

PROVISIONAL PATENT APPLICATION DRAFT

Title of the Invention: SYSTEM AND METHOD FOR IMMUTABLE PERSONAL DIGITAL DIARY WITH AUTOMATED SIZE-BASED CERTIFIED DOWNLOADS FOR LEGAL EVIDENCE USING INTEGRATED CRYPTOGRAPHIC HASHING, QUALIFIED TIMESTAMPING, AND MULTI-LEDGER BLOCKCHAIN ANCHORING

Inventor: Aerospace, Boston, Massachusetts, United States

Cross-Reference to Related Applications: None. This provisional application claims no benefit of earlier filings.

Field of the Invention The present invention relates to digital record-keeping systems, specifically to a consumer-accessible immutable personal diary platform that automatically generates court-admissible, self-verifying certified exports of text, images, videos, and recordings for patent evidence, litigation support, and CYA (Cover Your Ass) purposes through a novel integration of cryptographic hashing, accredited time-stamping authorities (TSA), and public blockchain anchoring.

Background of the Invention Traditional digital journaling applications (e.g., Day One, Notion) permit post-save edits and deletions, rendering them inadmissible as reliable evidence under Federal Rules of Evidence 803(6) (business records) or for USPTO patent priority (35 U.S.C. § 102). Enterprise Electronic Lab Notebooks (ELNs) provide audit trails but are prohibitively expensive and complex for individual inventors or professionals. Standalone blockchain timestamping services require manual per-file processing and lack an integrated diary interface. Remote Online Notarization (RON) platforms charge high per-document fees without ongoing immutable journaling.

No existing system combines (1) automatic locking of daily diary entries upon save, (2) seamless media uploads, and (3) automated, size-based certified downloads that embed SHA-256 hashes, RFC3161 TSA timestamps, and multi-ledger blockchain anchors into a single PDF/A bundle with QR-code verification. This gap leaves inventors without affordable, user-friendly tools for provable conception dates or litigation-ready records. The present invention solves these technical problems by providing a specific, improved computer-implemented workflow that enhances data integrity, verification speed, and chain-of-custody reliability in a freemium consumer application.

Summary of the Invention The invention provides a system and method wherein a user creates daily diary entries that are permanently locked (no edits/deletes) upon save. Any uploaded media is automatically processed through a certification engine that: (a) computes a cryptographic hash, (b) obtains a qualified TSA timestamp, (c) anchors the hash-timestamp pair to one or more public blockchains, and (d) generates a downloadable PDF/A bundle with embedded audit trail and self-verifying QR code. Downloads are priced by file size/type (text/pages, images/MB, videos/GB) plus a flat certification fee, enabling scalable monetization while ensuring legal permanence.

Technical improvements include: reduced verification latency via batched multi-ledger anchoring; enhanced tamper-resistance through chained diary-blockchain references; and consumer-scale usability for patent notebooks without enterprise overhead.

Brief Description of the Drawings (Figures may be added upon non-provisional conversion; described textually here for provisional sufficiency.)

Fig. 1: High-level system architecture diagram showing User Device → JournaLock Server (Hashing/TSA/Blockchain Module) → Certified Export Bundle.

Fig. 2: Flowchart of the immutable entry creation and certified download process.

Detailed Description of the Invention The JournaLock platform operates on web/mobile clients communicating with secure cloud servers (e.g., AWS or equivalent with SOC-2 compliance).

Embodiment 1 (Preferred – Core Method):

1. User authenticates and creates a daily entry via a text editor or voice-to-text interface.
2. Upon “Save & Lock” command, the entry is hashed (SHA-256), timestamped via accredited TSA (RFC3161), and anchored to Bitcoin and Ethereum ledgers (or equivalent). The entry is written to an immutable database (append-only ledger).
3. User uploads supporting files (images, videos, documents). Each file is independently hashed and linked to the diary entry’s hash.
4. When user requests a certified download:
 - System bundles selected content.
 - Computes aggregate Merkle-tree root hash.
 - Requests fresh TSA timestamp.
 - Anchors to blockchain (multi-ledger for redundancy).
 - Generates PDF/A-3 with embedded XMP metadata, audit log, and QR code linking to public verification endpoint.
 - Applies size-based pricing (e.g., \$0.10/page text; \$0.50/MB image; \$2.00/GB video) + \$9.99 certification.

This process improves the technical functioning of digital evidence systems by automating what was previously manual, error-prone notary or ELN workflows, reducing chain-of-custody breaks, and enabling real-time public verifiability.

Embodiment 2 (Freemium Variant): Basic diary access is free with limited downloads; premium unlocks unlimited size-based certified exports and higher storage tiers.

Embodiment 3 (Enterprise Extension): Team accounts with shared immutable ledgers and role-based access controls, still preserving individual entry immutability.

Embodiment 4 (Alternative Anchoring): Single-ledger (Bitcoin only) or private permissioned blockchain for regulated industries, with fallback to public anchors.

Best Mode: The preferred implementation uses SHA-256 for hashing, GlobalSign or equivalent TSA, and public blockchains to maximize admissibility and minimize cost. All data is encrypted at rest (AES-256) and in transit (TLS 1.3).

How the Invention Addresses Prior Art Limitations: Unlike generic timestamping (e.g., OriginStamp) or ELNs (e.g., Benchling), the invention integrates the diary UI directly with the certification engine, providing automatic locking and consumer pricing models never before combined in this manner.

Claims (Optional but Included for Clarity – Not Required for Provisional):

1. A computer-implemented method for creating and certifying immutable digital records comprising: receiving a diary entry; permanently locking the entry upon save; computing a cryptographic hash; obtaining a qualified timestamp; anchoring the hash-timestamp pair to at least one blockchain; and generating a size-priced certified export bundle with embedded verification metadata.
2. The method of claim 1 wherein the export bundle is a PDF/A file containing the original content, audit trail, and QR code for independent blockchain verification. (Additional dependent claims may be expanded in non-provisional filing.)