUPPORTING MATERIALS AND ACCESS

A technical appendix containing detailed sequence diagrams and PQC mapping is available to qualified reviewers under a standard non-disclosure agreement. An Implementation Flight Pack containing pilot templates, a ledger-as-asset playbook, a threat model checklist, and operational templates is available to parties that enter into a licensing agreement or a negotiated pilot license. Contact the licensor for access and distribution terms.

CONCLUSION

U.S. Patent No. 12,147,562 B1 defines a defensible, enterprise-oriented architecture that creates a new category: AIRIL, the AI-Assisted Runtime Integrity Layer. The Capsule Ledger abstraction makes the invention intuitive for business stakeholders while the patent claims protect the specific orchestration that produces a sealed, self-validating ledger. For organizations evaluating adoption, the architecture offers a practical path to regulated integrity, cryptographic agility, and ledger portability. The recommended next step is to review the confidential technical appendix under NDA and to discuss licensing terms that include access to the Implementation Flight Pack.

TERMINOLOGY AND INTERPRETIVE FIGURE AND TABLE EXPLANATIONS

The terms **AIRIL** (AI-Assisted Runtime Integrity Layer) and **Capsule Ledger** are **interpretive, explanatory names** selected solely to help prospective licensees understand the architecture described in U.S. Patent No. 12,147,562 B1. These names do **not** appear in the patent and are **not** intended to modify, expand, or replace any terminology

used in the issued claims. They serve only as conceptual aids to make the patented orchestration easier to communicate in commercial and technical discussions.

The figures and comparison table included in this Analytical Review are likewise **interpretive illustrations**. They incorporate Capsule Ledger terminology and explanatory labels to make the system architecture, workflows, and integrity model more accessible to evaluators. These illustrations are **not** verbatim reproductions of the patent figures and are **not** substitutes for the figures contained in the issued patent.

The **verbatim patent figures** remain the authoritative reference for the invention. If any perceived incongruence arises between these interpretive illustrations and the patent's published figures, the **patent governs**, and the interpretive materials should be understood as explanatory only. Nothing in these illustrations alters, limits, or expands the scope of the claims granted under U.S. Patent No. 12,147,562 B1.

Figure 1. Capsule Ledger architecture. Components, the two encryption layers, the AIE to AIS partial hash flow, and the Capsule Ledger boundary. This figure orients technical reviewers and business decision makers to the architecture at a glance.

Figure 2. Session initiation sequence. The 15-step handshake annotated with ephemeral key custody notes. This sequence diagram is included in the technical appendix.

Figure 3. Transaction lifecycle. AIE request to AIS, partial hash return, final hash creation, posting, and SLS storage. This lifecycle diagram is included in the technical appendix.

Table 1. AIRIL compared to major ledger families. High level attributes for quick evaluation.