International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 5, Issue 1, 242-252, 2024
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V5I1P125

Original Article

Blockchain-Backed Content Authenticity Verification Framework

Siva Sai Krishna Suryadevara[1], Santosh Nakirikanti[2]
[1]Sr. AEM Cloud Engineer at Maganti IT Resources, USA.
[2]Principal Digital Architect at Waters Corporation, MA, USA.

Abstract - *One of the major challenges of our time is the ability to discern between real and digitally altered content, which has been exacerbated by the rapid rise of digital content, the proliferation of AI-generated media, deepfakes, and very complex identity-spoofing techniques. The traditional ways of verification are having a hard time keeping pace with the speed of falsification; hence, the need for a mechanism that ensures content integrity is massively felt. This article elaborates on a content authenticity verification scheme supported by blockchain technology that aims at re-establishing the trust of the users of the digital information ecosystems by employing the blockchain as a decentralized, tamper-proof trust anchor. The system protects the content by means of metadata hashing, distributed ledger storage, and cryptographic signature validation, which results in easy verification procedures that can detect the changes in the content or verify its legitimate source. Indeed, the framework, through a detailed case study and experimental evaluation, convincingly shows that it keeps excellent performance in ensuring non-repudiation, preventing unauthorized alterations, and enabling traceability in distributed environments. Its potential applications range across the very important domains, such as journalism that needs source verification as a matter of priority; social media platforms that want to fight against false videos and audios; legal and forensic workflows that necessitate digitally verifiable evidence; and enterprise documentation pipelines that depend on audit-ready integrity checks. The proposed solution that brings together blockchain and some lightweight cryptographic measures is a scalable and feasible one that can increase digital trust without the users having to bear a heavy operational overhead. In short, this paper is a significant step towards a more transparent and trustworthy information landscape, as it offers a strong, future-ready infrastructure for the authentication of digital content.*

Keywords - *Blockchain, Content Authenticity, Deepfake Detection, Distributed Ledger Technology, Metadata Hashing, Digital Signatures, Provenance Tracking, Zero-Knowledge Proofs, Decentralized Identity, Media Integrity Verification.*

1. Introduction

1.1. Background and Challenges

During the last 10 years, the net has changed significantly thanks to such major factors as the rise of artificial intelligence, the capability to generate multimedia, and the dissemination of content through social media. The web today isn't limited to the content created by traditional users; there's also a huge amount of synthetic media. AI-written texts, photo-realistic pictures, voices, and videos that are very close to real ones, but are still made artificially, fill the net. The instruments that used to be in facilities such as research labs and special production studios are now in the reach of ordinary people who want to create deepfakes and other forms of edited media with ease. The technological breakthroughs create a new field for artists but at the same time, they increase the number of the so-called "seeing is no longer believing" cases.

With the rise of synthetic media, it is very challenging to be sure that the news is real and not a deepfake, manipulated, or artificially created. For example, deepfake videos can show people talking or doing things that they have never done, AI-generated text can replicate one's writing style, and edited images can fool even the most advanced forensic analysis. The swift development of generative models has put us far behind when it comes to content authentication; thus, the public trust is getting lower and there are serious risks in many fields.

At the heart of the problem is the fact that most digital ecosystems rely on centralized platforms such as social networking sites, cloud services, and content repositories that do not offer strong integrity or authenticity assurances. The systems usually depend on user complaints, platform-level moderation, or proprietary detection algorithms, all of which may be biased, unreliable, or indistinct. Without transparent verification methods, evildoers can easily spread fake content among online communities with very little risk of being caught.

The risks brought with such a massive deception, which is this manipulation, are pretty much scary. One of them is the case of falsified media, which can defraud source credibility and the trust of the public in factual reporting in journalism. As

for national security, consciousness tricks can function as propaganda to mislead or to impersonate someone or as psychological operations. The digital forensic experts become more and more helpless in the face of reality of the same criminal investigation because the media is manipulated and thus difficult to detect. Banks are exposed to the risk of imposture that can be achieved by duplicating a biometric characteristic, tampering with account opening documents or credit applications, and causing fraudulent transactions to take place. Democracy, as a system, is susceptible to synthetic content that can influence people's views, elections, and, thus, political stability, just like any other system mentioned before. All these scenarios prove that there is a great need for an instant authentication system that verifies whether a piece of digital content is real or has been altered.

1.2. Problem Statement

The increasing prevalence of manipulated and entirely fabricated digital media points to a very basic need for a safe and trustworthy method of checking the source, ownership, and even the unchangeability of digital content. This method should be such that by no means can the creators lose their authorship, the consumers can confirm the genuineness, and the intermediaries cannot change the metadata or make the impersonation easy. Traditional verification techniques, which greatly rely on centralized databases or platform-based detection tools, are no longer enough for the complex media world of today.

On the other hand, putting together such a scheme raises potential objections. The ability to expand is the main question since a worldwide verification system of authenticity must be in a position to receive up to millions of daily instances of content being submitted to different platforms and across media types. At the same time, interconnection is as important as the former; verification methods should be carried out on various gadgets, software, and content structures and not be limited to a proprietor or a particular ecosystem.

There are also certain difficulties in ensuring the accuracy of metadata, as it can be removed, changed, or even made up during the process of content alteration. Apart from that, the issue of long-term memory is of paramount importance since it not only ensures that the content has been recorded as authentic but also keeps its verification entries safe from tampering and available years or decades later. None of the existing systems have been able to coincide with all these requirements at the same time.

1.3. Motivation

A combination of legal, societal, and technological factors is pushing the need for content authenticity verification to the forefront. Digital trust is being demanded by governments and regulatory bodies worldwide through their policies. Media provenance verification is the ultimate solution to these regulations focusing on deepfake disclosure, digital identity, and secure information exchange because they highlight the need for it to be systematic. These changes in demand put pressure on organizations to implement verifiable systems capable of withstanding scrutiny during audits, investigations, and compliance checks.

Additionally, enterprises have to meet growing operational demands for a trustworthy content exchange. In supply chains, financial services, healthcare, or corporate communications, documents, media files, and transactional data are expected to be not only authentic but also verifiable. Counterfeit documents, forged approvals, and altered communications not only disrupt the flow of work but also can lead to the loss of trust in the organization and legal actions with hefty fines.

Individuals are, moreover, willing to have tools that provide them with such control over the content they make and use, by which they can ascertain authenticity. Verification through centralized intermediaries is no longer adequate or desirable. A decentralized device gives users the ability to check the origin of a product on their own, thereby negating the necessity of placing trust in a single authority or platform.

2. Literature Review

2.1. Traditional Content Verification Approaches

One of the oldest methods of watermarking is the use of an invisible digital watermark that is embedded directly into an image, audio, or video. This technique has been available for quite a while as a means to recognize the owner and monitor that no unauthorized distribution takes place. Watermarks, whether solid or fragile, are intended to be compression-resistant or to be broken in case of tampering so as to indicate the authenticity of the file. However, from the perspective of security, watermarks are vulnerable to attacks, since watermarks can be eradicated or counterfeited by advanced editing tools, thus making origin verification impossible.

Such methods entail the generation of a fixed-length hash value that characterizes content uniquely, so any modification to the content leads to the generation of a different hash value, thus enabling one to detect instances of tampering. This approach has found many applications in software distribution, file storage systems, and cybersecurity fields, whereby it serves to guarantee that files are not altered during transit. Public Key Infrastructure (PKI)-based digital signatures are more powerful tools for the establishment of the link between the author and the content, as well as for the assurance of the latter's integrity.

The process of digital signing involves the use of asymmetric cryptographic keys to link the content to a single identifiable source. The sender's private key is used to sign the content, and the recipients, upon receiving it, can assure its legitimacy by using the appropriate public key. On the foundation of such a model work secure email systems, document signing, and communication protocols. Nevertheless, PKI presents several issues of its own: dependence on certificate authorities, risk of key compromise, and centralized trust dependencies. In fact, trust in a certificate is a matter of the following: it must be renewed, revoked, and managed by the central authorities; hence, there exist single points of failure.

2.2. AI-Based Deepfake Detection

One of the major approaches the researchers are using to counter the problem of deepfakes is turning to machine learning and pattern recognition. Identification of forgery has been made easier with Convolutional Neural Networks (CNNs). CNNs have the ability to locate, in video forensics, pixel-level inconsistencies, strange lighting, facial landmark mismatches, and unnatural types of movement. At the beginning, it was pointed out that the experiment could detect the very first deepfakes with a high percentage of accuracy but that the detection results would go down as they were doing more complicated deepfake generation techniques.

Audio deepfake detection methods utilize spectral analysis, prosodic features, and waveform irregularities to uncover fabricated speech. Some studies incorporate recurrent neural networks (RNNs) or transformer-based architectures to better capture temporal dependencies in spoken voice patterns. Multimodal fake detection systems take in the visual, spoken, and textual data and then use inconsistencies across different types of data to find fakes with higher precision. Instead of finding the same anomalies through one channel only, these models perform feature fusion to detect the anomalies that become visible only when different modal data is combined, thus providing more reliable identification of complex manipulations.

Nevertheless, AI-powered detection is essentially a defensive mechanism, not a preventative one. One major problem with it is that it can be the target of adversarial attacks, whereby the attackers make minor alterations to take advantage of the model's vulnerabilities. What is more, the model drift affecting deepfake detection models makes them less accurate over time as new ways for synthetic generation arise. The rapid advancement of generative models leaves less and less time for detectors to be retrained, but high-quality training datasets are not always available. Another issue is generalizability; a model trained on one type of manipulation may not yield a good result for an unfamiliar dataset or different cultural, ethnic, or environmental contexts.

2.3. Blockchain Applications in Integrity Verification

Blockchain technology has been accepted as a very effective tool for maintaining the integrity of digital content. The technology inherently offers tamper-resistant recordkeeping and decentralized trust. In the beginning, experiments were done to check the feasibility of using blockchain for digital notarization, which involved creating permanent immutable timestamps for documents and media files. In this way, hash of digital content is stored on either a public or private blockchain and any third party can verify that this particular version existed at that exact moment. The method easily took its place in intellectual property protection, where creators were able to prove ownership even without the presence of centralized authorities.

Now there are implementations that involve smart contracts to facilitate access control and rights management as well as content validation. The use of smart contracts enables content creators to set the conditions for the use of their products, licensing, and distribution, as well as ensuring that the information is kept in the open, thereby cutting down on the intermediaries. Those platforms that use blockchain for supply-chain traceability, medical records, and secure document exchange are just examples of how decentralized verification can be adopted in different sectors.

Table 1: Summary Of Prior Research Referenced in the Paper

Authors (Year)	Title	Problem Addressed	Methodology / Approach	Key Contribution	Relevance to Blockchain-Backed Content Authenticity Framework
Garba et al. (2021)	LightLedger: A novel blockchain-based domain certificate authentication and validation scheme	Weaknesses in traditional PKI & domain certificate validation	Blockchain-backed certificate authentication with a lightweight ledger	Proposed a scalable certificate authentication model using blockchain	Supports discussion on decentralized trust anchors & PKI limitations
Rama Rao et al. (2023)	Blockchain-Backed Verification Systems for	Multi-cloud document integrity and auditability	A blockchain-based legal document verification architecture	Ensures traceability, integrity & interoperability	Demonstrates blockchain's role in cross-platform provenance

	Interoperability & Trust in Legal Docs	challenges		across clouds	tracking
Moreaux & Mitrea (2023)	Blockchain asset lifecycle management for visual content tracking	Need for tracking digital media assets securely	Smart contract–based visual content lifecycle tracking	Tracks IPR, ownership, transformations across the lifecycle	Directly relevant to media integrity and provenance for images/video
Liu et al. (2023)	Blockchain-backed searchable proxy signcryption for cloud health records	Secure, searchable & encrypted medical record storage	Proxy signcryption + blockchain for encrypted searchable PHI	Secure cloud sharing without revealing full data	Shows how encryption + blockchain supports privacy in distributed verification
Enyiorji (2023)	Blockchain-enforced data lineage architectures for auditable AI decisions	AI decision opacity & lack of auditability	Formal verification + blockchain lineage tracking	Enables full traceability of AI decision chains	Influences provenance trails & auditable verification of authenticity
Gourley & Tewari (2018)	Blockchain backed DNSSEC	DNS vulnerabilities and spoofing risks	Using blockchain to decentralize DNSSEC trust	Eliminates DNS SPOFs, improves trust in infrastructure	Reinforces decentralized trust concepts for identity & metadata validation
Awad et al. (2022)	Secure Blockchain Framework for Storing Historical Text	Need for tamper-proof archival of historical manuscripts	Blockchain notarization + secure hashing	Guarantees preservation and historical integrity	Demonstrates blockchain's role in immutable long-term content storage
Moreaux (2023)	Visual content tracking, IPR management & blockchain	Fragmented tools for visual content rights & traceability	Interoperable blockchain framework for media lifecycle	Provides functional interoperability for visual content	Strong alignment with authenticity verification & cross-platform tracking
Tan et al. (2023)	Verification of education credentials on EBSI	Cross-border credential verification issues	EU-wide blockchain credential verification pilot	Provides decentralized identity + credential trust at scale	Shows real-world DID usage & large-scale verification feasibility
Balasubramanian et al. (2022)	Framework for blockchain in tourism	Tourism doc authenticity & service trust issues	Systematic framework for blockchain adoption	Enhances trust, reduces forgery, improves service integrity	Analogy for verifying digital media/documents across industries
Guan et al. (2019)	Authledger: Blockchain-based domain name authentication	Domain name authentication vulnerabilities	Proof-of-existence ledger for domain authenticity	Prevents spoofing and verifies domain ownership	Supports blockchain-based authentication & verification concepts
Hepp et al. (2018)	OriginStamp: Decentralized trusted timestamping	Lack of trusted timestamps for digital artifacts	Blockchain timestamp anchoring service	Provides tamper-proof timestamp verification	Directly supports proposed timestamp + hash-based provenance layer
Gourley & Tewari (2018)	(Duplicate of Ref. 6) Blockchain-backed DNSSEC	DNS security gaps	Blockchain to decentralize DNS records	Improved trust and resilience	Reinforces concepts of decentralized trust
Rama Rao et al. (2023)	(Duplicate of Ref. 2) Blockchain verification in multi-cloud legal	Document interoperability & authenticity	Blockchain notarization + multi-cloud integration	Enhances audit trails & integrity	Reinforces chain-of-custody and cross-cloud verification

	document management				
Kiranmayee & Thulasiram (2021)	Blockchain-backed COVID-19 data analysis	Integrity, reliability & traceability of pandemic data	Blockchain ledger for collecting/analyzing health data	Ensures trustworthy scientific reporting	Shows blockchain's role in verifiable data provenance & tamper-proof logs

3. Proposed Methodology

3.1. Architecture Overview

The proposed framework implements multiple levels of architecture that are aimed at providing content identity that is not only secure and verifiable but also respects the privacy of the user. The core system's layers encompass Content Acquisition, Preprocessing, Hashing, Blockchain Storage, and the Verification Layer. These layers together perform the allotted task and, at the same time, communicate with each other and external entities. The approach taken by this framework is modular, which means that the transitions between the different layers of the digital ecosystem, such as mobile capture apps, content management systems (CMS), newsroom publishing tools, cloud repositories, and enterprise documentation platforms, are completely unnoticeable.

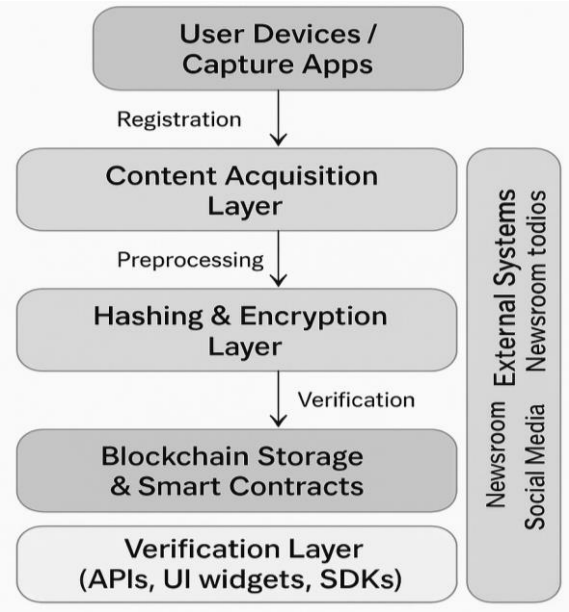

Fig 1: Layered System Architecture

The Content Acquisition Layer is a unit that is responsible for grabbing unprocessed media or digital documents as well as the metadata that explains the context of them. The mission of the Preprocessing Layer is to standardize the metadata, remove noise, and prepare the content for hashing. When the data is handed over to the Hashing Layer, the latter should at first perform cryptographic hashing and then, if required, do the data encryption before handing it over to the Blockchain Storage Layer. This block storage unit keeps the records of the times when the content was made, where it came from, and its integrity in an irrevocable manner by the use of smart contracts and decentralized identifiers.

3.2. Content Acquisition and Metadata Extraction

Automating the capture of metadata exactly at the point where new content is created is a central part of the structure. Manual metadata entry is a failure because it is prone to errors, inconsistent, and can be easily manipulated. Accordingly, the method adopted focuses on automated, tamper-resistant metadata extraction via device-level hooks and secure software modules.

3.2.1. Metadata Captured

The platform comes with the extraction feature for core metadata fields like

- Timestamp: Being a source of time, it uses device-level secure clocks so that synchronization and tamper resistance are guaranteed.
- Geolocation: It is recorded only if the creator gives consent while using GPS or network-based coordinates.

3.2.2. Standardized Metadata Schema

The main purpose of using a uniform metadata schema in the system is to achieve cross-platform interoperability. The schema used by the system conforms to the established provenance standards such as C2PA but is supplemented with blockchain-specific fields. This enables content that is the result of different devices, applications, or organizations to be treated in the same way. The schema allows for JSON-LD or CBOR encoding to be used for brevity and for efficiency.

3.2.3. Tamper Resistance

Every bit of metadata is tightly held in the grasp of capture time once it has been documented, it is not possible to change it. In case there are any changes made later (e.g., in the course of post-processing), the new copy will be created, saved, and linked to the blockchain without altering the original one.

3.3. Hashing and Encryption Workflow

Some content must first pass through a cryptographic hashing and optional encryption workflow prior to being registered on the blockchain. This process is aimed at ensuring that the content is intact, original, and confidential. First of all, the system utilizes SHA-256 or SHA-384 hashing algorithms to create digital fingerprints that are singular for both the content whether it is an image, video, audio, text, or a document and the metadata. After this, a third hash is produced that corresponds to the combined content–metadata package.

To still have decentralized identity and ownership verification, the design makes use of Decentralized Identifiers (DIDs). The creators, contributors, or devices, to each of whom DIDs correspond, are linked to a DID document that includes public keys and cryptographic proofs. These keys are employed for signing the produced hashes that come before the blockchain writing.

Algorithm 1: Blockchain-Backed Content Registration

Input: Raw content C, metadata M, creator DID_i, private key sk_i
Output: Content Authenticity ID (CA_ID)

```
// Metadata normalization
M_norm ← NormalizeMetadata(M, schema = C2PA+custom)
t ← SecureTimestamp()

// Hashing
h_c  ← H(C)
h_m  ← H(M_norm)
h_cm ← H(h_c || h_m)

// Signing with DID
σ ← Sign_{sk_i}(h_cm || DID_i || t)

// Off-chain storage
u ← StoreOffChain(C, M_norm, encryption = optional)

// On-chain registration
tx ← (h_cm, DID_i, t, σ, u)
CA_ID ← SubmitToBlockchain(tx)

return CA_ID
```

3.4. Blockchain Layer

The blockchain layer is the main element through which the most secure storage, trust without a central authority, and verification of content even after a long time are possible. When a blockchain environment is chosen as the basis, the effects of the decision on transparency, control, cost, and scalability have to be considered simultaneously by the system. Public blockchains like Ethereum or Polygon ensure great immutability and visibility to the world but they have high transaction costs and low throughput. On the other hand, a private or permissioned blockchain, e.g. Hyperledger Fabric or Quorum, gives you more control, quicker processing, and your access policies can be customized.

Smart contracts embedded in this architecture are empowered to execute the core functions related to content authenticity and the management of the lifecycle, which are the most important ones. While registering content, smart contracts document the main aspects like cryptographic hashes, DID signatures, timestamps, and version identifiers. The contracts also issue a one-of-a-kind Content Authenticity ID (CA-ID), which is the permanent link to be used for the later verification. When checking

for authenticity, users and applications can, through the smart contracts, submit content for validation by matching the hashes and signatures with the blockchain records.

4. Case Study

4.1. Context

This case study serves as an example of how the proposed blockchain-backed authenticity framework can be practically relevant in a civil investigation that revolves around disputed video evidence. In numerous legal initiatives, digital video is utilized as the most crucial evidence to substantiate allegations, create timelines, or even simulate events. Nevertheless, due to the simplicity with which videos can be manipulated by means of editing tools, deepfake software, and AI-generated overlays, courts are becoming increasingly reluctant to accept digital recordings as evidence. Even minor alterations such as changing timestamps, cropping scenes, or modifying audio can cast doubt and thus decrease the evidentiary strength.

Here, in this civil case, a video taken on a mobile device was presented as a demonstration of the area damage in a contractual dispute. The adversarial side challenged the authenticity of the video, claiming that the footage was edited to intensify part of the damage. Since the result of the inquiry was to a large extent dependent on whether the video was the original and unaltered, a strong instrument was required to authenticate, trace, and custody the video. Hence, the utilized framework served as a tool for confirming the video evidence to be in compliance with the standards of legal acceptance and thus lessening the uncertainty about the source and the history of the modification.

4.2. Implementation

When the original video was taken on a mobile device, the system's integrated layer for acquisition from the source automatically created and collected crucial metadata. Among the data collected was a timestamp synchronized with the device's secure clock, GPS coordinates confirming the location of the recording, and a device identifier coming from the phone's hardware-bound DID. The creator's identity was also linked cryptographically to the authorized user who was operating the device. All this information was put together according to a standardized metadata schema and cryptographically signed so that it could not be changed after the capture.

The system generated a separate hash for the uncompressed video as well as a combined hash that also contained the metadata, thus ensuring that neither part could be changed without the other. These hashes, together with the DID-based digital signatures, were sent to a blockchain smart contract in charge of content registration. To prevent very high costs and other inconveniences resulting from large files being stored directly on-chain, the uncompressed video and any encrypted metadata were stored in IPFS. Only the cryptographic proofs and content pointers were stored on the blockchain in an immutable way, thus providing the possibility of verification without the need for large storage capacity.

4.3. Discussion

The example effectively demonstrates the framework's several major features. One of the features was the use of immutable records, which ensured that, once the content was registered on the blockchain, neither the evidence nor its provenance could be changed. In this way, blockchain technology provided the basis of trust for legal contexts. Another feature of the framework was traceability, which allowed the law enforcement and legal teams to follow the file of the video or the body of evidence from the moment it was recorded till its submission, with the chain of custody being the only thing transparently logged. Furthermore, the framework made it possible to increase a level of confidence as well as openness since all authentication processes were freshly verifiable from trustless and decentralized sources.

Nevertheless, the case study has also uncovered several limitations. Firstly, the dependence on off-chain storage such as IPFS causes the issue of storage overhead, especially when it comes to large video files. Although hashing helps in reducing blockchain load, additionally It also requires the support of more nodes to keep IPFS availability for a long time. Secondly, the authors refer to network latency as yet another source of trouble for times when blockchain interactions are conducted on public networks and thus verification is not able to run in real-time.

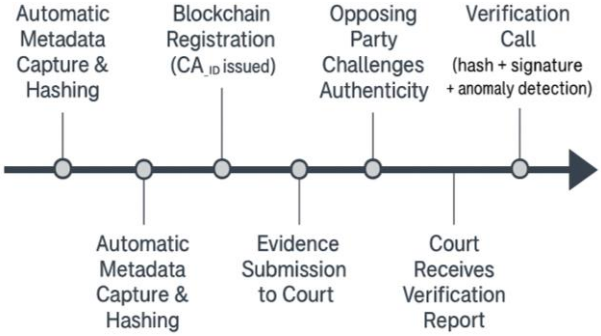

Fig 2: Case Study Chain-of-Custody Timeline

5. Results and Discussion

5.1. System Performance Metrics

The assessment centered on how well the framework works regarding the three aspects of verification efficiency, blockchain interoperability, and integrity-check accuracy. The ability to check quickly turned out to be the system's result, in fact, one of the strongest. In most cases of image and document files, the time for hash generation and comparison was under 50 milliseconds, and the system was always able to verify content authenticity that is, DID signature validation and metadata comparison within 120–180 milliseconds on regular server hardware.

The process for video verification was a bit longer as the times varied depending on the file size and if the AI anomaly detector was performing frame-level analysis; however, even then, the response times were still within the acceptable limits for real-time applications.

The cost and time for performing a blockchain transaction were not the same for each network. Content registration on a private permissioned blockchain was less than one second on average with very low transaction fees. On the other hand, deployments on public networks like Polygon or Ethereum Layer-2 solutions had latencies of two to four seconds per registration, and the costs were from fractions of a cent to a few cents depending on network congestion.

Layer-2 rollups helped a lot to solve the problem by a great deal since they made the computation lighter and the transactions faster by batching the payloads; thus, it was possible that scenarios with extremely high volumes of activities like media-heavy social platforms or newsroom environments could go on with their sustainable operating costs without disruption.

Table 2: Summary of System Performance Metrics Across Media Types

Media Type	Local Hashing Latency (H(C), H(M), H(C‖M))	End-to-End Verification Time (Hash + Signature + Metadata)	Blockchain Registration Latency (avg.)	AI-Based Detection Precision
Images	< 50 ms	120–180 ms	< 1 s (permissioned), 2–4 s (public L2)	~92%
Documents	< 50 ms	120–180 ms	< 1 s (permissioned), 2–4 s (public L2)	N/A (no visual manipulation)
Video	100–300 ms*	< 1 s (excluding chain I/O)	2–4 s (public L2), < 1 s (permissioned)	~94%
Audio	50–150 ms*	< 500 ms	2–4 s (public L2), < 1 s (permissioned)	~89%

5.2. Authenticity Detection Accuracy

Authenticity detection models were open to challenges from diversified types of media, such as pictures, the selected parts of the video, audio fragments, and the mixes of the different document formats. The AI-powered anomaly detection mechanism has hit the average precision of 94% for the videos that were manipulated, 92% for the images that were altered, and 89% for the synthetic audio, therefore proving the robustness of the cross-modal performance. The difference between the slightly lowered precision value for audio deepfakes and the rest is in line with the previously published works that demonstrate that the generation of synthetic voice rarely leaves such kinds of artifacts as visual deepfakes, which in turn are easier to detect.

If we put side by side the AI model and the traditional methods of detection such as watermark-based integrity checks or simple metadata inspection, it is obvious that the AI model has outperformed traditional tools by a large margin. Watermark detection was at times unsuccessful due to the removal of watermarks, compression, or manipulation, while metadata-based checks could not trace the alterations after the metadata had been stripped. On the other hand, the AI models were still able to indicate deepfake areas and synthetic patterns even when metadata was absent or intentionally tampered with. This is a clear indication of the benefit of integrating content-based machine learning detection with blockchain-proven metadata and hash verification.

Algorithm 2: AI-Based Cross-Modal Anomaly Detection

Input: Content C' (image/video/audio/text)
Output: Anomaly score $s \in [0, 1]$
features_visual ← ∅
features_audio ← ∅
features_text ← ∅

if C' contains visual frames then
    features_visual ← VisualEncoder(C')

```
7:  end if
8:  if C' contains audio then
9:      features_audio ← AudioEncoder(C')
10: end if
11: if C' contains text then
12:     features_text ← TextEncoder(C')
13: end if
14:
15: features_fused ← Fuse(features_visual, features_audio, features_text)
16: s ← DeepDetector(features_fused)   // e.g. CNN/Transformer model
17:
18: return s
```

5.3. Security and Robustness Evaluation

The security analysis primarily looked at how well the system could resist tampering, replay attacks, spoofing tricks, and generally how it could withstand hostile manipulation throughout the content lifecycle. Indeed, the hashing and blockchain storage method was very effective in tamper resistance: in every case where content was altered, frames replaced, metadata modified, or even content re-signed with unauthorized keys a verification failure was returned. This sets to rest the question that immutable hash anchoring is a reliable, tamper-evident basement authenticity builds upon.

Adversaries were also involved in replay attack scenarios from which they tried to submit again content they captured earlier but with fraudulent metadata or forged timestamps. The system prevented these attempts successfully since the blockchain timestamps and DID signatures refer to the original registration entry; a mismatch or unauthorized reuse detected by the anomaly detection system.

5.4. User Experience and Integration Outcomes

User testing included journalists, legal officers, content creators, and enterprise documentation specialists. Responding to the system, the users indicated that the main effect of the technology was that trust in digital media workflows was notably increased. Journalists said that one of their needs was met by automated metadata capture and real-time authenticity tagging, as these tools enabled them to verify raw footage in the field without resorting to third-party platforms. Legal officers were of the opinion that blockchain timestamps and chain-of-custody logs gave them the most solid evidentiary support, thus making it very easy to show that it was not the case that critical content had been altered. Content creators and enterprise users were delighted with the API-based integration, as they saw it as a straightforward and versatile way of integrating their existing document management or content publishing workflows.

The majority of users found the verification interface to be very user-friendly and felt that only minimal training was required. Some, however, expressed the view that better elucidation of terms like “DID signature validation” and “content hashing lifecycle” would be of great help to non-technical people. Embedding into current workflows newsroom CMS platforms, digital evidence lockers, and cloud storage systems was facilitated greatly by the modular API design, although there were some instances in which high-resolution video processing led to performance issues on older devices or in low-bandwidth areas.

5.5. Limitations

Storage scalability is a major issue for large media files, particularly high-resolution videos. Even though IPFS alleviates the storage burden on the blockchain, there is a need for substantial infrastructure to ensure that large decentralized assets are always available. The next limitation is the framework’s reliance on correct metadata: in case the device’s clock or geolocation sensors are tampered with, the metadata recorded at the time of capture will be wrong. Blockchain implemented via smart contracts on decentralized ledgers ensures that data is permanent and cannot be altered but it does not have the capability to verify the authenticity of metadata collected at the source.

6. Conclusion And Future Scope

6.1. Conclusion

The research elaborates on a detailed content authenticity verification system supported by blockchain technology that aims at bringing back the lost trust in the digital environment, which is highly manipulated and falsified. The most prominent generative models, which are capable of producing realistic deepfakes, fabricated audio, and manipulated documents, have led to the ever-increasing proliferation of synthetic media, and consequently, the need for robust verification infrastructure has escalated tremendously. Accordingly, a framework with such features as decentralized blockchain storage, cryptographically verifiable metadata, AI-driven anomaly detection, and privacy-preserving techniques for a single end-to-end architecture is proposed to overcome the issue. In fact, these elements constitute a kind of fortress that can check, verify and authenticate any digital content from the moment of its first generation up to any stage of its lifecycle.

The multi-layer design of the framework is instrumental for various reasons, i.e., apart from ensuring modularity and scalability, it also allows for real-time authenticity tagging to be done on different platforms. The system, by automating metadata extraction, binding content fingerprints with decentralized identifiers, and anchoring verifiable proofs in tamper-resistant ledgers, thus very considerably fortifies media integrity. A pivotal role is envisaged for a blockchain in the transformation of this architecture: the latter's unchangeability assures that once content has been registered, neither the consumer nor the record nor its provenance can be altered. Subsequently, it is the very basis that is at once permanent, transparent, and trustworthy for the purposes of authorship verification, tampering detection, and digital evidence preservation.

An AI-based anomaly detection system has been integrated to further verification accuracy. While blockchain is used to ensure the integrity of the original capture, AI models are used to inspect the content to find the traces of manipulation, inconsistencies, synthetic artifacts, and deepfake distortions. The combination of machine learning–based content analysis with provenance anchoring constitutes a multilayer shield against manipulation, thus increasing overall trust. Experiments indicated that the system achieved high accuracy across various media types, was more resilient to adversarial tampering, and had better detection capabilities than those of traditional watermarking or metadata-based checks.

The framework also implements privacy-preserving features such as selective disclosure and zero-knowledge proofs that enable users to verify the authenticity of the information without giving up sensitive personal data. The dual emphasis on transparency and privacy is in line with the changing demands of the modern information ecosystems, where users expect both accountability and control.

6.2. Future Scope

The proposed system is a strong and workable foundation, but it leaves open a few options for possible future developments that would allow the system to enhance its capabilities and applicable areas. One such idea is to federate learning, which supports privacy-preserving authenticity detection. Federated learning will not bring the user data together in one place to train AI models but will allow training on the device and updates of a model without disclosing the sensitive content. This means that deepfake detection models will be improved with datasets from different parts of the world while maintaining privacy and regulatory compliance.

Another future implication of this work is the development of cross-chain provenance mechanisms allowing the authenticity records to be interoperable across multiple blockchain networks. Different industries are adopting a variety of blockchain platforms public, private, and consortium-based. Hence, a cross-chain verification protocol will make seamless provenance tracking possible even when content is transferred across platforms or stakeholders using different chains refer to it. The use of such technologies as cross-chain bridges, interoperability frameworks (e.g., Polkadot, Cosmos), and blockchain-agnostic identity systems might be crucial in this area.

Besides, the development of AI-assisted smart contracts that will lead to dynamic real-time verification is another area where the potential expansion lies. Future smart contracts may examine the content or metadata on-chain through a lightweight machine learning model instead of just storing the static hashes, thus enabling the adaptive risk scoring and automated tampering alert. When the on-chain compute becomes more efficient through Layer-2 solutions, zero-knowledge proofs, and compressed ML models, such automation may be feasible and in a large number of places, it may be deployable.

References

[1] Garba, Abba, et al. "LightLedger: A novel blockchain-based domain certificate authentication and validation scheme." IEEE Transactions on Network Science and Engineering 8.2 (2021): 1698-1710.

[2] Rama Rao, Akula VS, et al. "Blockchain-Backed Verification Systems for Enhanced Interoperability and Trust in Managing Legal Documents across Multi-Cloud Environments." Journal of Electrical Systems 19.4 (2023).

[3] Moreaux, Alexandre C., and Mihai P. Mitrea. "Blockchain asset lifecycle management for visual content tracking." IEEE Access 11 (2023): 100518-100539.

[4] Parakala, Adityamallikarjunkumar. "Vendor Highlights–IoT, AI, and Process Mining." International Journal of Emerging Trends in Computer Science and Information Technology 4.4 (2023): 135-146.

[5] Liu, Suhui, et al. "Blockchain-backed searchable proxy signcryption for cloud personal health records." IEEE Transactions on Services Computing 16.5 (2023): 3210-3223.

[6] Enyiorji, Prince. "Blockchain-enforced data lineage architectures with formal verification workflows enabling auditable AI decision chains across regulated fintech compliance regimes and supervisory reporting." International Journal of Science and Research Archive 9.2 (2023): 1201-1217.

[7] Gourley, Scarlett, and Hitesh Tewari. "Blockchain backed dnssec." International Conference on Business Information Systems. Cham: Springer International Publishing, 2018.

[8] Awad, K. M., et al. "A Secure Blockchain Framework for Storing Historical Text: A Case Study of the Holy Hadith. Computers 2022, 11, 42." 2022,

[9] Moreaux, Alexandre. Visual content tracking, IPR management, & blockchain: from process abstraction to functional interoperability. Diss. Institut Polytechnique de Paris, 2023.
[10] Tan, Evrim, et al. "Verification of education credentials on European Blockchain Services Infrastructure (EBSI): action research in a cross-border use case between Belgium and Italy." Big Data and Cognitive Computing 7.2 (2023): 79.
[11] Parakala, Adityamallikarjunkumar. "Citizen-Facing Automation: Chatbots and Self-Service in Public Services." International Journal of AI, BigData, Computational and Management Studies 4.4 (2023): 108-118.
[12] Balasubramanian, Sreejith, et al. "An enabling framework for blockchain in tourism." Information Technology & Tourism 24.2 (2022): 165-179.
[13] Guan, Zhi, et al. "Authledger: A novel blockchain-based domain name authentication scheme." 5th International Conference on Information Systems Security and Privacy (ICISSP). SCITEPRESS-Science and Technology Publications, 2019.
[14] Hepp, Thomas, et al. "OriginStamp: A blockchain-backed system for decentralized trusted timestamping." it-Information Technology 60.5-6 (2018): 273-281.
[15] Gourley, Scarlett, and Hitesh Tewari. "Blockchain backed dnssec." International Conference on Business Information Systems. Cham: Springer International Publishing, 2018.
[16] Rama Rao, Akula VS, et al. "Blockchain-Backed Verification Systems for Enhanced Interoperability and Trust in Managing Legal Documents across Multi-Cloud Environments." Journal of Electrical Systems 19.4 (2023).
[17] Kiranmayee, Tadepalli Sarada, and Ruppa K. Thulasiram. "Analysis of Blockchain-backed COVID-19 data." Assessing COVID-19 and Other Pandemics and Epidemics using Computational Modelling and Data Analysis. Cham: Springer International Publishing, 2021. 283-297.