Independent Submission
Internet-Draft
Intended status: Informational
Expires: 22 September 2026

L. Reilly
Individual Author

22 March 2026

First Triple-Fingerprint Multi-Layer Permanence Record Under the Reilly EternaMark (REM) Protocol

draft-reilly-rem-triple-fingerprint-00

Abstract

This document records and formally attests the first cryptographic permanence record produced by a live implementation of the Reilly EternaMark (REM) Protocol [DRAFT-REM] that simultaneously generates SHA-256 [RFC6234], SHA3-512 [FIPS202], and BLAKE3 [BLAKE3SPEC] fingerprints for a single submitted artifact, and anchors those fingerprints across six independent permanence layers: Bitcoin blockchain timestamping via OpenTimestamps [OTS], IPFS [IPFS] distributed storage via Pinata, Zenodo DOI registration [ZENODO], Internet Archive Wayback Machine submission [IA], a persistent SQLite database layer, and a resolvable REMID permanent identifier [DRAFT-REM].

This record constitutes what the author believes to be the first document in history to be simultaneously anchored with SHA-256, SHA3-512, and BLAKE3 under a single open IETF-documented protocol specification with a live running implementation.

The SHA3-512 component of this record provides 256-bit post-quantum security against Grover’s algorithm [GROVER], exceeding the NIST post-quantum security threshold [NISTPQC].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at https://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

This Internet-Draft will expire on 22 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The Reilly EternaMark (REM) Protocol [DRAFT-REM] defines a specification for Multi-Layer Permanence -- a cryptographic permanence architecture combining simultaneous hash fingerprinting, Bitcoin blockchain timestamping, decentralized storage, academic DOI registration, and web archiving into a single automated pipeline governed by an open IETF-documented standard.

On 22 March 2026 at 17:53:04 UTC, the first live implementation of the REM Protocol at:

https://rem-protocol-agent-production.up.railway.app/

received a document submission and produced what is believed to be the first triple-fingerprint permanence record in history -- a single document simultaneously anchored with SHA-256 [RFC6234], SHA3-512 [FIPS202], and BLAKE3 [BLAKE3SPEC] fingerprints across six independent permanence layers.

This Internet-Draft formally attests that record, provides the complete cryptographic fingerprints, permanence layer attestations, and verification endpoints, and documents the post-quantum security properties of the triple-fingerprint architecture.

The attested artifact is titled:

"First Triple-Fingerprint Permanence Record -- REM Protocol"

authored by Lawrence John Reilly Jr., originator of the REM Protocol and the concept of Multi-Layer Permanence.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals.

Multi-Layer Permanence:
: The REM Protocol architecture combining cryptographic hashing, Bitcoin timestamping, IPFS storage, DOI registration, and web archiving into a unified permanence pipeline under a single IETF-documented protocol specification.

Triple-Fingerprint Record:
: A permanence record carrying simultaneous SHA-256, SHA3-512, and BLAKE3 cryptographic fingerprints of the same artifact.

REMID:
: A permanent resolvable identifier issued by the REM Protocol following the format REMID:YYYY.MMDD/[sha256-prefix].

OTS Proof:
: An OpenTimestamps [OTS] proof file anchoring a hash to the Bitcoin blockchain via calendar server Merkle aggregation.

3. Triple-Fingerprint Architecture

The REM Protocol’s Agent 1 (Hasher) generates three independent cryptographic fingerprints for every submitted artifact before any other agent in the pipeline activates. This section describes each algorithm and its role in the architecture.

3.1. SHA-256

SHA-256 [RFC6234] is a member of the SHA-2 family, standardized by NIST in FIPS 180-4 [FIPS180]. It produces a 256-bit digest and serves as the foundation of the Bitcoin proof-of-work mechanism [BITCOIN]. Its inclusion in the REM Protocol provides:

- Maximum institutional credibility -- SHA-256 is the most widely recognized and legally cited hash algorithm globally.
- Bitcoin-native compatibility -- the SHA-256 fingerprint directly connects each REM record to Bitcoin’s security model.
- Legal framework alignment -- SHA-256 is recognized under the US ESIGN Act [ESIGN], UETA [UETA], and EU eIDAS regulation [EIDAS].

3.2. SHA3-512

SHA3-512 [FIPS202] is a member of the SHA-3 family, standardized by NIST in 2015. It uses a Keccak sponge construction that is mathematically independent from the Merkle-Damgard construction used by SHA-256. Its inclusion provides:

- Algorithmic independence -- a cryptanalytic breakthrough affecting SHA-256 would not affect SHA3-512 and vice versa.
- Post-quantum resilience -- at 512-bit output, SHA3-512 provides

256-bit security against Grover's algorithm [GROVER], exceeding the NIST post-quantum minimum threshold [NISTPQC].

- NIST standardization -- SHA3-512 satisfies US federal post-2015 cryptographic requirements.

3.3. BLAKE3

BLAKE3 [BLAKE3SPEC] is a modern cryptographic hash function released in January 2020. It is based on a binary tree structure enabling practically unlimited parallelism. Its inclusion provides:

- Performance at scale -- BLAKE3 is 4-10x faster than SHA-256 in software, enabling high-throughput enterprise deployments.
- Modern cryptographic design -- BLAKE3 represents the current state of the art in hash function design.
- Architectural diversity -- three structurally independent algorithms defeat any single algorithmic attack vector.

3.4. Post-Quantum Resilience Analysis

Quantum computers attack hash functions via Grover's algorithm [GROVER], which provides a quadratic speedup reducing effective security bits by half. The triple-fingerprint architecture provides layered post-quantum resilience:

Algorithm	Output	Classical Security	Quantum Security
SHA-256	256 bits	128 bits	128 bits (min)
SHA3-512	512 bits	256 bits	256 bits (SAFE)
BLAKE3	256 bits	128 bits	128 bits (min)

SHA3-512's 256-bit quantum security exceeds the NIST post-quantum security minimum threshold of 128 bits by a factor of two [NISTPQC].

All three algorithms would require simultaneous defeat for a REM record to be cryptographically compromised. Given the structural independence of SHA-256 (Merkle-Damgard), SHA3-512 (Keccak sponge), and BLAKE3 (binary tree), simultaneous defeat is considered practically impossible under any foreseeable classical or quantum adversarial model.

4. Multi-Layer Permanence Stack

The REM Protocol pipeline processes each submission through seven independent agents. Six produce external permanence attestations.

4.1. Layer 1: Cryptographic Hash Integrity

Agent 1 (Hasher) generates SHA-256, SHA3-512, and BLAKE3 fingerprints simultaneously before any network activity occurs. All subsequent permanence layers anchor records bound to these fingerprints, ensuring end-to-end cryptographic integrity.

4.2. Layer 2: Bitcoin Blockchain Timestamp

Agent 2 (Bitcoin) submits the SHA-256 fingerprint to three independent OpenTimestamps [OTS] calendar servers:

- alice.btc.calendar.opentimestamps.org
- bob.btc.calendar.opentimestamps.org
- finney.calendar.eternitywall.com

Each calendar aggregates submissions into a Merkle tree and commits

the root to the Bitcoin blockchain in a single transaction. The resulting OTS proof file provides independent third-party cryptographic proof that the document existed at the submitted timestamp, verifiable against the Bitcoin blockchain by any party without trusting the REM Protocol infrastructure.

The timestamp moment is captured at submission time and cannot be altered regardless of Bitcoin block confirmation timing. Confirmation provides the final cryptographic seal via Agent 7 (OTS Watcher), which polls calendar servers every ten minutes and auto-upgrades the OTS proof upon block confirmation.

4.3. Layer 3: REMID Permanent Identifier

Agent 3 (REMID) issues a permanent resolvable identifier following the REMID namespace defined in [DRAFT-REM]:

```
REMID:YYYY.MMDD/[first-8-hex-chars-of-sha256]
```

The REMID resolves to a live verification page displaying all permanence layer statuses, the complete citation record, and file verification functionality. The REMID is permanently bound to the SHA-256, SHA3-512, and BLAKE3 fingerprints of the artifact.

4.4. Layer 4: IPFS Distributed Storage

Agent 4 (IPFS) pins the artifact to two independent Pinata [PINATA] IPFS providers, generating a content-addressed CID. The artifact is retrievable by any IPFS node globally using the CID alone, without dependence on the REM Protocol infrastructure.

4.5. Layer 5: Internet Archive

Agent 5 (Archive) submits three URLs to the Internet Archive Wayback Machine [IA] Save API. Wayback Machine archival provides a third independent web-based permanence layer, operated by a nonprofit institution with a documented 30-year preservation mandate.

4.6. Layer 6: Academic DOI Registration

Agent 5.5 (Zenodo) publishes the artifact to Zenodo [ZENODO] and registers a Digital Object Identifier (DOI) via DataCite [DATACITE]. The DOI provides academic-grade permanent citation infrastructure recognized by scholarly publishers, institutions, and intellectual property frameworks globally.

5. The Attested Record

This section provides the complete, verifiable attestation of the first triple-fingerprint multi-layer permanence record produced by the REM Protocol implementation.

5.1. Artifact Metadata

Title:	First Triple-Fingerprint Permanence Record -- REM Protocol
Author:	Lawrence Reilly
Description:	The first document in history anchored with SHA-256, SHA3-512, and BLAKE3 simultaneously under a single open IETF protocol. Authored by Lawrence Reilly, originator of the REM Protocol and Multi-Layer Permanence.
Filename:	First_Triple_Hash_Permanence_Record_2026.docx
Byte Length:	11,489 bytes
REM Version:	1.1
Record ID:	08f11667-2128-4032-b8a1-3eb0e3752792
Issued:	2026-03-22T17:53:04.880923 UTC

Protocol: draft-reilly-rem-protocol-01

5.2. Cryptographic Fingerprints

The following fingerprints were generated simultaneously by Agent 1 (Hasher) at 2026-03-22T17:53:04 UTC. Any party may independently verify these fingerprints by hashing the original artifact file using the respective algorithms.

SHA-256:
29c75b03969a9a8138214f06dcd3d6edd7cfddb3a358031ef614239764127746

SHA3-512:
5794acd3b0330c343839330ad6a4ca2dec1e9bac3709c3f1d501d706c18f2cc
7e7e3946dfe6c440faac5e7e6c3edee21c5d0a6e75ef8e322e399e30729589d06

BLAKE3:
6f7bf278ef5e72ae9746eb8b4e051358eec79442fdd40ab44c44914f30d65015

5.3. Permanence Layer Attestations

REMID:
REMID:2026.0322/29c75b03

REMID Resolver:
https://rem-protocol-agent-production.up.railway.app/id/REMID%3A2026.0322%2F29c75b03

Zenodo DOI:
10.5281/zenodo.19164261

Zenodo Concept DOI:
10.5281/zenodo.19164260

Zenodo Record:
https://zenodo.org/records/19164261

IPFS CID:
bafkreibjy5nqhfu2tkatqikpa3onhvxn27h53m5dlabr55queolwietxiy

IPFS Gateway:
https://gateway.pinata.cloud/ipfs/bafkreibjy5nqhfu2tkatqikpa3onhvxn27h53m5dlabr55queolwietxiy

IPFS JSON CID:
bafkreif2sa43imr25dnwemrab4qllhe3sbi6y5jpdjje5jeywc5osagunq

Bitcoin OTS Submission:
2026-03-22T17:53:05.961535 UTC
Submitted to 3/3 calendars: alice, bob, finney

Bitcoin OTS Calendar Receipts:

Alice (alice.btc.calendar.opentimestamps.org):
8AiojVe4Z8x4FgjwEPucZ5Y6e1+Yf9SE+RTZvYoI8SCCvayBVJqYwat+IuqbZX
YIf5A28N/f93dntXwEhTCtjQjwIBNJ4EtoidPp6zUXitJIATMJkxONHLCBmGuh
ImbNnumQCPEEacAsgfAI7xCrisOMc98Ag9/jDS75DI4uLWh0dHBzOi8vYWxpY2
UuYnRjLmNhbGVuZGFyLm9wZW50aW1lc3RhbXBzLm9yZw==

Bob (bob.btc.calendar.opentimestamps.org):
8AiNamgw4DOyBwjwEOaukBbUF6vX3coh5PEaOhQI8SCswCZ3nBBLR1FxnQiINq
nh8sIekvQRk02656XwoaHI3gjxBGnALIHwCJrk/dCpffIHAIPf4w0u+QyOLCto
dHRwczovL2JvYi5idGMuY2FsZW5kYXIub3BlbnRpbWVzdGFtcHMub3Jn

Finney (finney.calendar.eternitywall.com):
8BBWDZEZhXxRrz6rJ7Xjdh2lCPEg7itfqtO8AZP2MgISES25yhOCzusGLSFe9

So40tKHhuII8SDhVp8IPXZZYUDBhFtMB0IoLpQXySEthUZaz+HOB8/nugjxBGn
ALIHwCAzKcbKlFSc2AIPf4w0u+QyOKShodHRwczovL2Zpbm5leS5jYWxlbmRh
ci5ldGVybml0eXdhbGwuY29t

Internet Archive:
Submitted 3 URLs to Wayback Machine Save API
Search: https://web.archive.org/web/*/https://rem-protocol-agent-production.up.railway.app/id/REMID%3A2026.0322%2F29c75b03

5.4. Machine-Readable Record

The complete REM Record in JSON format (rem_version 1.1) is permanently available at:

https://rem-protocol-agent-production.up.railway.app/record/08f11667-2128-4032-b8a1-3eb0e3752792/json

The JSON record includes all agent outputs, receipt data, and permanence layer attestations in a machine-readable format conforming to Section 6.1 of [DRAFT-REM].

6. Verification

6.1. Independent Hash Verification

Any party may independently verify the cryptographic fingerprints in Section 5.2 by:

1. Retrieving the original artifact from IPFS using the CID in Section 5.3 or from Zenodo using the DOI in Section 5.3.

2. Computing the SHA-256, SHA3-512, and BLAKE3 fingerprints of the retrieved file using any conforming implementation.

3. Comparing the computed fingerprints against those in Section 5.2.

A match confirms the artifact is cryptographically identical to the original submission and has not been altered since 2026-03-22T17:53:04 UTC.

The VERIFY BY FILE function at the live verification endpoint (Section 6.2) performs this verification automatically in the browser when the original file is provided.

6.2. Live Verification Endpoint

The REM Protocol provides a live verification page for this record:

https://rem-protocol-agent-production.up.railway.app/verify/REMID%3A2026.0322%2F29c75b03

This endpoint displays:

- Real-time permanence layer status for all six layers
- Complete cryptographic fingerprints
- Bitcoin OTS proof status and block confirmation details
- IPFS retrieval link
- Zenodo DOI and citation data
- File verification by upload
- Citation record in machine-readable format
- Downloadable Verification Certificate

The live system accepts new document submissions at:

https://rem-protocol-agent-production.up.railway.app/

7. Historical Significance

To the best of the author's knowledge and research, the record attested in Section 5 of this document represents:

1. The first document permanently anchored with SHA-256, SHA3-512, and BLAKE3 simultaneously under a single open IETF-documented protocol with a live running implementation.

2. The first open protocol permanence system to include BLAKE3 as a production hash algorithm alongside SHA-256 and SHA3-512.

3. The first IETF-documented permanence protocol to formally address post-quantum resilience through SHA3-512 inclusion as a core architectural requirement.

4. The first autonomous multi-agent permanence pipeline governed by an IETF Internet-Draft specification to achieve operational status with publicly accessible document submission.

Prior systems combining blockchain timestamping with distributed storage [IPFS] exist, most notably OpenTimestamps [OTS] and various blockchain-IPFS hybrid architectures. However, none combine triple-fingerprint hashing, academic DOI registration, web archiving, and a resolvable permanent identifier namespace under a single unified open protocol specification with a live implementation. The REM Protocol constitutes a new category of permanence infrastructure rather than an extension of prior work.

8. Security Considerations

8.1. Hash Algorithm Independence

The three hash algorithms employed -- SHA-256, SHA3-512, and BLAKE3 -- use structurally independent constructions:

- SHA-256 uses a Merkle-Damgard construction [RFC6234]
- SHA3-512 uses a Keccak sponge construction [FIPS202]
- BLAKE3 uses a binary tree construction [BLAKE3SPEC]

A cryptanalytic attack effective against one construction is extremely unlikely to be effective against either of the other two. The triple-fingerprint architecture therefore provides defense in depth against future cryptanalytic developments.

8.2. Post-Quantum Security

As analyzed in Section 3.4, SHA3-512 provides 256-bit quantum security against Grover's algorithm [GROVER], exceeding the NIST post-quantum minimum threshold [NISTPQC]. REM records produced by the live implementation are therefore post-quantum resilient through the SHA3-512 permanence layer.

Implementors SHOULD include SHA3-512 or equivalent 512-bit output hash algorithms in any REM Protocol-compliant implementation seeking post-quantum permanence guarantees.

8.3. Multi-Layer Redundancy

The six-layer permanence architecture ensures that no single point of failure can compromise a REM record. The permanent layers -- Bitcoin blockchain, IPFS, Zenodo DOI, and Internet Archive -- are operated by independent organizations on independent infrastructure. No single entity controls more than one layer. An adversary seeking to erase or alter a REM record would require simultaneous control of Bitcoin mining consensus, the global IPFS network, CERN's Zenodo

infrastructure, and the Internet Archive -- a practical impossibility.

9. IANA Considerations

This document has no IANA actions.

The REMID namespace (REMID:YYYY.MMDD/[hash-prefix]) is defined and administered by the REM Protocol specification [DRAFT-REM]. Registration of this namespace with IANA is deferred to a future revision of [DRAFT-REM].

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/rfc/rfc6234>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[FIPS180] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015, <https://doi.org/10.6028/NIST.FIPS.180-4>.

[FIPS202] National Institute of Standards and Technology, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", FIPS PUB 202, DOI 10.6028/NIST.FIPS.202, August 2015, <https://doi.org/10.6028/NIST.FIPS.202>.

[DRAFT-REM] Reilly, L., "Reilly EternaMark (REM) Protocol: Dual-Layer Digital Permanence via DOI Registration and Bitcoin-Layer Cryptographic Timestamping", Internet-Draft draft-reilly-rem-protocol-01, IETF Datatracker, 2026, <https://datatracker.ietf.org/doc/draft-reilly-rem-protocol/>.

10.2. Informative References

[BITCOIN] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", October 2008, <https://bitcoin.org/bitcoin.pdf>.

[BLAKE3SPEC] O'Connor, J., Aumasson, J-P., Neves, S., and Z. Wilcox-O'Hearn, "BLAKE3 -- one function, fast everywhere", January 2020, <https://github.com/BLAKE3-team/BLAKE3-specs/blob/master/blake3.pdf>.

[DATACITE] DataCite, "DataCite Metadata Schema Documentation for the Publication and Citation of Research Data and Other Research Outputs", Version 4.5, 2024, <https://schema.datacite.org>.

[EIDAS] European Parliament, "Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)", Official Journal of the European Union, August 2014.

[ESIGN] United States Congress, "Electronic Signatures in Global and National Commerce Act (ESIGN)", 15 U.S.C. 7001 et seq., June 2000.

[GROVER] Grover, L.K., "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp. 212-219, 1996, DOI 10.1145/237814.237866.

[IA] Internet Archive, "Wayback Machine Save API", <https://web.archive.org/save>.

[IPFS] Benet, J., "IPFS -- Content Addressed, Versioned, P2P File System", arXiv preprint arXiv:1407.3561, 2014, <https://arxiv.org/abs/1407.3561>.

[NISTPQC] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization", <https://csrc.nist.gov/projects/post-quantum-cryptography>.

[OTS] Todd, P., "OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin", 2016, <https://opentimestamps.org>.

[PINATA] Pinata, "IPFS Pinning Service", <https://pinata.cloud>.

[UETA] National Conference of Commissioners on Uniform State Laws, "Uniform Electronic Transactions Act (UETA)", 1999.

[ZENODO] European Organization for Nuclear Research and OpenAIRE, "Zenodo: Research. Shared.", 2013, <https://zenodo.org>.

Author’s Address

Lawrence John Reilly Jr.

Email: lawrencejohnreilly@gmail.com
GitHub: https://github.com/lawrencejohnreilly-creator/rem-protocol
IETF Datatracker: https://datatracker.ietf.org (search: Reilly)
Live System: https://rem-protocol-agent-production.up.railway.app/
DOI Archive: https://zenodo.org/search?q=reilly