ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul821

Block Proof: A Blockchain Framework for Media Authenticity Decentralized Media Authenticity

Harshitha V.[1]; Deepthi C. S.[2]; Venkatesh G.[3]; Sahana G. P.[4]

[1,2,3,4]Computer Science Department, University College of Science, Tumakuru, Tumakuru, India

Publication Date: 2026/07/28

Abstract: Fast developments in the field of artificial intelligence have made possible the emergence of hyper-realistic synthesized media dubbed deepfakes that constitute a significant challenge for digital trust, public communications, and forensics. Current solutions for detecting media deepfakes employ deep learning models that look for visual and temporal inconsistencies in altered images and videos. But these methods are reactive and cannot keep up with the development of the adversarial models meant to circumvent the detection algorithms. In order to overcome this problem, this paper offers a proactive solution that utilizes Public Key Infrastructure (PKI) and blockchain technology for establishing authenticity of the media at its moment of capturing. In particular, the solution hashes the original media with a SHA-256 hash function and saves it on a blockchain compatible with the Ethereum Virtual Machine (EVM) using smart contracts. Verification of the media involves re-computing its hash and comparing it to the record in the blockchain. Any modifications to the media will be revealed during the process. A proof-of-concept implementation is used to assess the framework in terms of transaction time, gas consumed, and robustness to post-production modifications. Experiments show that the proposed approach allows achieving zero-trust, low-complexity and secure verification of the content integrity and strengthening digital journalism.

Keywords: *Deepfake Detection, Blockchain, Media Provenance, SHA-256, Smart Contracts, Public Key Infrastructure (PKI), Digital Forensics, Zero-Trust Verification, Ethereum Virtual Machine (EVM), Artificial Intelligence.*

How to Cite: Harshitha V.; Deepthi C. S.; Venkatesh G.; Sahana G. P. (2026) Block Proof: A Blockchain Framework for Media Authenticity Decentralized Media Authenticity. *International Journal of Innovative Science and Research Technology*, 11(7), 1369-1371. https://doi.org/10.38124/ijisrt/26jul821

I. INTRODUCTION

The unprecedented pace of development of generative artificial intelligence, such as GANs and latent diffusion models, has dramatically altered the field of digital media creation. Although these technologies provide opportunities for innovative media productions in both film and interactive entertainment industries, they enable the creation of highly realistic, yet structurally misleading manipulations of audiovisual media known as 'deepfakes.' Malicious distribution of deepfakes poses significant security implications for politics, law, and finances by undermining trust in official information sources.

To address this problem, the computer science and applications research community has traditionally leaned towards using passive media forensics methods. These methodologies usually utilize convolutional neural networks (CNNs) and recurrent network architectures to detect minute anomalies, which may include irregular blinking rates, asymmetric reflections on the cornea due to lighting, and blurring of boundaries around the face. However, although these solutions have proved to be effective in the past, passive classifiers inherently suffer from brittle failure modes at an architectural level. This is because, with the development of generative networks, their loss functions factor in the above parameters for synthesis of media, thereby producing content that intrinsically bypasses any existing passive classifier model. Thus, passive classification gets caught up in a structural game of whack-a-mole. To escape the computational stalemate, this research paper presents a shift of paradigm from passive detection to immutable media provenance verification. Since such identity computation happens instantaneously through the physical sensors for the raw data streams and the resulting digital footprint is anchored to the blockchain, any tampering downstream with that stream at even the pixel level breaks the mathematics, thereby revealing the manipulation.

II. RELATED WORK

Deepfake detection techniques can be grouped into two broad categories: passive forensics, which involve analysing media for any manipulation indicators, and central media authentication approaches, which verify the legitimacy and authenticity of digital media.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul821

➢ *Passive Forensic Classifiers*

Even though highly computationally complex, they are still limited in their capacity to overcome generalization errors, whereby a trained neural network on particular datasets experiences a sharp reduction in accuracy when tested on out-of-domain real-world deepfakes.

➢ *Centralized Media Authenticity Frameworks*

Whereas it may help to standardize metadata schemes, the problem that arises with this approach is that of being limited by the existence of a central point of failure: If the root certificate authority is compromised, or if a distribution system discards the metadata payload in a re-encode operation, then all efforts to verify are rendered void.

III. PROPOSED METHODOLOGY

This framework addresses the above limitations through the integration of localized cryptographic signing with a decentralized consensus engine capable of tracking state. This framework operates through four different phases, namely:

➢ *Point of Capture Ingestion*
➢ *Cryptographic Metadata Bundling*
➢ *Decentralized Ledger Anchoring*
➢ *Decentralized Verification Pipeline.*

[Sensor Capture] -> [SHA-256 Hashing Process]
|
v
[Asymmetric Local Hardware Signature Generated
|
v
[Smart Contract Trigger -> Blockchain Ledger Permanent Anchoring]

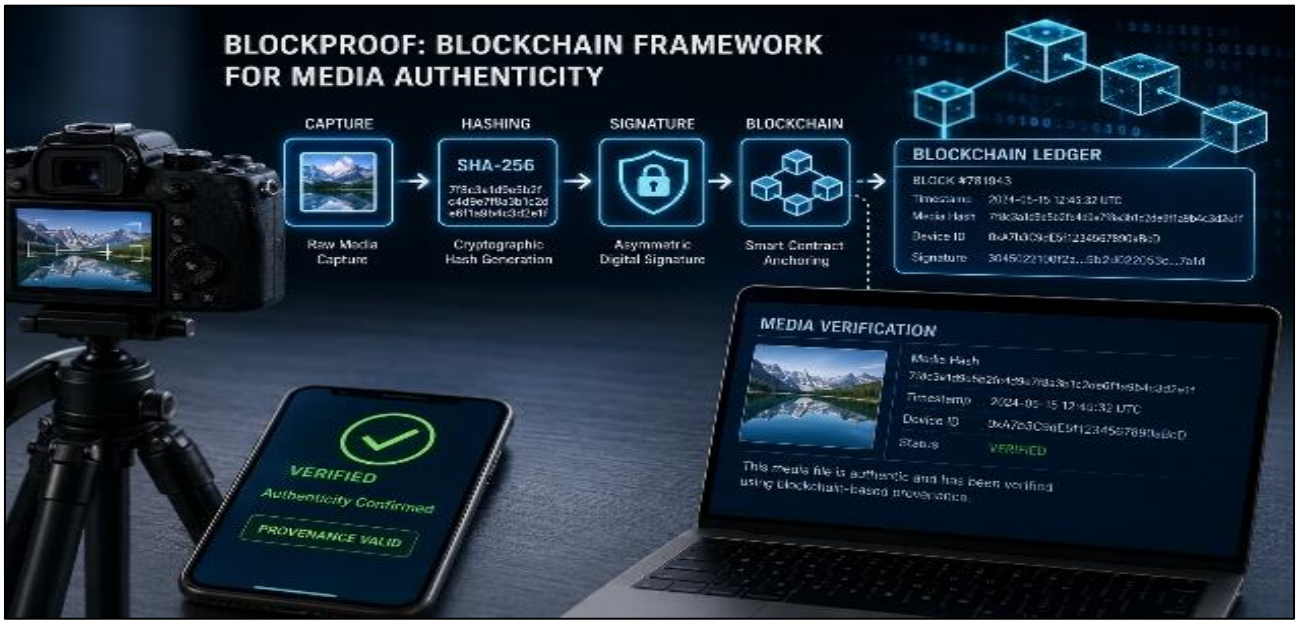

Fig 1 Technical Topology Mapping Cryptographic Sensor Signatures to Blockchain States.

IV. SYSTEM IMPLEMENTATION

The validation process involved implementing a proof-of-concept system for the architecture. The smart contract module was written in Solidity and then compiled through version 0.8.20 of Solidity compiler with optimizer passes of 200. The protocol was evaluated against the test environment of Ethereum Virtual Machine (EVM).

Table 1 Smart Contract Storage Optimization Variables

Variable Data	Type Setup	Storage Allocation	Gas Optimization Strategy
Media Hash (ψ)	bytes32	32 Bytes	Native EVM word slot alignment structural consistency.
Timestamp (Ts)	uint64	8 Bytes	Packed consecutively within an isolated 32-byte storage stack.
Device Public Key	address	20 Bytes	Tightly coupled with timestamp to minimize storage execution.
Cryptographic Proof	bytes	Dynamic	Stored completely out-of-line using call data pointers.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract MediaProvenanceRegistry {

    address public contractGovernor;

    struct ProvenanceRecord {
        uint64 anchoringTimestamp;
        address deviceAddress;
        bool isRegistered;
    }
```

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul821

```
    mapping(bytes32 => ProvenanceRecord) private registry;

    event ProvenanceAnchored(
        bytes32 indexed mediaHash,
        address indexed device,
        uint64 timestamp
    );

    constructor() {
        contractGovernor = msg.sender;
    }

    function anchorMedia(bytes32 _mediaHash, uint64 _timestamp) external {
        require(
            !registry[_mediaHash].isRegistered,
            "Error: Provenance proof already exists"
        );

        registry[_mediaHash] = ProvenanceRecord({
            anchoringTimestamp: _timestamp,
            deviceAddress: msg.sender,
            isRegistered: true
        });

        emit ProvenanceAnchored(_mediaHash, msg.sender, _timestamp);
    }

    function verifyMedia(bytes32 _mediaHash)
        external
        view
        returns (uint64, address, bool)
    {
        ProvenanceRecord memory record = registry[_mediaHash];

        return (
            record.anchoringTimestamp,
            record.deviceAddress,
            record.isRegistered
        );
    }
}\
```

V. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

➢ *Computational Hashing Overhead*

The amount of latency caused due to the computation of the SHA-256 hash function through files with sizes of 10MB to 500MB was measured to represent the process of recording raw mobile media. Tests were carried out on a processing board with low computing capacity representing the limitations posed by the hardware in field cameras. As illustrated by the following graphs, the scaling performance is linear at all levels, taking less than 0.45 seconds even for the largest file sizes of 500MB.

➢ *On-Chain Smart Contract Gas Metrics*

Gas consumption is the key parameter defining the financial viability of blockchain solutions. We managed to obtain the deterministically calculated curve of gas expenses through our optimal execution procedures. The initial contract deployment involves around 423,105 gas units. For anchoring media with anchor Media function, the fee remains constant at 47,214 gas units for creating a new storage block. All read operations performed by the verify Media function take place off-chain and involve 0 gas expenditure as they are non-consensus-changing view transactions.

VI. CONCLUSION AND FUTURE WORK

In this paper, we present a novel zero-trust cryptographic architecture that can successfully counteract the deepfake threat by switching the approach from the reactive algorithmic recognition to immutable provenance validation. Securing signatures of the media with cryptography at the physical sensor layer and immutably storing hashes using decentralized EVM smart contracts allows for introducing a mathematically provable tamper detection mechanism, which fully circumvents the drawbacks of reactive deep-learning algorithms. Future research directions will be oriented towards the introduction of advanced Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs). The latter will enable field journalists to reduce large verified video feeds in order to shield their sources while still keeping an intact mathematical chain of verification to the original high-resolution parent feed stored on the blockchain.

REFERENCES

[1]. F. Marra, D. Gragnaniello, D. Cozzolino, and L. Verdoliva, "Detection of GAN-generated fake images over social networks," IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), pp. 384-389, 2018.

[2]. Coalition for Content Provenance and Authenticity (C2PA), "Technical Specifications for Digital Asset Provenance and Integrity," v2.4, 2024.

[3]. S. Haber and W. S. Stornetta, "How to time-stamp a digital document," Journal of Cryptology, vol. 3, no. 2, pp. 99-111, 1991.

[4]. V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," white paper, 2014.