SYSTEM AND METHOD FOR ESTABLISHING CRYPTOGRAPHIC PROVENANCE AND CONTINUITY OF DIGITAL ARTIFACTS REPRESENTING COGNITIVE EVENTS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application Serial No. 63/955,018, filed January 6, 2026, and titled "SYSTEM AND METHOD FOR ESTABLISHING PROVABLE ORIGINATION AND TEMPORAL CONTINUITY OF HUMAN THOUGHT USING CRYPTOGRAPHIC CUSTODIAL CHAINS," the entire contents of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present disclosure relates to cryptographic recordkeeping, evidentiary custody systems, authorship verification, and legal-grade provenance. More particularly, it relates to systems and methods for cryptographically sealing, timestamping, chaining, anchoring, and custodially preserving human-originated cognitive artifacts ("Thoughts") to establish provable origination, temporal priority, continuity of ideation, and evidentiary integrity without requiring public disclosure.

BACKGROUND OF THE INVENTION

[0003] Conventional mechanisms for establishing authorship, invention priority, and provenance rely on publication platforms, patent offices, notaries, institutional trust, or centralized digital services. These mechanisms are slow, jurisdiction-bound, disclosure-forcing, and increasingly ineffective in the presence of generative systems capable of producing synthetic artifacts at scale. File timestamps can be manipulated, custody can be disputed, and perfect duplication destroys evidentiary scarcity.

[0004] More fundamentally, modern computing systems (including conventional file systems, collaboration platforms, registries, and timestamping services) do not implement a cryptographically governed object type or custody protocol that

> (i) deterministically canonicalizes a digital artifact explicitly attributed to , via cryptographic credentials, to a declared human author with cryptographically verifiable authorship into stable bytes,

Attorney Docket No. 19842-015USU1

(ii) binds the artifact to cryptographic identifiers and trusted temporal attestations,

(iii) preserves the artifact within an immutable custody bundle under author-controlled disclosure, and

(iv) supports cryptographic chaining and optional public or consortium anchoring to provide tamper-evident origination and continuity. In addition, as generative systems increasingly produce synthetic bitstreams at scale, mere possession of a digital artifact or a platform timestamp no longer provides reliable evidence of human origination, priority, or integrity.

SUMMARY OF THE INVENTION

[0005] The invention provides systems, methods, and computer-readable media implementing a cryptographically governed object type and custody protocol for digital records of human cognitive artifacts, comprising Genesis records, append-only chained Thought records, deterministic canonicalization, cryptographic hashing, timestamp attestation, custodial storage, optional multi-custodian redundancy, public or consortium ledger anchoring, selective disclosure controls, deterministic restoration, and evidentiary certificate generation.

[0006] In exemplary embodiments, the system enables provable establishment of origination, temporal priority, custody, and lineage of digital records of human cognitive artifacts independent of publication, patent filing, or institutional trust. Embodiments further support trade secret continuity, research provenance, creative authorship verification, long horizon legacy chains, jurisdiction-specific evidentiary packaging, and cryptographically recorded third-party awareness, interest, or valuation signaling generated without disclosure of sealed content, thereby enabling market signaling and defensive verification while preserving confidentiality. The system further supports declared provenance classification (e.g., human originated, assisted, mixed, machine generated, or unknown) for evidentiary clarity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 is a system architecture diagram illustrating an exemplary Proof-of-Thought™ platform, showing an author device in communication with a processing system including canonicalization, hashing and chaining, timestamp attestation, custody, control, anchoring, and verification modules.

[0008] FIG. 2 is a flow diagram illustrating sealing a Genesis Thought, including canonicalization, hash generation, trusted timestamp attestation, custody bundle creation, immutable storage, and issuance of a cryptographic receipt.

[0009] FIG. 3 is a schematic diagram illustrating an append-only cryptographic Thought chain in which each subsequent Thought incorporates predecessor hash values to establish irreversible continuity and provable chronological ordering.

[0010] FIG. 4 is a custody topology diagram illustrating redundant multi-custodian preservation across multiple independent custodial authorities to provide jurisdiction-resilient evidentiary permanence and cryptographic integrity verification.

[0011] FIG. 5 is a schematic diagram illustrating generation of a human-readable evidentiary certificate and machine-engraved seal derived from sealed Thought data, including hashes, timestamp attestations, chain identifiers, and custody references.

[0012] FIG. 6 is a schematic diagram illustrating selective disclosure and verification of sealed Thoughts using cryptographic control references for verification, controlled disclosure, and retrieval of custody-bound verification data.

[0013] FIG. 7 is a conceptual diagram illustrating a time-indexed Genesis–Thought continuum depicting the evolutionary progression of an idea across successive sealed Thoughts.

DETAILED DESCRIPTION

[0014] **Definitions (Non-Limiting).**

[0015] **"Thought"** means a digital artifact representing an original human cognitive event or expression, transformed into a digital record, including without limitation text, images, audio, video, diagrams, structured data, software code, archives, or three-dimensional model data.

[0016] **"Genesis Thought"** means a first sealed Thought establishing origination and temporal priority for a Thought chain.

[0017] **"Thought Chain"** (also referred to herein as a "Chained Thought" or "Chain Thought") means an append-only cryptographic sequence of sealed Thoughts evidencing temporal evolution of cognition.

[0018] "Custody Bundle" means a cryptographically bound package comprising canonicalized content, cryptographic identifiers, timestamp attestations, chain references, custody proofs, and associated metadata sufficient to verify integrity, priority, and continuity.

[0019] "Custodial Authority" means a neutral preservation entity, human-operated or automated, configured to maintain immutable custody bundles, enforce protocol-defined access restrictions, and produce cryptographic audit proofs demonstrating correct preservation behavior.

[0020] "Control Authority" means a cryptographic capability, protocol role, or key-based authority that governs continuation of a Thought Chain, selective disclosure, verification, delegation, revocation, escrow, succession, or restoration operations, where such authority is technically enforced by the system rather than by discretionary human decision-making.

[0021] "Control Reference" or "Control Key" means a cryptographic reference, token, or key material embodying Control Authority for a given Custody Bundle or Thought Chain.

[0022] "Thought Vault" means a logical or physical custodial container implemented by the system for storing one or more Custody Bundles under immutable storage semantics and cryptographic access control, such that sealed Thoughts are preserved, audited, and disclosed only according to valid Control Authority.

[0023] "Canonicalization" means a deterministic transformation of a digital artifact into a stable byte sequence that is invariant to formatting, encoding, metadata ordering, or platform-specific representation, such that identical semantic content produces identical canonical bytes.

[0024] "Trusted Timestamp Attestation" means a cryptographically verifiable assertion of time issued by an external or independent time source and bound to a cryptographic identifier such that alteration or reassignment invalidates verification.

[0025] "Successor Thought" means a sealed Thought that cryptographically references at least one predecessor Thought within a Thought Chain to establish chronological continuity.

[0026] Overview of Operation. In exemplary embodiments, an author submits an original Thought transformed into a digital record of a human cognitive artifact to a processing system. The system operates exclusively on digital records and cryptographic metadata, and does not evaluate, judge, or interpret the underlying cognitive content beyond deterministic transformation and verification. The processing system canonicalizes the submitted artifact to

a deterministic byte representation, generates a cryptographic hash identifier, binds one or more trusted timestamp attestations to the identifier, creates a custody bundle, and stores the custody bundle in an immutable custodial storage system. The system issues a cryptographic receipt to the author evidencing successful sealing.

[0027] The author may submit subsequent Thoughts to extend the chain. Each subsequent Thought incorporates at least one predecessor identifier and its own timestamp attestation into cryptographic computation, thereby enforcing append-only chaining and proving irreversible chronological continuity on a machine-enforced basis. Optionally, cryptographic representations of custody bundles are programmatically anchored by the processing system to one or more public or consortium ledgers for independent temporal verification. Verification of existence, priority, and continuity may be performed without disclosure of underlying content.

[0028] Referring now to FIG. 1, a system architecture is illustrated showing both functional modules and sequential processing stages for establishing cryptographic custody of a human cognitive artifact.

[0029] The system comprises a Canonicalization Module (A) configured to receive a raw digital artifact from an author device and transform the artifact into a deterministic canonical byte representation that is invariant to incidental formatting, encoding, or platform-specific differences. A Hashing and Chaining Module (B) is configured to compute a cryptographically secure identifier from the canonical byte representation and to incorporate one or more predecessor identifiers, thereby enforcing append-only continuity across successive sealed artifacts.

[0030] A Timestamp Attestation Interface (C) is configured to interact with one or more trusted external time sources to cryptographically bind a verifiable temporal attestation to the computed identifier. An Author Control Interface (D) is configured to manage the issuance, delegation, and enforcement of cryptographic control keys, thereby technically enforcing author sovereignty over access, disclosure, and verification operations associated with the sealed artifact.

[0031] As further depicted by the process flow arrows in FIG. 1, the system operates in a defined sequence of steps. In a first step (1), the system performs canonicalization and hashing to establish a unique cryptographic fingerprint of the artifact. In a second step (2), the system performs timestamp attestation to fix temporal priority. In a third step (3), the system

Attorney Docket No. 19842-015USU1

performs custody bundle creation, packaging the canonical data, cryptographic identifiers, and timestamp attestations into a unified evidentiary unit. In a final step (4), the custody bundle is committed to immutable preservation storage, and a cryptographic receipt is generated and returned to the author device.

[0032] Collectively, the architecture and sequence illustrated in FIG. 1 establish machine-enforced origination, temporal continuity, and evidentiary integrity of the human cognitive artifact without reliance on discretionary human trust.

[0033] Referring now to FIG. 2, a sequential workflow is illustrated for sealing a Genesis Thought according to one embodiment of the system.

[0034] In a first step, an Author Thought, representing a digital artifact corresponding to a human cognitive event, is submitted to the system. In a subsequent step, the system performs Canonicalization, transforming the submitted artifact into a deterministic canonical byte representation that is invariant to formatting, encoding, metadata ordering, or platform-specific representation.

[0035] In a next step, Hash Generation is performed, wherein a cryptographic hash value is generated from the canonical byte representation, such that any modification to the canonical bytes produces a materially different hash value. In a further step, the system obtains a Timestamp Attestation, cryptographically binding the hash value to at least one trusted independent time source.

[0036] In a subsequent step, a Custody Bundle is created, packaging at least the canonical byte representation, the cryptographic hash value, and the timestamp attestation into a unified evidentiary structure. In a next step, the custody bundle is committed to Immutable Custody Storage operating under write-once or append-only semantics that prevent alteration, substitution, or retroactive rewriting.

[0037] Finally, in a concluding step, a Cryptographic Receipt is issued to the author. The cryptographic receipt serves as machine-verifiable evidence that the Genesis Thought has been successfully sealed, timestamped, and preserved by the system.

[0038] Referring now to FIG. 3, a schematic representation of an append-only Thought Chain is illustrated. The chain originates with a Genesis Thought (T0), for which an initial cryptographic hash value (H0) is generated based on a canonicalized byte representation of T0.

[0039] Each subsequent Thought in the chain is cryptographically bound to its predecessor. For example, a subsequent Thought (T1) is processed to generate a hash value (H1) derived from a deterministic combination of the canonicalized content of T1 and the prior hash value H0. This process is repeated for subsequent Thoughts (T2, T3), such that $H2 = Hash(T2 \parallel H1)$ and $H3 = Hash(T3 \parallel H2)$, respectively.

[0040] This recursive hashing structure ensures that each Thought is immutably linked to the full history of preceding Thoughts. Any alteration to a prior Thought (e.g., T0 or T1) would result in a corresponding change to all subsequent hash values, thereby breaking cryptographic continuity and rendering tampering mathematically detectable.

[0041] Referring now to FIG. 4, a custody topology diagram illustrating a redundant multi-custodian architecture is shown. An Author submits a Thought to a Proof-of-Thought Custody Layer, which operates as a protocol-level interface for canonicalization, cryptographic sealing, and custody bundle generation.

[0042] Rather than relying on a single preservation entity, the system distributes one or more custody bundles to a plurality of independent custodians, illustrated as Custodian A, Custodian B, and Custodian C. Each custodian is configured to maintain an immutable copy of the custody bundle under write-once or append-only storage semantics that prevent alteration, substitution, or retroactive rewriting.

[0043] The Proof-of-Thought Custody Layer enforces custody control, authorization, and verification logic independently of any individual custodian, such that no single custodian constitutes a trust anchor or point of failure. This topology provides fault tolerance, jurisdictional resilience, and long-term evidentiary survivability, ensuring that the sealed Thought remains verifiable even if one or more custodians become unavailable, compromised, or cease operation.

[0044] Referring now to FIG. 5, a schematic is shown illustrating steps for generating evidentiary outputs derived from a Sealed Thought. Following sealing and custody establishment, cryptographic state data associated with the Sealed Thought is provided, as a subsequent step, to a Seal Engraving Engine.

[0045] In this step, the Seal Engraving Engine is configured to algorithmically derive a tamper-evident representation from one or more elements of the cryptographic custody state, without exposing the sealed content itself. In certain embodiments, this derivation step

includes generating visual, textual, or machine-readable encodings deterministically from cryptographic metadata associated with the Sealed Thought.

[0046] As a further step, the Seal Engraving Engine outputs a Machine-Engraved Certificate, which may be embodied as a digital document, such as a PDF, or as a physical artifact, such as a printed or engraved certificate. The Machine-Engraved Certificate embeds verification fields including, but not limited to, a cryptographic hash reference, one or more trusted timestamps, a chain or sequence indicator, and a custody reference associated with the Sealed Thought.

[0047] In a verification step, the Machine-Engraved Certificate is cryptographically bound to the underlying custody record such that any modification to the sealed data, custody chain, or verification parameters renders the certificate invalid or non-verifiable. In this manner, the certificate functions as a human-readable evidentiary artifact that remains machine-verifiable against the underlying cryptographic record.

[0048] Referring currently to FIG. 6, the diagram illustrates the Selective Disclosure and Verification protocol. A Verifier, who may be a third party or auditor, initiates a request. The system, governed by the Control Key held by the author, authorizes a specific level of disclosure. The Custody Layer returns verification evidence via a first pathway (11), providing cryptographic proofs such as the Hash and Timestamp without revealing the content. If full disclosure is authorized, the system provides a Verified Disclosure via a second pathway (12). This separation allows the existence, priority, and integrity of a Thought to be proven to external parties while maintaining strict privacy control over the underlying intellectual property (via path 11) until the author chooses to reveal it (via path 12).

[0049] **Cryptographic Architecture: Canonicalization and Cryptographic Sealing.** Canonicalization transforms a submitted Thought into a deterministic byte sequence that is stable across encoding differences, formatting changes, metadata ordering, line endings, containerization, compression headers, and platform variations. The canonicalization process is configured such that semantically identical content produces identical canonical bytes, while any semantic or bit-level difference produces a distinct canonical representation.

[0050] A cryptographic hash is computed over the canonical bytes to generate an immutable content identifier. The hash function may comprise a secure one-way function selected to exhibit collision resistance and an avalanche property, such that any bit-level alteration of the

canonical bytes produces a materially different identifier. This property renders tampering, substitution, truncation, or re-encoding of sealed Thoughts cryptographically detectable.

[0051] In exemplary embodiments, the canonical byte representation and resulting hash identifier are treated as authoritative for all subsequent custody, chaining, timestamping, anchoring, and verification operations. No downstream operation alters the canonical bytes after sealing.

[0052] In certain implementations, a user interface renders a cryptographically-derived visualization or summary prior to final sealing to provide transparency into the canonicalization and hashing event, without exposing or modifying the canonical byte sequence itself.

[0053] In certain implementations, the user interface renders a cryptographically-derived visualization prior to final sealing to provide transparency into the canonicalization and hashing event.

[0054] **Illustrative Canonicalization Example (Non-Limiting)**. To clarify the role of canonicalization prior to cryptographic sealing, the following simplified example is provided. This example is non-limiting and is intended to illustrate deterministic normalization of semantically identical content that would otherwise hash differently due to incidental representation differences.

[0055] Example Thought (intended semantic content):

[0056] In practice, the same semantic content may be represented by different byte sequences depending on software, platform, or storage conditions.

[0057] **Input A (non-canonical form):** UTF-8 text including a byte order mark (BOM), Windows-style CRLF line ending, and trailing spaces.

[0058] Textual view:

[0059] Use graphene membrane for front projection film.

[0060] Representative byte sequence (hexadecimal, non-exhaustive): EF BB BF 49 6E 76 65 6E 74 69 76 65 20 6E 6F 74 65 3A 20 55 73 65 20 67 72 61 70 68 65 6E 65 20 6D 65 6D 62 72 61 6E 65 20 66 6F 72 20 66 72 6F 6E 74 20 70 72 6F 6A 65 63 74 69 6F 6E 20 66 69 6C 6D 2E 20 20 0D 0A

Input B (non-canonical form): UTF-8 text with no BOM, Unix-style LF line ending, and no trailing spaces.

[0061] Textual view:

[0062] Use graphene membrane for front projection film.

[0063] Representative byte sequence (hexadecimal, non-exhaustive): 49 6E 76 65 6E 74 69 76 65 20 6E 6F 74 65 3A 20 55 73 65 20 67 72 61 70 68 65 6E 65 20 6D 65 6D 62 72 61 6E 65 20 66 6F 72 20 66 72 6F 6E 74 20 70 72 6F 6A 65 63 74 69 6F 6E 20 66 69 6C 6D 2E 0A

[0064] Although Input A and Input B are semantically identical to a human reader, they are not byte-identical and would ordinarily produce different cryptographic hash outputs if hashed directly.

[0065] In exemplary embodiments, the system applies a deterministic canonicalization function prior to hashing. Canonicalization may include, without limitation:

    1.   Removal of non-semantic encoding markers (e.g., UTF-8 BOM).

    2.   Normalization of line endings to a canonical form (e.g., LF).

    3.   Removal of trailing whitespace where not semantically meaningful.

    4.   Normalization of structural ordering and container metadata where applicable.

[0066] After canonicalization, both Input A and Input B yield the same canonical byte sequence.

[0067] **Canonical form (textual view):** Use graphene membrane for front projection film.

[0068] **Canonical byte sequence (hexadecimal):** 49 6E 76 65 6E 74 69 76 65 20 6E 6F 74 65 3A 20 55 73 65 20 67 72 61 70 68 65 6E 65 20 6D 65 6D 62 72 61 6E 65 20 66 6F 72 20 66 72 6F 6E 74 20 70 72 6F 6A 65 63 74 69 6F 6E 20 66 69 6C 6D 2E 0A

[0069] The cryptographic identifier is computed exclusively over the canonical byte sequence (and, in certain embodiments, cryptographically bound timestamp attestation data). As a result, both non-canonical inputs produce the same identifier, while any substantive modification to the content produces a different canonical byte sequence and therefore a different identifier.

[0070] This example demonstrates that cryptographic sealing reflects the substance of the digital record rather than incidental differences in formatting, encoding, or storage representation, enabling reliable provenance, priority, and continuity verification.

[0071] **Timestamp Attestation and Temporal Priority:** In exemplary embodiments, a trusted timestamp attestation is obtained and cryptographically bound to the hash identifier of each sealed Thought to establish temporal priority. The binding operation associates the hash identifier with one or more verifiable time values such that the timestamp cannot be altered, removed, or reassigned without invalidating the identifier.

[0072] Timestamp attestations may be obtained from one or more independent time sources, including without limitation trusted timestamping authorities, public time services, consortium-operated services, secure time beacons, or other verifiable temporal anchors. Multiple independent attestations may be obtained for a single Thought to improve resilience against single-source failure, compromise, or dispute.

[0073] Each timestamp attestation is incorporated into the custody bundle and, where applicable, into cryptographic material used for successor chaining. By binding timestamps directly to canonicalized content identifiers, the system prevents post-hoc backdating, reordering, or substitution of sealed Thoughts. Any modification to the canonicalized content, hash identifier, or associated timestamp produces a different cryptographic result that is detectable during verification.

[0074] The timestamp attestation mechanism therefore provides a machine-enforced basis for temporal priority that is independent of file-system timestamps, platform clocks, or institutional recordkeeping.

[0075] **Append-Only Chaining and Continuity:** Subsequent Thoughts extend an existing Thought Chain by incorporating a cryptographic reference to a predecessor Thought (including, without limitation, a predecessor hash value, chain identifier, or other derived commitment) into the successor Thought's hash computation. As a result, each successor Thought is mathematically bound to the exact state of its predecessor at the time of sealing.

[0076] Because secure cryptographic hash functions exhibit an avalanche effect in which a single-bit change to an input produces a substantially different output, any alteration, omission, or substitution of a predecessor Thought invalidates the cryptographic identifiers of

all successor Thoughts. This property renders the chain append-only and enforces irreversible chronological continuity on a machine-enforced basis.

[0077] In exemplary embodiments, Thought Chains may be linear or may branch to represent divergent ideation paths originating from a common predecessor Thought. Branching preserves full cryptographic lineage to the shared origin while allowing independent evolution of parallel cognitive developments.

[0078] The chain records continuity of ideation rather than intellectual hierarchy. A successor Thought may represent a minor revision, an intermediate exploration, or a substantial conceptual or inventive breakthrough, while remaining cryptographically anchored to its antecedents.

[0079] **Custodial Storage, Neutrality, and Auditability:** Custody Bundles are stored in an immutable custodial storage system configured to prevent alteration, removal, substitution, or retroactive rewriting after sealing. In exemplary embodiments, immutability is enforced through cryptographic integrity verification, write-once or append-only storage semantics, and tamper-detection mechanisms that invalidate custody proofs upon unauthorized modification.

[0080] Custodial Authorities operate under protocol-enforced neutrality constraints that restrict unauthorized access, disclosure, alteration, monetization, mining, profiling, training, or derivation of secondary value from preserved Thoughts absent explicit cryptographic authorization from a Control Reference associated with the Custody Bundle.

[0081] Custodial systems may further maintain cryptographic audit logs, integrity proofs, and preservation attestations demonstrating correct custody behavior over time. Such audit materials may include, without limitation, storage proofs, access proofs, custody verification records, and cross-custodian consistency checks suitable for evidentiary presentation.

[0082] **Multi-Custodian Redundancy (Optional):** In certain embodiments, Custody Bundles are redundantly preserved across a plurality of independent Custodial Authorities. Each Custodial Authority maintains immutable custody of sealed Thoughts while independently verifying cryptographic identifiers, timestamp attestations, and chain references associated with each Custody Bundle.

[0083] Multi-custodian redundancy provides resilience against single-custodian failure, compromise, jurisdictional disruption, or service discontinuity. Cryptographic consistency

checks may be performed across Custodial Authorities to confirm that identical Custody Bundles are preserved without divergence, substitution, or omission.

[0084] In exemplary implementations, custody verification records generated by each Custodial Authority may be aggregated, compared, or cross-validated to produce cross-custodian consistency proofs suitable for evidentiary presentation, regulatory compliance, and long-horizon archival assurance.

[0085] **Selective Disclosure, Verification, and Control Authority:** In exemplary embodiments, authors are issued one or more cryptographic control references associated with a Custody Bundle that enable third-party verification of existence, temporal priority, integrity, and chain continuity without requiring disclosure of the underlying Thought content. Verification is performed by recomputing cryptographic identifiers, validating bound timestamp attestations, and confirming predecessor references using disclosed proofs or derived commitments, without revealing canonicalized content bytes.

[0086] Selective disclosure is performed by cryptographically authorizing access to a Custody Bundle, a defined subset of its contents, or specific derived verification materials, while preserving immutability and chain integrity guarantees. Disclosure authorizations may be partial, scope-limited, time-bounded, revocable, escrowed, or conditioned on multi-party approval, and may be implemented using asymmetric keys, capability tokens, threshold signatures, or policy-based cryptographic controls.

[0087] Custodial Authorities are cryptographically restricted from accessing or disclosing Thought content absent a valid control reference, such that disclosure capability is technically constrained by the protocol rather than institutional trust. Control authority further governs continuation of a Thought Chain, delegation of rights, revocation of access, escrow arrangements, succession planning, and enforcement of multi-signature or rule-based authorization models, all implemented on a machine-verifiable basis rather than discretionary human decision-making.

[0088] **Succession, Escrow, and Long-Horizon Legacy Chains:** In certain embodiments, the system supports inheritance, escrow, conditional release, and long-horizon succession of control over Thought Chains through cryptographically enforced control references. Control Authority associated with a Custody Bundle or Thought Chain may be escrowed, time-locked, event-locked, or conditionally activatable based on protocol-defined criteria, including without limitation lapse of activity, satisfaction of multi-party authorization

thresholds, presentation of successor credentials, or expiration of specified temporal conditions.

[0089] Succession is implemented as a machine-evaluated cryptographic process rather than discretionary human judgment. Escrowed or delegated control references may be split across multiple parties using threshold cryptography, multi-signature schemes, or policy-based authorization logic, such that no single party can unilaterally assume control absent satisfaction of the defined cryptographic conditions. Upon satisfaction of succession conditions, Control Authority may be transferred to a successor entity while preserving immutability, chain continuity, and custody integrity.

[0090] Accordingly, Thought Chains may persist in a sealed but recoverable state across extended time horizons, including decades or generations, enabling preservation of intellectual legacies, research continuity, and evidentiary priority without requiring continuous access, disclosure, or custodial intervention. Succession policies may be expressed as cryptographic rules or governance policies associated with control references.

[0091] **Deterministic Restoration and Evidentiary Packaging:** In certain embodiments, sealed Thoughts are restored from custodial storage in a bitwise-identical form to the originally sealed canonical byte representation (i.e., the sealed state, not any pre-canonicalized or unsealed form). Restoration operations are performed only upon presentation of valid Control Authority and include recomputation of cryptographic hash identifiers and verification against stored identifiers, timestamp attestations, and chain references to confirm integrity and authenticity.

[0092] Deterministic restoration ensures that any restored instance of a Thought is mathematically identical to the sealed instance, such that verification results are reproducible across systems, custodians, jurisdictions, and points in time. Any deviation in restored content produces a verification failure detectable through hash mismatch or broken chain references.

[0093] In exemplary implementations, restored Thoughts and associated verification materials may be assembled into structured evidentiary packages suitable for legal, regulatory, or archival use. Such evidentiary packages may include, without limitation, canonicalized content, cryptographic identifiers, timestamp attestations, predecessor and successor chain proofs, custody verification records, multi-custodian consistency proofs, anchoring proofs, and human-readable certificates or seals.

[0094] Evidentiary packages may be formatted in jurisdiction-specific or proceeding-specific forms while preserving cryptographic verifiability, enabling independent third parties to validate origination, temporal priority, continuity, and integrity without reliance on custodial discretion or institutional trust.

[0095] Public or Consortium Ledger Anchoring: In certain embodiments, cryptographic representations of Custody Bundles, including without limitation content hashes, chain identifiers, Merkle roots, or other derived commitments, are anchored to one or more public or consortium-operated distributed ledgers to provide independent, third-party temporal verification. Ledger anchoring establishes an external, tamper-resistant corroboration of the existence and state of a Custody Bundle at or before a given time, without requiring disclosure of the underlying Thought content.

[0096] Anchoring operations may be performed for Genesis Thoughts, for successor Thoughts, periodically for batches of Custody Bundles, or according to protocol-defined policy. In certain implementations, only minimal cryptographic commitments are anchored, such that no expressive content, metadata, or personally identifiable information is revealed on the ledger.

[0097] Multiple independent ledgers may be used concurrently or sequentially, including public blockchains, consortium-operated ledgers, or hybrid ledger infrastructures. Cross-ledger anchoring improves resilience against ledger failure, censorship, reorganization, or obsolescence by enabling independent verification from multiple sources. Ledger anchoring thus supplements, rather than replaces, trusted timestamp attestations and custodial audit proofs, providing an additional, machine-verifiable layer of temporal corroboration.

[0098] Multimedia Custody, Preview, and Universal Binary Preservation: Thoughts may include multiple media types including, without limitation, images, portable document format (PDF) files, documents, archives, audio files, video files, media files, software code, structured data, sensor outputs, simulation results, computer-aided design (CAD) files, and three-dimensional model data. The custody bundle preserves media-type descriptors, canonicalization rules, codec or format identifiers, and integrity metadata sufficient to ensure that heterogeneous binary formats are preserved without normalization loss.

[0099] In certain implementations, authorized previews are provided that allow limited human inspection or machine verification (e.g., image thumbnails, audio snippets, video playback, document rendering, or metadata inspection) without transferring custodial control

of the underlying sealed binary or exposing the full canonicalized content. Preview generation is performed against derived or transformed representations that do not substitute for, overwrite, or modify the sealed canonical bytes.

[0100] Universal binary preservation ensures that arbitrary file formats, including proprietary, obsolete, or future-unknown formats, are preserved in a custody-agnostic manner. Deterministic restoration enables binary-accurate reconstitution of sealed assets exactly as sealed, independent of codec availability, software versioning, or platform changes, thereby maintaining evidentiary integrity across long time horizons.

[0101] **Receipts, Certificates, and Machine-Engraved Seals:** Upon sealing, the system may issue a cryptographic receipt containing at least a hash identifier, timestamp attestation, chain reference, and custody verification reference. The system may generate a human-readable evidentiary certificate (e.g., PDF) and/or a physical seal (printed, engraved, etched, laser-marked, embossed) containing machine-generated indicia derived from sealed Thought data. Any alteration of the underlying Thought invalidates the certificate by cryptographic verification failure.

[0102] **Provenance Classification (Declared Origination Metadata):** In certain embodiments, a Genesis Thought or any node within a Thought Chain may be associated with declared provenance metadata indicating an origination classification such as human-originated, assisted, mixed-origin, machine-generated, or unknown. Such provenance classification may be asserted by an originating author at sealing time and cryptographically bound to the Custody Bundle as non-alterable metadata.

[0103] The declared provenance classification is preserved for evidentiary clarity, auditability, and downstream interpretation, without requiring enforcement, inspection, or censorship of the underlying creation process. Verification systems may rely on the classification to distinguish human cognitive origination from machine-generated or hybrid artifacts when evaluating priority, authorship, inventorship, or admissibility, while recognizing that the classification itself reflects an asserted context rather than a determinative judgment by the custodial system.

[0104] **Third-Party Awareness and Signal Recording Without Disclosure:** In certain embodiments, a system is configured to enable third-party awareness and response recording with respect to a Sealed Thought without disclosing the contents of the Thought.

[0105] A Thought may be sealed at a first time, generating canonical bytes and an associated cryptographic identifier. Following sealing, one or more third parties may be provided with limited identifying information associated with the Thought, such as a title, category, abstract, handle, hash, or other non-revealing metadata, while withholding access to the sealed content itself.

[0106] In response to such limited information, a third party may generate a response indicating awareness of the existence of the Sealed Thought. In some embodiments, the response comprises an acknowledgement of awareness generated without access to or review of the sealed content. In further embodiments, the response may include an optional signal, such as an indication of interest, perceived relevance, or valuation range, generated without disclosure of the sealed content and without transfer of any rights in the Thought.

[0107] Responses are recorded by the system as append-only entries in a registry or meta-layer cryptographically associated with, but logically distinct from, the Sealed Thought's immutable chain. Each response entry may include a timestamp, responder identifier or pseudonym, response type, and optional contextual data. The separation of the response registry from the Sealed Thought chain preserves author control over the sealed record while permitting third-party signaling.

[0108] In some embodiments, the system records the scope of information disclosed to the responder at the time the response was generated, thereby establishing that the response was produced without access to the sealed content. This recorded scope may be used to demonstrate non-disclosure of the Thought to the responder.

[0109] In certain embodiments, the responder identifier is associated with a verifiable reputation attribute, accreditation status, or role classification managed by the system, allowing responses to convey differentiated signaling value while preserving responder pseudonymity.

[0110] Recorded responses do not grant ownership, license, confidentiality obligations, or other rights in the Sealed Thought, and are recorded solely as non-binding signals associated with post-sealing awareness.

[0111] In some embodiments, recorded responses are presented in chronological or aggregated form to illustrate post-sealing activity associated with the Sealed Thought, while maintaining protection of the sealed content.

[0112] Implementation Examples and Reduction to Practice (Non-Limiting): An exemplary implementation includes a network-accessible software system comprising client interfaces and server-side processing pipelines configured to perform deterministic canonicalization, cryptographic hashing, timestamp attestation binding, custody bundle creation, immutable storage, chain management, verification, certificate generation, selective disclosure, and deterministic restoration as described herein.

[0113] In one non-limiting example, an author interacts with a web-based or native application executing on a general-purpose computing device. The application transmits a digital artifact to a processing service that canonicalizes the artifact, computes cryptographic identifiers, obtains one or more trusted timestamp attestations, assembles a custody bundle, and stores the bundle within one or more immutable custodial storage systems. A cryptographic receipt and optional evidentiary certificate are returned to the author.

[0114] In another non-limiting example, a Thought Chain is extended over time by submitting successive artifacts that reference predecessor identifiers. The system enforces append-only continuity, generates successor custody bundles, and optionally anchors derived cryptographic commitments to one or more public or consortium ledgers. Verification of existence, priority, and continuity may be performed at any time without disclosure of underlying content.

[0115] In further non-limiting examples, the system supports selective disclosure workflows, succession and escrow policies, multi-custodian redundancy, jurisdiction-specific evidentiary packaging, and restoration of sealed artifacts in bitwise-identical form. These examples illustrate practical reduction to practice using conventional computing infrastructure combined with the cryptographic protocols described herein, without limiting the scope of the claimed invention.

[0116] Exemplary Embodiments (Non-Limiting): The following embodiments are provided to illustrate representative implementations of the disclosed systems and methods. These embodiments are non-limiting and are intended to demonstrate practical applications, variations, and combinations of features described throughout the Detailed Description. Individual elements of any embodiment may be combined with elements of other embodiments, omitted, or reordered without departing from the scope of the invention.

[0117] Embodiment 1 — Genesis Thought Sealing System
In this embodiment, a system is configured to establish origination and temporal priority of a

Genesis Thought by creating a cryptographically sealed custody bundle. The process may include:

- Receiving a first digital submission representing a Genesis Thought.

- Canonicalizing the submission into a deterministic byte sequence.

- Hashing canonical bytes to produce a Genesis identifier.

- Obtaining one or more trusted timestamp attestations bound to the Genesis identifier.

- Creating a custody bundle comprising canonical data, identifier, attestations, and metadata.

- Placing the custody bundle into immutable custodial storage and issuing a cryptographic receipt.

[0118] Embodiment 2 — Chained Thought Continuation

In this embodiment, a previously sealed Genesis Thought is extended to form an append-only cryptographic Thought Chain evidencing continuity over time. The process may include:

- Receiving a subsequent Thought intended to extend a chain.

- Canonicalizing the subsequent Thought.

- Computing a successor identifier incorporating a predecessor identifier.

- Obtaining a successor timestamp attestation.

- Storing a successor custody bundle immutably to prove chronological continuity.

[0119] Embodiment 3 — Thought Receipt and Evidentiary Certificate Generation

In this embodiment, the system produces human-readable artifacts that cryptographically reflect the sealed state of a Thought without altering the underlying custody bundle. The process may include:

- Generating a human-readable evidentiary certificate including identifiers, attestations, chain identifiers, and custody references.

- Rendering the certificate digitally and/or physically; invalidating upon underlying Thought modification.

[0120] Embodiment 4 — Machine-Engraved Seal Generation

In this embodiment, cryptographic indicia derived from sealed Thought data are machine-generated and embedded into a digital artifact at the time of sealing, forming a tamper-

evident engraved or embossed seal that is cryptographically bound to the associated custody bundle. The indicia are generated dynamically from certificate data produced during the sealing process. The process may include:

- Generating tamper-evident certificate indicia algorithmically derived from sealed Thought data.

- Digitally engraving, embossing, or otherwise embedding the indicia into electronic documents, certificates, or media files in a manner that is verifiable and invalidated upon alteration.

- In certain implementations, the same machine-generated indicia may additionally be rendered onto physical artifacts including printed certificates, engraved plates, plaques, packaging, artwork, or archival media.

[0121] Embodiment 5 — Selective Disclosure and Verification

In this embodiment, cryptographic control mechanisms enable verification and disclosure of sealed Thoughts without compromising custodial integrity or author sovereignty. The process may include:

- Issuing private control references enabling verification without disclosure, controlled disclosure, chain extension, and succession management.

- Preventing custodial disclosure absent cryptographic authorization.

[0122] Embodiment 6 — Multi-Custodian Redundancy

In this embodiment, custody bundles are preserved across multiple independent custodial authorities to improve resilience and jurisdictional robustness. The process may include:

- Redundantly storing custody bundles across multiple custodial authorities.

- Cryptographically verifying consistency across custodians for jurisdiction resilience.

[0123] Embodiment 7 — Human–AI Origination Boundary (Declared and/or Authenticated Context)

In this embodiment, origination context is preserved to distinguish human cognitive events from machine-generated or assisted artifacts without requiring semantic evaluation. The process may include:

- Associating Genesis sealing with authenticated human authorship context and/or declared provenance metadata when AI assistance may be present.

- Preserving human origination integrity without requiring publication.

[0124] Embodiment 8 — Long-Horizon Intellectual Legacy Chains

In this embodiment, Thought Chains are preserved over extended temporal horizons to support continuity across individuals, organizations, or generations. The process may include:

- Maintaining Thought chains across decades, generations, or organizations.

- Supporting inheritance, escrow, archival custody, and civilizational knowledge preservation.

[0125] Embodiment 9 — Jurisdictional Evidentiary Interfaces

In this embodiment, custody bundles are exported into formats compatible with legal, regulatory, and adjudicative systems while preserving cryptographic integrity. The process may include:

- Exporting custody bundles into jurisdiction-specific evidentiary formats compatible with courts, patent offices, regulators, and discovery systems.

- Preserving cryptographic integrity and chain proofs.

[0126] Embodiment 10 — Private Economic and Licensing Layers

In this embodiment, economic and licensing functionality is layered atop the custodial system without compromising neutrality or author control. The process may include:

- Layering licensing, escrow, brokerage, disclosure notarization, and monetization services atop Proof-of-Thought while remaining subordinate to custodial neutrality and author sovereignty.

[0127] Embodiment 11 — User-Defined Semantic Labeling and Chain Nomenclature

In this embodiment, non-authoritative semantic labels are associated with Thoughts to improve human interpretability without affecting cryptographic integrity. The process may include:

- Receiving, from an originating author, one or more user-defined semantic labels associated with a Genesis Thought, individual Thoughts, or the Thought Chain as a whole.

- Binding the user-defined labels to the corresponding custody bundle as non-authoritative descriptive metadata that does not affect canonicalization, hash computation, timestamp attestation, or chain integrity.

- Permitting independent customization of labels for a Genesis Thought and for successor Thoughts to reflect evolving semantic interpretation, narrative structure, project organization, or creative intent.

- Preserving label history immutably such that changes to labels are recorded as successive metadata states without modifying sealed content bytes or cryptographic identifiers.

- Rendering user-defined labels in user interfaces, evidentiary certificates, receipts, previews, or visualizations to improve human interpretability while maintaining cryptographic verifiability.

[0128] Mathematical Formalization of Canonicalization, Hashing, and Chaining

[0129] In certain embodiments, the cryptographic operations described herein may be expressed formally to illustrate deterministic behavior of the disclosed system, without limiting the scope of the invention to any particular algorithm, cryptographic primitive, or mathematical representation.

[0130] Let C_i denote the deterministic canonical byte sequence produced from a submitted Thought T_i by a canonicalization function $\mathcal{K}(\cdot)$, such that:

$$C\_i = \mathcal{K}(T\_i)$$

[0131] wherein the canonicalization function $\mathcal{K}$ is configured to be invariant under non-semantic differences including, without limitation, formatting variations, encoding differences, metadata ordering, containerization, or platform-specific representation, such that semantically identical artifacts yield identical canonical byte sequences.

[0132] Let $H(\cdot)$ denote a secure cryptographic hash function exhibiting collision resistance and an avalanche property. A Genesis Thought identifier ID_0 is computed as:

$$ID_0 = H(C_0 \| TS_0)$$

[0133] wherein TS_0 represents one or more trusted timestamp attestations cryptographically bound to the canonical byte sequence C_0, such that alteration of the canonical bytes or timestamp data invalidates the identifier.

[0134] For each successor Thought T_n in a Thought Chain, a successor identifier ID_n is computed by incorporating at least one predecessor reference, for example:

$$ID_n = H(C_n \| ID_{n-1} \| TS_n)$$

[0135] wherein ID_{n-1} is the identifier of an immediate predecessor Thought and TS_n is a trusted timestamp attestation associated with the successor Thought T_n.

[0136] Due to the avalanche property of secure cryptographic hash functions, any bit-level modification to C_{n-1}, TS_{n-1}, or any earlier predecessor propagates forward, thereby invalidating all successor identifiers ID_n for $n > 0$. This property enforces append-only continuity and irreversible chronological ordering of Thoughts on a machine-enforced basis.

[0137] In embodiments supporting branching, multiple successor identifiers may reference a common predecessor identifier while remaining independently verifiable. Each branch preserves cryptographic lineage to the shared predecessor while allowing independent continuation and evolution of Thought Chains.

[0138] All identifiers remain verifiable by recomputation using disclosed canonical bytes, timestamp attestations, and predecessor references, without reliance on custodial discretion or subjective interpretation.

[0139] This formalization illustrates, without limitation, how canonicalization, cryptographic hashing, timestamp binding, and chaining collectively enforce determinism, immutability, and continuity of sealed Thoughts across time.

Attorney Docket No. 19842-015USU1

CLAIMS

1. A computer-implemented method for establishing provable origination and temporal continuity of a human cognitive artifact, comprising:

(a) receiving, by a processing system, a digital artifact representing a human cognitive event;

(b) deterministically canonicalizing the digital artifact into a stable canonical byte representation that is invariant to formatting, encoding, metadata ordering, or platform-specific representation, without evaluating or interpreting semantic content of the digital artifact;

(c) computing a cryptographic hash value over at least the canonical byte representation using a secure one-way hash function exhibiting an avalanche property;

(d) obtaining at least one trusted timestamp attestation that is cryptographically bound to the cryptographic hash value;

(e) creating a custody bundle comprising at least the canonical byte representation, the cryptographic hash value, and the trusted timestamp attestation;

(f) storing the custody bundle in an immutable custodial storage system configured to prevent alteration, substitution, or retroactive modification of the custody bundle after creation; and

(g) issuing, to an originating human author, a cryptographic control reference implemented by cryptographic key material or capability tokens that is technically enforced by the processing system and that governs at least one of continuation, verification, selective disclosure, restoration, delegation, escrow, succession, or revocation with respect to the custody bundle, wherein the method establishes origination and temporal priority of the digital artifact on a machine-enforced basis independent of publication, institutional trust, or human discretionary judgment, and wherein anchoring a cryptographic commitment derived from the custody bundle to a public or consortium ledger is optional and not required to establish said origination or temporal continuity.

2. The method of claim 1, wherein transforming the first digital artifact into the deterministic canonical byte representation comprises normalizing at least one of encoding format, line endings, metadata ordering, container structure, compression headers, or non-semantic formatting differences, such that semantically identical artifacts yield identical canonical byte representations.

3. The method of claim 1, wherein the processing system does not evaluate, infer, classify, or interpret semantic meaning of the digital artifact and operates exclusively on the deterministic canonical byte representation and associated cryptographic metadata.

4. The method of claim 1, wherein generating the first cryptographic hash value comprises applying a one-way cryptographic hash function exhibiting collision resistance and an avalanche property such that any bit-level alteration of the canonical byte representation produces a different hash value.

5. The method of claim 1, wherein obtaining the trusted timestamp attestation comprises receiving a cryptographically verifiable time assertion from at least one independent time source selected from a trusted timestamping authority, public time service, consortium-operated service, or secure time beacon.

6. The method of claim 5, further comprising binding a plurality of independent trusted timestamp attestations to the first cryptographic hash value to improve resilience against single-source compromise, failure, or dispute.

7. The method of claim 1, wherein the custody bundle further comprises one or more cryptographic proofs selected from a Merkle proof, a digital signature, or a zero-knowledge proof sufficient to enable third-party verification of integrity, temporal priority, and custody preservation without disclosure of the underlying digital artifact.

8. The method of claim 1, wherein storing the first custody bundle comprises writing the custody bundle to an append-only or write-once storage system configured to prevent alteration, substitution, or retroactive modification after sealing.

9. The method of claim 8, wherein the immutable custodial storage system utilizes a zero-knowledge encryption architecture or client-side encryption architecture that technically precludes custodial access, training, profiling, monetization, or derivation of secondary value from the canonical byte representation absent possession of valid cryptographic control authority.

10. The method of claim 1, further comprising receiving a subsequent digital artifact; canonicalizing the subsequent digital artifact into a subsequent deterministic canonical byte representation; generating a successor cryptographic hash value incorporating the first cryptographic hash value; and immutably storing a successor custody bundle, thereby forming an append-only cryptographic chain.

11. The method of claim 10, wherein multiple successor custody bundles reference a common predecessor custody bundle to represent branching cognitive lineages.

12. The method of claim 1, wherein the cryptographic control reference enables verification of existence, integrity, or temporal priority of the first custody bundle by a third party without disclosure of the canonical byte representation.

13. The method of claim 12, wherein continuation of a Thought chain, selective disclosure, restoration, delegation, revocation, escrow, or succession is governed by cryptographic key management logic that is machine-enforced and not dependent on discretionary human decision-making.

14. The method of claim 1, further comprising redundantly storing the first custody bundle across a plurality of independent custodial authorities and performing cryptographic consistency verification across the custodial authorities.

15. The method of claim 1, further comprising restoring a bitwise-identical binary instance of the canonical byte representation from custodial storage and verifying integrity using the first cryptographic hash value.

16. The method of claim 15, further comprising assembling the restored canonical byte representation together with cryptographic identifiers, timestamp attestations, and chain references into a verifiable serialization format or structured container suitable for independent evidentiary validation.

17. The method of claim 1, further comprising associating the first custody bundle with declared provenance metadata indicating an origination classification selected from human-originated, assisted, mixed-origin, machine-generated, or unknown.

18. The method of claim 1, further comprising: recording, by the system, a third-party response indicating awareness of the existence of a Sealed Thought, wherein the response is generated based solely on non-revealing metadata associated with the Sealed Thought and without access to the canonical byte representation.

19. The method of claim 1, further comprising: recording, by the system, a disclosure scope associated with the third-party response, the disclosure scope specifying the information made available to the third party at the time the response was generated, thereby establishing that the response was produced without disclosure of the sealed content of the Sealed Thought.

20. The method of claim 1, wherein third-party responses are recorded as append-only entries in a signaling registry that is cryptographically linked to, but logically distinct from, a custody chain of the Sealed Thought.

21. The method of claim 1, wherein the third-party response comprises a response type selected from acknowledgment of awareness, valuation signal, interest indication, time-bound interest, or conditional valuation.

22. The method of claim 1, wherein the third-party response is associated with a responder identifier that is pseudonymous yet verifiably linked to a reputation score, accreditation status, or prior activity record maintained by the system.

23. The method of claim 1, wherein each recorded disclosure event is represented as a cryptographic node linked to a prior disclosure event, thereby forming a disclosure chain that is independently verifiable and logically distinct from a custody chain associated with the sealed Thought.

24. A cryptographic provenance system for establishing provable origination and temporal continuity of a human cognitive artifact, comprising:

a) one or more processing modules configured to receive a first digital artifact representing a human cognitive event, without evaluating or interpreting semantic content of the artifact;

b) a canonicalization module configured to transform the first digital artifact into a deterministic canonical byte representation invariant to formatting, encoding, metadata ordering, or platform-specific representation;

c) a cryptographic hashing module configured to generate a first cryptographic hash value from the canonical byte representation, wherein the hash function exhibits an avalanche property such that any bit-level modification to the canonical byte representation produces a materially different hash value;

d) a timestamp attestation interface configured to obtain at least one trusted timestamp attestation cryptographically bound to the first cryptographic hash value;

e) a custody bundle assembly module configured to generate a first custody bundle comprising at least the canonical byte representation, the first cryptographic hash value, and the at least one trusted timestamp attestation;

f) an immutable custodial storage system configured to store the first custody bundle under write-once or append-only semantics that prevent alteration, substitution, or retroactive rewriting; and

g) a cryptographic control module configured to issue a control reference associated with the first custody bundle, wherein access, disclosure, verification, continuation, restoration, delegation, revocation, escrow, or succession of the custody bundle is technically enforced by cryptographic authorization rather than discretionary human decision-making, wherein the system establishes provable origination, temporal priority, and evidentiary integrity of the human cognitive artifact on a machine-enforced basis.

25. The system of claim 24, further comprising: a signaling registry module configured to record third-party responses associated with a Sealed Thought, and a verification engine configured to enforce read-access controls based on a recorded disclosure scope, wherein the verification engine ensures that said third-party responses are generated without accessing the canonical byte representation of the Sealed Thought.

26. The system of claim 24, wherein the signaling registry module is configured to record third-party responses as append-only entries in a signaling registry that is cryptographically linked to, but logically distinct from, a custody chain associated with the Sealed Thought.

27. The system of claim 24, wherein the signaling registry module is further configured to represent each recorded disclosure event as a cryptographic node linked to a prior disclosure event, thereby forming a disclosure chain that is independently verifiable and logically distinct from a custody chain associated with the Sealed Thought.

28. The system of claim 27, wherein the verification engine is configured to validate third-party responses by reference to the disclosure chain, thereby confirming that the responses were generated without access to the canonical byte representation of the Sealed Thought.

29. A non-transitory computer-readable medium storing instructions that, when executed by one or more processors of a computing system, cause the computing system to perform operations for establishing provable origination and temporal continuity of a human cognitive artifact, the operations comprising:
a) receiving a first digital artifact representing a human cognitive event, without evaluating or interpreting semantic content of the artifact;
b) transforming the first digital artifact into a deterministic canonical byte representation invariant to formatting, encoding, metadata ordering, or platform-specific representation;
c) generating a first cryptographic hash value from the canonical byte representation, wherein the hash value exhibits an avalanche property such that any bit-level modification to the canonical byte representation produces a materially different hash value;
d) obtaining at least one trusted timestamp attestation cryptographically bound to the first cryptographic hash value;
e) generating a first custody bundle comprising at least the canonical byte representation, the first cryptographic hash value, and the at least one trusted timestamp attestation;
f) storing the first custody bundle in an immutable custodial storage system that prevents alteration, substitution, or retroactive rewriting; and
g) issuing a cryptographic control reference associated with the first custody bundle, wherein continuation, disclosure, verification, restoration, delegation, revocation, escrow, or

succession of the custody bundle is technically enforced by cryptographic authorization rather than discretionary human decision-making;

whereby execution of the instructions causes the computing system to establish machine-verifiable origination, temporal priority, and evidentiary integrity of the human cognitive artifact.

30. The non-transitory computer-readable medium of claim 29, the operations further comprising: recording, by the system, a third-party response indicating awareness of the existence of a Sealed Thought, wherein the response is generated based solely on non-revealing metadata associated with the Sealed Thought and without access to the canonical byte representation.

ABSTRACT

Systems, methods, and computer-readable media are disclosed for establishing cryptographically provable origination, custody, and temporal continuity of digital artifacts representing human cognitive events. A submitted digital artifact is deterministically transformed into a canonical byte representation without evaluating or interpreting semantic content, and a cryptographic identifier is generated exhibiting tamper-evident properties. One or more trusted timestamp attestations are cryptographically bound to the identifier, and a custody bundle comprising the canonical data, identifiers, and attestations is immutably preserved under technically enforced access control. Successive artifacts may incorporate predecessor identifiers to form an append-only cryptographic chain evidencing chronological continuity. Cryptographic commitments derived from custody bundles may optionally be anchored to one or more public or consortium ledgers for independent temporal verification without disclosure of underlying content. The disclosed architecture provides a machine-enforced mechanism for establishing verifiable provenance and priority of human-originated digital records in environments containing synthetic or machine-generated bitstreams.

Attorney Docket No. 19842-015USU1