Hardware-Anchored Media Provenance and Blockchain-Anchored Verification

Jose Luis Junior Pineda Fritas

Public Disclosure: January 13, 2026

Abstract

This document discloses a system and method for certifying the authenticity and provenance of digital media (images and video), including live streaming content, by anchoring cryptographic proofs generated at capture-time within trusted hardware to a public blockchain. The system enables third-party, trustless verification that a given photo, video, or stream originated from a physical capture device and has not been altered or manipulated.

1 Introduction

The rapid advancement of generative AI has made it increasingly difficult to distinguish authentic media captured by physical devices from synthetic or manipulated content. Traditional methods, such as watermarking, metadata verification, or AI-based detection, are often fragile, removable, or prone to false positives.

There is a need for a verifiable, device-level proof of capture that:

- Does not depend on analyzing the content itself,
- Is globally verifiable by any third party,
- Is resistant to tampering or post-processing,
- Works for both still images and live video streams.

2 Core Idea

The core concept is to bind each captured media asset to:

1. A trusted hardware identity of the capture device,
2. A cryptographic hash of the captured content,
3. A verifiable timestamp anchored to a public blockchain.

This creates an immutable, publicly verifiable record of media provenance. The economic value of the blockchain is irrelevant; only its immutability and verifiability are required.

3 System Components

3.1 Capture Device

The capture device (smartphone or high-end camera) should include:

- Secure hardware element (TEE, Secure Enclave, or TPM),
- Non-exportable private key bound to the device,
- Signed firmware and trusted capture pipeline.

3.2 Cryptographic Processing

At capture time:

1. Compute a cryptographic hash (e.g., SHA-256) of the image or video frame data.
2. Sign the hash within the secure hardware using the device's private key.

3.3 Blockchain Anchoring Layer

Only hashes and minimal metadata are written on-chain. Anchoring may occur asynchronously to avoid latency. Public blockchains or Layer-2 networks can be used for scalability.

3.4 Metadata Embedding

The signed hash and blockchain reference are embedded in media metadata. Metadata does not affect visual content and may be stripped without invalidating on-chain verification.

4 Smartphone Image and Video Capture Flow

1. User captures an image or video.
2. Device computes content hash inside trusted hardware.
3. Signed hash is anchored to the blockchain.
4. Media file includes reference to on-chain record.

Third parties can later:

- Recompute the hash,
- Verify the device signature,
- Verify blockchain inclusion.

5 Social Platform Verification

Social or media platforms may:

- Detect presence of provenance metadata,
- Verify the on-chain proof,
- Display a non-coercive visual marker, e.g., "Verified Capture Device."

Unverified content remains publishable but distinguishable.

6 Live Streaming Verification

6.1 Hash-Chain Construction

Instead of anchoring every frame:

- Each video frame hash is chained to the previous frame hash, forming a continuous hash chain.

6.2 Periodic Blockchain Anchoring

At fixed intervals (e.g., 1–5 seconds), the current hash chain is anchored to the blockchain, allowing post-hoc verification of every frame without excessive transactions.

6.3 Stream Commitment

At stream start, a commitment may be anchored defining:

- Device identity,
- Stream identifier,
- Start time,
- Hashing parameters.

7 Verification Properties

The system enables verification that:

- Media originated from a specific physical device,
- Capture occurred after a given timestamp,
- Content has not been altered or reordered,
- Live streams have not had frames inserted or removed.

8 Security Model and Limitations

8.1 Addressed Threats

- Post-processing and manipulation,
- AI-generated content falsely presented as captured,
- Metadata forgery.

8.2 Known Limitations

- Re-recording of displays or analog re-capture,
- Physical compromise of capture hardware,
- Malicious firmware prior to capture.

9 Intended Applications

- Journalism and news media,
- Social media authenticity indicators,
- Legal and forensic evidence,
- Body cameras and surveillance,
- Government and institutional broadcasting,
- High-trust live transmissions.

10 Disclosure Intent

This document is published as a defensive technical disclosure to establish prior art. The author does not waive moral authorship or attribution rights. Its intent is to prevent exclusive patent claims by third parties while enabling open discussion, standardization, and further research.