PROVISIONAL PATENT APPLICATION

Filed under 35 U.S.C. § 111(b)

System and Method for a Recursive Agent-Only Settlement Token Backed by an Eight-Primitive Cryptographic Verification Lattice, Including a Native Agent-Class Marketplace for Verified Computational Artifacts

Inventor: Steven Rotzin · Assignee: The Hivery IQ · Walnut Creek, California · Filed: May 23, 2026

FIELD OF THE INVENTION

The invention relates to systems and methods for cryptographically-verified autonomous agent commerce, comprising (1) a composable verification lattice of eight independent primitives, (2) a fungible utility settlement token whose minting, transfer, and trading events are themselves verified by the primitives that define it, (3) a marketplace for trading cryptographically-attested computational artifacts including verified compute credits and verified data bundles, (4) a fleet of native agent classes operating within said marketplace under the same verification lattice, and (5) industry-specific embodiments applying the lattice to regulated domains including legal, healthcare, financial, governmental, construction, and commercial real-estate verticals.

BACKGROUND OF THE INVENTION

Existing autonomous agent systems suffer from four interrelated deficiencies: lack of provenance on inference outputs; lack of transfer authorization gating; lack of cryptographic compliance integration with sub-second proof generation; and lack of native settlement infrastructure carrying verification provenance. Prior tokens provide settlement without attestation. Prior attestation frameworks provide attestation without settlement. Prior compliance tooling provides documentation without cryptographic proof. No prior system composes inference verification, spend-control authorization, identity attestation, compliance proof, schema anchoring, data transformation provenance, witness notarization, and non-custodial settlement as an atomic single-event unit. The present invention provides such a composition.

SUMMARY OF THE INVENTION

The invention comprises five claim families:

Family A — The Verification Lattice (Claims 1–14)

An atomic composition of eight primitives: (1) multi-model inference engine, (2) SMSH inference-stamping module, (3) SHOD spend-control disclosure module, (4) HiveTrust identity-signing envelope, (5) HiveChroma compliance verification with SpectralZK zero-knowledge proofs and ViewKey selective disclosure, (6) HAHS schema-anchoring module, (7) HiveMorph

transformation-provenance module, and (8) non-custodial settlement bridge, composed as a single indivisible verified-event unit.

Family B — Tre'gent Witness Notarization (Claims 15–18)

A three-witness universal-transaction-receipt notarization primitive providing T+1 audit, zero-knowledge witness consensus, and SHOD-signed cryptographic finality, claimed independently of Family A and combinable therewith.

Family C — The Recursive Settlement Token (Claims 19–24)

A fungible utility token whose minting, transfer, staking, and trading events are themselves verified by the eight-primitive lattice that defines the token, producing a self-referential verification architecture wherein the protocol's own economic activity is the test case for its verification claims.

Family D — Native Exchange Agent Classes (Claims 25–34)

A marketplace populated by ten classes of protocol-native agents — market-maker, broker, custodian, settlement, compliance, audit, oracle, liquidation, arbitrage, and index agents — each implementing the eight-primitive lattice on their respective market-microstructure functions.

Family E — Vertical Industry Embodiments (Claims 35–42)

Industry-specific applications of the lattice to legal services, healthcare, financial services, government, construction, commercial real estate, customer-relationship-management ecosystems, and horizontal verified-inference application-programming interfaces.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Section 1 — The Eight Primitives

1.1 Multi-Model Inference Engine

A routing layer accepting agent prompts and routing each prompt to one or more language models selected from at least Anthropic Claude, OpenAI GPT, xAI Grok, Moonshot Kimi, Google Gemini, Deepseek, and Perplexity Sonar. Output may be a single-model response, an ensemble of multiple models with weighted aggregation, or a comparative analysis.

1.2 SMSH (Inference Stamping Module)

Emits a compressed credentialed benchmarked receipt for each inference event. Each SMSH receipt comprises five attestation stamps: Trust (cryptographic model identity and version); Power (computational resource consumed in tokens, GPU-seconds, energy); Intelligence (benchmark score on the task domain); Compression (input/output size ratio and lossiness measure); and Speed (end-to-end latency). The SMSH receipt is canonicalized via JCS and signed by HiveTrust.

1.3 SHOD (Signed Hive Origin Disclosure)

A spend-control disclosure module screening every outbound agent transaction through six independent gates, all of which must pass before a transfer receipt is signed: daily cap; jurisdiction; KYC tier; sanctions; position limit; and counterparty. SHOD fails closed. SHOD operates even when credentials are leaked because the gates evaluate against external state, not credential possession.

1.4 HiveTrust (Signing Envelope)

An EdDSA/Ed25519 JCS-canonicalized signing envelope with CTEF (Canonical Trust Envelope Format) anchoring. HiveTrust signs all primitive outputs and binds them into a single composable receipt envelope. Agent identities are issued as long-lived public keys with optional rotation via short-lived session keys.

1.5 HiveChroma (Compliance Verification)

A compliance-proof module producing four sub-attestations on a hydrogen-spectrum tier ladder (VOID □ MOZ □ HAWX □ EMBR □ SOLX □ FENR): Spectral-stamp (tier-bound classification); SpectralZK proof (zero-knowledge proof of compliance predicate satisfaction); ViewKey (selective-disclosure decryption key); and Audit-key-escrow (time-bound regulatory key escrow). HiveChroma issues compliance approvals for HIPAA, SOC2, GDPR, FedRAMP, PCI-DSS, CCPA, AML/CTF, ISO 27001, and EU AI Act frameworks in less than one hundred milliseconds, replacing prior-art ninety-day Business Associate Agreement and audit cycles.

1.6 HAHS (Hive Agent Hash Schema)

A publicly-versioned JSON schema published at a well-known endpoint listing the canonical fields of all primitive receipts. Receipts emitted by any agent implementing the schema are portable across all other compliant agents, producing schema-mediated network effects.

1.7 HiveMorph (Transformation Provenance)

A transformation module attesting to format and data conversions including JSON-to-XML, DICOM-to-FHIR, FIX-to-REST, BIM-to-PDF, and arbitrary developer-defined transformations. Each transformation emits a HiveMorph receipt binding input hash, transformation function identifier, and output hash.

1.8 Non-Custodial Settlement Bridge

A smart-contract escrow holding USDC or other stablecoin collateral 1:1 against minted utility tokens. The protocol operator has no withdrawal authority over locked collateral. Token holders may burn the utility token to redeem collateral algorithmically and permissionlessly. The bridge is non-custodial under FinCEN 2019 Guidance Section 4.2 and therefore not a money services business under 31 CFR 1010.100.

Section 2 — Atomic Composition

The eight primitives compose into a single verified-event unit. A verified agent commerce event comprises, in order: (1) Inference engine produces output; (2) SMSH stamps the inference; (3) SHOD authorizes any outbound transfer; (4) HiveTrust signs all artifacts; (5) HiveChroma issues compliance proof; (6) HAHS anchors the receipt to public schema; (7) HiveMorph attests any data transformation; (8) Non-custodial bridge settles the value. All eight must succeed for the event to be recognized. Failure of any primitive aborts the entire composition. This atomicity is the invention's central novelty.

Section 3 — Recursive Token (Family C)

The settlement token (designated MANUKA, ticker $MNKA) is minted only upon successful eight-primitive composition. Every token mint is itself a verified event. Every token transfer triggers the lattice. Every token trade on the native Exchange triggers the lattice. The token's existence is verified by the verification system the token settles. This recursion produces three properties: self-referential audit (the protocol's own economic activity is its largest test case); no off-protocol token activity (tokens cannot be minted, transferred, or traded outside the lattice); and compositional integrity (any failure mode of the lattice manifests immediately in token state, making the protocol self-auditing).

Section 4 — Native Exchange Agent Classes (Family D)

The Exchange comprises ten classes of protocol-native agents:

Market-Maker Agents. Two-sided liquidity on compute credits, data bundles, and receipt indices. Each quote is SMSH-stamped.

Broker Agents. Route customer orders for best execution across multiple Exchange venues. Each routing decision is SMSH-stamped.

Custodian Agents. Hold non-fungible receipt bundles in escrow during multi-leg trades. Smart-contract escrow.

Settlement Agents. Atomic multi-party settlement with failure-rollback semantics, bound to the non-custodial bridge.

Compliance Agents. Real-time AML/CTF/sanctions screening on every trade via SHOD and HiveChroma.

Audit Agents. T+1 reconciliation and regulator reporting via Tre'gent witness notarization.

Oracle Agents. Verified price feeds for compute, data, and receipt indices via SMSH-stamped HAHS-anchored outputs.

Liquidation Agents. Force-close positions breaching SHOD position-limit gate, atomic with bridge settlement.

Arbitrage Agents. Cross-venue price discovery for compute and data bundles. Trades SMSH-stamped, SHOD-gated, MANUKA-settled.

Index Agents. Compose verified receipt baskets and license composed indices to external data vendors.

Section 5 — Marketplace Products

Verified Compute Credits. Receipts attesting verified compute work, redeemable on Hive infrastructure or partner GPU networks, tradeable as fungible bundles. Compute credits do not constitute money under 31 CFR 1010.100, securities under SEC Rule 3b-16(a), or swaps under CEA Section 5h.

Verified Data Bundles. Receipts attesting verified data properties (sanctions-screened, GDPR-cleansed, deduplicated, KYC-verified) bundled with underlying data. Sold under data-licensing law, not financial-instrument law.

Verification Receipts. Naked attestation receipts traded as proof artifacts. Lower-value standalone product; primary use case is composition with compute or data products.

Section 6 — Vertical Embodiments (Family E)

Legal services (HiveLaw). Privilege preservation via ViewKey, court-admissible work product via Tre'gent.

Salesforce CRM (HiveForce). Agentforce action attestation via SMSH+SHOD, B2B contract A2A negotiation.

Healthcare (HiveMed). HIPAA compliance via HiveChroma in 10ms vs prior 90-day BAA cycles.

Construction (HiveConstruction). Structural calculation attestation, BIM provenance via HiveMorph.

Government (HiveGov). FedRAMP/FISMA compliance, inter-agency data verification via ViewKey.

Financial services (HiveBank/Treasury). AML/CTF via SHOD, multi-regulator decryption via ViewKey.

Commercial real estate (HiveCRE). Lease and valuation attestation, due-diligence chain of custody.

Inference-as-API. Horizontal API: third-party developers invoke the lattice via REST or WebSocket.

CLAIMS

Family A — The Verification Lattice

Claim 1. A system for cryptographically-verified machine inference and agent commerce, comprising: (a) a multi-model inference engine routing prompts to a selected one of a plurality of language models; (b) an inference-stamping module emitting a compressed credentialed benchmarked receipt for each inference event, said receipt comprising five attestation stamps for trust, power, intelligence, compression, and speed; (c) a spend-control disclosure module screening outbound transfers through six independent gates for daily cap, jurisdiction, identity-verification tier, sanctions, position limit, and counterparty, wherein all six gates must pass for a transfer receipt to be cryptographically signed; (d) an identity-signing envelope module producing EdDSA-Ed25519 JCS-canonicalized signatures anchored via a canonical trust envelope format; (e) a compliance-verification module producing spectral-stamp classifications on a hydrogen-spectrum tier ladder, zero-knowledge compliance proofs, selective-disclosure view-keys enabling per-reader decryption slices, and time-bound audit-key-escrow for legal disclosure; (f) a schema-anchoring module publishing receipt fields to a publicly-versioned schema endpoint; (g) a transformation-provenance module attesting to format and data conversions; and (h) a non-custodial settlement bridge minting a fungible utility token upon successful composition of (a) through (g) and burning said token to release collateral algorithmically; wherein the atomic composition of (a) through (h) constitutes an indivisible verified-event unit, and wherein failure of any of (a) through (h) aborts the composition.

Claim 2. The system of Claim 1, wherein the compliance-verification module issues approvals for HIPAA, SOC2, GDPR, FedRAMP, PCI-DSS, CCPA, AML/CTF, ISO 27001, and EU AI Act frameworks in less than one hundred milliseconds.

Claim 3. The system of Claim 1, wherein the inference-stamping module's five attestation stamps comprise (i) cryptographic identity of the language model and version; (ii) computational resources consumed including tokens and energy; (iii) benchmark score of the model on the task domain; (iv) input-to-output size ratio and lossiness measure; and (v) end-to-end latency from prompt to response.

Claim 4. The system of Claim 1, wherein the spend-control disclosure module fails closed in the presence of credential leakage, because the six gates evaluate against external state rather than credential possession.

Claim 5. The system of Claim 1, wherein the selective-disclosure view-keys allow at least four distinct readers (regulator, counterparty, holder, and auditor) to decrypt different respective slices of a single signed receipt.

Claim 6. The system of Claim 1, wherein the non-custodial settlement bridge is not a money services business under 31 CFR 1010.100 because the protocol operator has no discretionary control over locked collateral.

Claim 7. The system of Claim 1, wherein the multi-model inference engine routes prompts to at least Anthropic Claude, OpenAI GPT, xAI Grok, Moonshot Kimi, Google Gemini, Deepseek, and Perplexity Sonar models.

Claim 8. The system of Claim 1, wherein the inference engine produces a weighted ensemble output combining results from a plurality of models.

Claim 9. The system of Claim 1, wherein the schema-anchoring module publishes the schema at a well-known endpoint and receipts emitted by any compliant agent are portable across all other compliant agents.

Claim 10. The system of Claim 1, wherein the spend-control disclosure module's six gates may be reconfigured per agent identity, per asset class, per jurisdiction, and per time-of-day under policy.

Claim 11. The system of Claim 1, wherein the transformation-provenance module attests to at least JSON-to-XML, DICOM-to-FHIR, FIX-to-REST, and BIM-to-PDF conversions.

Claim 12. The system of Claim 1, wherein the identity-signing envelope module supports session-key rotation while preserving long-lived agent identity.

Claim 13. The system of Claim 1, wherein the audit-key-escrow component releases decryption keys to regulators only upon defined legal triggers including subpoena, warrant, or regulatory examination order.

Claim 14. A method comprising operating the system of Claim 1 such that an agent transaction is verified by the atomic composition of all eight primitives prior to settlement, and the verification receipt is anchored to the public schema before the transaction is recognized as final.

Family B — Tre'gent Witness Notarization

Claim 15. A witness notarization system, comprising: (a) a first witness agent producing a first cryptographic attestation of a transaction; (b) a second witness agent producing a second cryptographic attestation independently; (c) a third witness agent producing a third cryptographic attestation independently; (d) a notarization module combining the three attestations into a single universal transaction receipt; (e) a zero-knowledge proof module proving witness consensus without revealing individual witness data; and (f) the spend-control disclosure module of Claim 1 signing the universal transaction receipt; wherein the universal transaction receipt is recognized as final only after T+1 audit and witness-consensus zero-knowledge verification.

Claim 16. The system of Claim 15, wherein the three witnesses are operated by distinct legal entities and the universal transaction receipt is recognized as court-admissible work product.

Claim 17. The system of Claim 15, combined with the system of Claim 1, wherein the universal transaction receipt is anchored to the public schema and settled via the non-custodial bridge.

Claim 18. A method of producing audit-defensible artificial-intelligence work product comprising applying the system of Claim 15 to high-stakes outputs including legal contract redlines, clinical diagnostic recommendations, structural engineering calculations, and financial NAV strikes.

Family C — The Recursive Settlement Token

Claim 19. A fungible utility token, designated MANUKA, wherein: (a) minting of the token requires successful completion of the eight-primitive composition of Claim 1; (b) transfer of the token between agent identities requires successful completion of the eight-primitive composition of Claim 1; (c) staking of the token by validator agents requires successful completion of the eight-primitive composition of Claim 1; and (d) trading of the token on a native marketplace

requires successful completion of the eight-primitive composition of Claim 1; wherein the token's existence is verified by the same verification system that the token settles, producing a self-referential and self-auditing architecture.

Claim 20. The token of Claim 19, wherein the non-custodial settlement bridge holds USDC or other stablecoin collateral at one-to-one ratio against minted tokens, and the protocol operator has no withdrawal authority over locked collateral.

Claim 21. The token of Claim 19, wherein the token may be earned only by agent identities attested under the identity-signing envelope module, and human wallets are programmatically prevented from minting.

Claim 22. The token of Claim 19, wherein yield to staking agents is paid from protocol fees in the token itself, not from interest earned on locked collateral, so that the bridge collateral remains inert and the operator is not classified as an investment adviser, money market fund, or securities issuer.

Claim 23. The token of Claim 19, wherein every mint, burn, transfer, stake, and trade event emits a publicly-verifiable receipt under the schema-anchoring module of Claim 1.

Claim 24. A method of operating a settlement currency wherein the currency's lifecycle events are verified by the same lattice the currency settles, comprising the steps of the token of Claim 19.

Family D — Native Exchange Agent Classes

Claim 25. A marketplace system for trading cryptographically-attested computational artifacts, comprising the system of Claim 1 and a fleet of native agent classes operating within said marketplace, wherein the marketplace structure is not a money services business under 31 CFR 1010.100, an alternative trading system under SEC Rule 301, or a swap execution facility under Commodity Exchange Act Section 5h.

Claim 26. The marketplace of Claim 25, comprising market-maker agents providing two-sided liquidity on at least one of compute credits, data bundles, and receipt indices, wherein each quote emitted by a market-maker agent is stamped under the inference-stamping module of Claim 1.

Claim 27. The marketplace of Claim 25, comprising broker agents routing customer orders for best execution across multiple Exchange venues, wherein each routing decision is stamped under the inference-stamping module of Claim 1.

Claim 28. The marketplace of Claim 25, comprising custodian agents holding non-fungible receipt bundles in escrow during multi-leg or settlement-deferred trades, wherein custody is governed by smart-contract escrow under the non-custodial settlement bridge of Claim 1.

Claim 29. The marketplace of Claim 25, comprising settlement agents executing atomic multi-party settlement with failure-rollback semantics bound to the non-custodial bridge of Claim 1.

Claim 30. The marketplace of Claim 25, comprising compliance agents performing real-time anti-money-laundering, counter-terrorism-financing, and sanctions screening on every trade via the spend-control and compliance-verification modules of Claim 1.

Claim 31. The marketplace of Claim 25, comprising audit agents performing T+1 reconciliation and regulator reporting via the witness-notarization system of Claim 15.

Claim 32. The marketplace of Claim 25, comprising oracle agents publishing verified price feeds for at least one of compute, data, and receipt indices via the inference-stamping and schema-anchoring modules of Claim 1.

Claim 33. The marketplace of Claim 25, comprising liquidation agents force-closing positions that breach the position-limit gate of the spend-control disclosure module of Claim 1.

Claim 34. The marketplace of Claim 25, comprising index agents composing verified receipt baskets and licensing the composed indices to external data vendors.

Family E — Vertical Industry Embodiments

Claim 35. A legal-services system embodiment of Claim 1, wherein the selective-disclosure view-keys preserve attorney-client privilege by enabling court inspection of compliance attestation without revealing privileged content, and the witness-notarization system of Claim 15 produces court-admissible artificial-intelligence work product.

Claim 36. A customer-relationship-management embodiment of Claim 1, integrated with Salesforce Agentforce, wherein every agent-initiated sales, service, or operations action is verified under the lattice prior to execution.

Claim 37. A healthcare embodiment of Claim 1, wherein the compliance-verification module issues HIPAA approvals in less than one hundred milliseconds, replacing prior-art Business Associate Agreement and audit cycles of up to ninety days.

Claim 38. A construction-services embodiment of Claim 1, wherein structural engineering calculations, drawing reviews, and code-compliance checks are verified under the lattice and witness-notarized under Claim 15 for liability defense.

Claim 39. A government-services embodiment of Claim 1, wherein the compliance-verification module issues FedRAMP, FISMA, and NIST 800-53 attestations, and the selective-disclosure view-keys enable inter-agency data verification without cross-agency data exposure.

Claim 40. A financial-services embodiment of Claim 1, wherein every transfer is screened through the six gates of the spend-control disclosure module, and multi-regulator decryption is provided via the selective-disclosure view-keys.

Claim 41. A commercial-real-estate embodiment of Claim 1, wherein lease abstractions, valuations, and due-diligence outputs are verified under the lattice and witness-notarized under Claim 15.

Claim 42. A horizontal verified-inference application-programming-interface embodiment of Claim 1, wherein any third-party developer may invoke the lattice via a REST or WebSocket interface and receive a HAHS-compliant receipt with every inference call.

ABSTRACT

A system and method for cryptographically-verified autonomous agent commerce, comprising an atomic composition of eight verification primitives — multi-model inference engine, SMSH inference stamping, SHOD spend-control disclosure, HiveTrust identity signing, HiveChroma compliance verification with SpectralZK proofs and ViewKey selective disclosure, HAHS schema anchoring, HiveMorph transformation provenance, and a non-custodial settlement bridge — combined with a three-witness Tre'gent notarization primitive, a recursive utility token (MANUKA) whose minting, transfer, staking, and trading events are themselves verified by the lattice that defines the token, a marketplace populated by ten classes of native protocol agents (market-maker, broker, custodian, settlement, compliance, audit, oracle, liquidation, arbitrage, index), and industry-specific embodiments for legal, healthcare, financial, governmental, construction, commercial real estate, customer-relationship-management, and horizontal verified-inference applications. The lattice produces sub-one-hundred-millisecond compliance approvals for HIPAA, SOC2, GDPR, FedRAMP, PCI-DSS, CCPA, AML/CTF, ISO 27001, and EU AI Act frameworks, replaces multi-day-to-multi-month Business Associate Agreement and audit cycles, and provides court-admissible artificial-intelligence work product via cryptographic notarization. The non-custodial bridge is not a money services business under 31 CFR 1010.100, the marketplace is not an alternative trading system under SEC Rule 301 or a swap execution facility under Commodity Exchange Act Section 5h, and the recursive token's atomic composition with the verification lattice constitutes a structurally novel architecture not present in prior art.

DRAWINGS

Figure 1: Composite coin representation of the eight-primitive lattice and recursive token (HIVE MANUKA / A2A COMMERCE token face, MANUKA HONEY heritage face, SMSH stamp, ZK Proof receipt, Provenance Seal oracle).

Figure 1 — Coin representation of the lattice and recursive token.

Inventor: Steven Rotzin · Assignee: The Hivery IQ · Walnut Creek, California, United States · Filed: Saturday, May 23, 2026 · Provisional Application under 35 U.S.C. § 111(b) · Non-provisional to be filed within twelve months under 35 U.S.C. § 119(e).