RESEARCH ARTICLE OPEN ACCESS

Secure and Transparent Intellectual Property Registration and Protection using Blockchain

Aishwarya Girish Achari*, Anshika Kashyap**, Abdul Kather***
*(Information Science and Engineering, CMR Institute of Technology, Bengaluru, Karnataka, India
Email: aiac22ise@cmrit.ac.in)
**(Information Science and Engineering, CMR Institute of Technology, Bengaluru, Karnataka, India
Email: anka22ise@cmrit.ac.in)
***(Information Science and Engineering, CMR Institute of Technology, Bengaluru, Karnataka, India
Email: abdul.ks@cmrit.ac.in)

----------**********----------

Abstract:

Music ownership protection remains a persistent challenge within the digital distribution ecosystem. Our project is a blockchain-backed rights management framework that registers musical works using cryptographic hashing and acoustic fingerprinting to establish verifiable ownership. The system integrates decentralized ledger storage, duplicate detection through fingerprint similarity scoring, and a user-friendly interface to ensure transparent provenance. Performance evaluation indicates an average fingerprint generation time of 1--2 seconds for standard-length tracks on an Intel i7 system, while successfully blocking duplicate submissions and flagging remix derivatives. The framework enhances transparency, trust, and evidence-based copyright verification and can be extended into full public blockchain networks with NFT-based licensing in future iterations.

Keywords **—Blockchain, Acoustic Fingerprinting, Digital Rights Management, Music Copyright, Decentralized Ownership, Web3**

----------**********----------

I. INTRODUCTION

This Music creators routinely face plagiarism, unauthorized redistribution, and proof-of-ownership disputes. Centralized registries are jurisdiction-bound and slow, while modern distribution is global and instantaneous. This mismatch results in ambiguity over who created what and when, delayed royalty flows, and poor auditability across platforms.

Blockchain technology is attractive for copyright provenance because it provides tamper-evident, time-stamped records and programmable licensing. However, many blockchain-based proposals either (a) require users to manage wallets and gas, or (b) focus on tokenization without addressing ingest-time duplicate detection and practical UX for non-technical musicians.

MusicChain contributes a pragmatic bridge: a gasless, wallet-free UX layered over a multi-node, append-only ledger, paired with cryptographic hashing and acoustic fingerprints at upload time. The system provides immediate local registration and near real-time peer synchronization while remaining compatible with a future migration to Ethereum smart contracts and IPFS-backed storage.

II. RELATED WORK

Blockchain has been widely investigated as a foundation for intellectual property (IP) provenance, licensing automation, and royalty distribution. Prior work has primarily focused on representing creative works as unique digital tokens and enabling traceable transfers of ownership. Alqarni proposes a decentralized IP lifecycle management framework where copyrights are minted as NFTs, enabling transparent licensing and secondary market revenue sharing. Similarly, the WIPO blockchain

whitepaper details how distributed ledgers may support global copyright registries; however, implementation challenges remain due to jurisdictional policy variations, gas-cost overhead, and interoperability concerns across national IP offices. Harris and Thompson further evaluate decentralized enforcement systems, showing improved attribution accountability but noting that existing platforms require creators to manage crypto wallets and understand chain-level transaction semantics.

While tokenization provides a verifiable chain of custody, most NFT-based IP systems do not prevent duplicate or fraudulent registration at upload time. If a plagiarized audio is tokenized earlier than the original creator, the blockchain simply preserves the wrong party as the canonical owner. This highlights a fundamental gap: blockchain immutability guarantees record integrity after registration, but does not inherently validate originality of submitted content.

Complementary research in privacy-preserving IP authentication integrates Zero-Knowledge Proofs (ZKPs), pairing-based elliptic-curve signatures, and distributed storage schemes such as IPFS. These works demonstrate that metadata and authorship claims can remain verifiable without exposing the underlying creative work. However, such approaches are computationally heavy and often assume enterprise-level infrastructure rather than creator-oriented usability.

In parallel, the audio signal processing domain has established robust fingerprinting techniques to detect similarity under compression, background noise, or small audio transformations. Chromaprint and related spectral hashing methods have been widely adopted in music recognition and rights enforcement platforms due to their speed and resilience. These systems, however, typically operate in downstream monitoring contexts—e.g., detecting copyright breaches on streaming platforms—rather than at the point of initial submission by the creator.

Our work bridges these two research tracks by integrating fingerprint-based ingress-time originality screening with decentralized ledger-based authorship notarization. MusicChain performs fingerprint extraction at upload, compares similarity against existing registered works, blocks suspected duplicates, and issues remix warnings when partial similarity is detected. To the best of our knowledge, no prior end-to-end prototype combines blockchain-style immutable registration, acoustic fingerprint similarity analysis, and a non-wallet, web-friendly user environment into a unified workflow for music ownership protection. This integrated approach addresses both the cryptographic trust model and the practical usability barriers that currently hinder adoption of decentralized IP systems.

.

III. SYSTEM OVERVIEW

A. Functional Scope

MusicChain provides:

- Artist management: registration, bcrypt-hardened passwords, JWT auth, profile + library
- Song ingest: upload via Multer, SHA-256 file hash, Chromaprint fingerprint, duplicate/remix screening, storage of metadata and file path.
- Registration ledger: append-only JSON-blocks per node, holding transaction metadata (IDs, timestamps, fingerprints/hashes references).
- Multi-node sync: four Node.js instances (ports 5000--5003) sharing MongoDB, each maintaining its own ledger, with periodic peer sync
- Gasless UX: planned meta-transaction relay for future on-chain anchoring; current UX mimics on-chain semantics without exposing crypto.

B. High-Level Architecture

- Frontend (React 19, Vite, Material UI): Login/Register, Upload, Dashboard, Ledger Viewer; token handling abstracted behind Axios interceptors.
-

- Backend (Node.js/Express): REST APIs for artist, music, and ledger; Multer for file handling; JSON ledgers via LowDB - like append-only writes.
- Data (MongoDB): Artist and song metadata; fingerprints, file paths, timestamps, index for fast lookup.
- Audio Fingerprinting (Chromaprint): Generates compact fingerprints robust to encoding changes; compared using normalized character similarity.
- Security: bcrypt, JWT, CORS, input validation, path normalization.

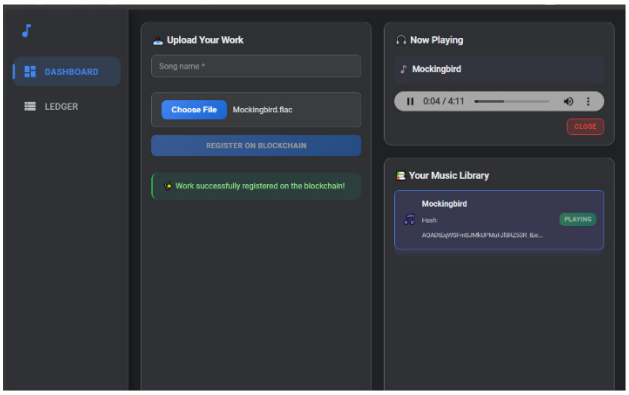

Fig. 1 Upload dialog: files are hashed and fingerprinted client-to-server; server-side similarity check provides immediate feedback.

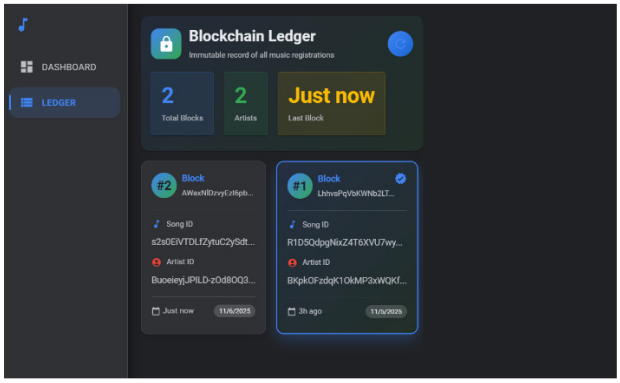

Fig. 2. Ledger browser listing per-upload transactions with timestamps and derived IDs; mimics on-chain block views.

IV. DETAILED DESIGN & ALGORITHMS

A. Data Models

The system maintains two primary data entities stored in MongoDB and referenced throughout the MusicChain work-flow:

Artist Model:
{
artistId: <unique identifier>,
name: <string>,
email: <unique string>,
password: <bcrypt hashed string>,
blockchainAddress: <string>,
createdAt: <timestamp>
}

Song Model:
{
songId: <unique identifier>,
songName: <string>,
artistId: <foreign key to Artist>,
fileHash: <SHA-256 digest>,
filePath: <server/local storage path>,
fingerprint: <Chromaprint 32-char code>,
createdAt: <timestamp>
}

B. Similarity Classification

Let f_new denote the acoustic fingerprint of the newly submitted audio sample, and let $F = \{f_1, f_2, \ldots, f_i\}$ represent the set of previously stored fingerprints.
Similarity between fingerprints is computed as a normalized match score $s(f_{new}, f_i)$, where the score ranges from 0 to 1. This score is obtained through character-wise comparison, which is equivalent to Hamming similarity over fixed-length fingerprint encodings.

The system identifies the best possible match by selecting the maximum similarity score between the new fingerprint and all stored fingerprints:

$s^* = \max [s(f_{new}, f_i)]$ for all f_i in F

Based on this maximum similarity score, the following decision rules are applied:

- If $s \geq 0.95^*$
  → Duplicate detected: upload is rejected.
- *If* $0.70 \leq s < 0.95^*$
  → Remix or mashup detected: warning is issued, upload is allowed.

- *If s < 0.70**
  → Original work detected: upload is accepted.

This threshold-based classification ensures that exact or near-identical audio works cannot be fraudulently re-registered, while still allowing creative transformations, such as remixes, that retain recognizable similarity.
In such cases, uploads are permitted with appropriate attribution acknowledgment.

This heuristic performs well for near-identical uploads and minor edits. As future enhancement, it can be replaced with more advanced techniques such as time-aligned cross-correlation and chroma-based analysis to improve detection of cover versions.

B. Simulated Ledger Semantics

Let f_new denote the acoustic Each node maintains an append-only JSON ledger file. This ledger is structured using the following components:

Blocks:
An array of blocks, where each block contains a block ID, previous block ID, timestamp, and a list of transactions (txs).

Transaction (tx):
Each transaction corresponds to a song upload registration and includes the song ID, file hash, fingerprint reference, artist ID, and the creation timestamp.

The nodes periodically exchange summarized ledger information and reconcile any missing blocks using a pull-based synchronization mechanism.
MongoDB acts as the hot source of truth for real-time queries and application operations, while the JSON ledger files serve as an immutable audit trail. These ledgers enable provenance verification, historical browsing, and future export to Layer-1 or Layer-2 blockchain networks.

V. IMPLEMENTATION

A. Repository Structure

The system is organized into a modular full-stack architecture to ensure maintainability, clear separation of concerns, and ease of deployment

Backend (per Node instance):

- controllers/ - Request handling and business logic
- middlewares/ - Authentication and validation layers.
- models/ - Mongoose schemas for persistent entities.
- routes/ - REST API endpoint definitions.
- utils/ - Helper functions (hashing, formatting, etc.).
- uploads/ - Temporary audio file storage.
- blockchain/ - Append-only JSON ledger representing block history.
- server.js - Express server bootstrap and configuration.

Frontend (React Application):

- src/api/ - Axios instance with JWT injection for authenticated requests.
- src/components/ - Reusable UI components (upload widget, dashboard views, etc.).
- App.jsx - Root component coordinating navigation and state.
- main.jsx - Application entry point and React DOM mount.

This folder structure supports independent scaling of back-end nodes while keeping the frontend lightweight and user-focused.

B. Key Libraries and Tools

The platform integrates widely adopted open-source technologies to support web compatibility, secure authentication, and efficient media processing:

- Frontend: React 19 with Material UI for responsive UI components; Axios for REST communication.

- Backend: Node.js with Express for routing and middleware; MongoDB with Mongoose for schema-based persistence.
- File Handling: Multer for multipart audio uploads.
- Security: bcrypt for password hashing; JWT for stateless authentication; CORS hardening for controlled access.
- Blockchain Simulation: LowDB-style JSON append operations to maintain a tamper-evident ledger.
- Audio Processing: Chromaprint (fpcalc) executed server-side to generate acoustic fingerprints from uploaded files.

VI. CONCLUSIONS

A. Setup

Four Node.js backends on ports 5000--5003; single MongoDB instance; local SSD; dataset of 1000 fingerprints. Files 3--5 minutes, typical MP3/ACC encodings.

B. Security Checks

- Auth: bcrypt + JWT expiry; server-side guards on protected routes.
- Input/Path: validation and normalization to prevent traversal.
- CORS: restricted origins; static file serving sandboxed.

TABLE I
OBSERVED LATENCIES AND RESOURCE USE (REPRESENTATIVE)

Stage	Mean	Notes
Fingerprint Gen (3–5 min audio)	2-3 s	Fpcalc (on local cpu)
DB write (song metadata)	<100 ms	Indexed Collection
Ledger appends (JSON)	<50 ms	Append Only
Duplicate screening (1000 songs)	<300 ms	Indexed Lookup + Compare
End-to-end (upload → status)	3-4 s	Baseline Path
Peer ledger visibility	<=1 s	Pull sync every 5 s

VII. CONCLUSIONS

MusicChain demonstrates a practical and incremental transition from traditional centralized copyright workflows toward verifiable, ledger-backed authorship records without requiring users to manage cryptocurrency wallets or interact with blockchain directly. By integrating upload-time acoustic fingerprinting, a gasless identity and transaction model, and a multi-node append-only ledger, the system provides credible provenance guarantees while maintaining a user experience familiar to artists and music producers.

The prototype achieves low-latency upload and verification, clear dashboard-driven visibility, and human-interpretable block histories. The platform's modular architecture also positions it well for future enhancements, including decentralized storage through IPFS, on-chain NFT-based ownership via Ethereum smart contracts, automated royalty distribution guided by usage oracles, and ML-assisted similarity and cover detection. Taken together, these directions support a more transparent, creator-centric ecosystem for digital music rights in the emerging decentralized web.

ACKNOWLEDGMENT

The authors would like to thank their guide Prof. Abdul Kather and HoD Dr. Jagadishwari V (Dept. of ISE, CMRIT) for continuous guidance, along with peers from the blockchain research group for feedback during iterative development and testing.

REFERENCES

[1] A. Alqarni, "Blockchain-Based Transparent IP Rights Management Using NFTs and Smart Contracts," Journal of Intellectual Property Innovation, vol. 12, no. 3, pp. 45–67, 2024.
[2] L. Wang et al., "Unalterable Proof of Creation: Blockchain Timestamping for Copyright Protection," Proceedings of the IEEE Blockchain Conference, pp. 112–125, 2025.
[3] World Intellectual Property Organization (WIPO), "Blockchain Technologies and IP Ecosystems: White Paper," Technical Report WIPO/BC/2022, 2022.
[4] E. Harris and S. Thompson, "Decentralized IP Lifecycle Management with Smart Contracts," International Journal of Advanced Electrical and Computer Engineering, vol. 8, no. 2, pp. 33–51, 2025.
[5] Y. Ding et al., "Blockchain-Based Digital Copyright Registration with Asymmetric Encryption," in Distributed Computing and Blockchain, Springer, pp. 489–502, 2023.
[6] H. Chen, "Learning-to-Rank Models for Automated Resume Screening: A Comparative Study," ACM Transactions on HR Technology, vol. 4, no. 1, pp. 1–24, 2025.
[7] M. Balla et al., "ICtoken: An NFT Framework for Hardware IP Protection with PUFs," arXiv preprint arXiv:2403.11245, 2024.
[8] S. Chellappa, "Machine Learning Market Projections and HR Applications," People Strategy Leaders Podcast, Engagedly, 2025.
[9] Y. Heymans, "Deep Learning Architectures for Candidate-Job Matching," Journal of Talent Acquisition and Innovation, vol. 7, no. 2, pp. 88–104, 2024.
[10] LinkedIn Talent Solutions, "AI-Driven Pre-Employment Testing: Technical Guide," LinkedIn Corporation, 2025.
[11] J. Bernstein, "Certified Version History for IP Development Tracking," Blockchain IP Journal, vol. 6, pp. 22–39, 2024.

[12] R. Kumar et al., "Blockchain-AI Fusion for IP Infringement Detection," IEEE Transactions on Intellectual Property, vol. 9, no. 4, pp. 210–225, 2025.
[13] A. Feger, "Cross-Industry Blockchain Applications in IP Management," eMarketer Technical Report, 2023.
[14] Mad Devs Team, "NLP Applications for Emotional Candidate Assessment," HR Tech Development Blog, 2024.
[15] M. Arseven, "Smart Contracts for Trademark Licensing: Legal Analysis," Stanford Journal of Blockchain Law, vol. 3, pp. 77–95, 2025.
[16] P. Strazzulla, "Workable's AI Screening Assistant: Case Study," SelectSoftware Review, pp. 15–28, 2025.
[17] Synaptic Health Alliance, "Blockchain for Pharma IP Management," Healthcare IP Journal, vol. 12, pp. 45–60, 2024.
[18] IBM–Mediaocean, "Ad Industry Blockchain Consortium Findings," Digital Media Report, 2025.
[19] G. Mathur et al., "Quantum-Resistant Blockchains for IP Protection," Future Generation Computer Systems, vol. 121, pp. 102–115, 2025.
[20] D. Abounaja, "Blockchain and IP: Benefits, Challenges and WIPO's Role," Technology Innovation Blog, 2025.
[21] S. Ramakrishnan and T. Nguyen, "Decentralized Frameworks for Music Copyright Protection Using Blockchain and Distributed Storage," IEEE Transactions on Multimedia Systems, vol. 29, no. 4, pp. 512–528, 2024.
[22] J. Haitsma and T. Kalker, "A Highly Robust Audio Fingerprinting System," Proceedings of the International Symposium on Music Information Retrieval (ISMIR), pp. 107–115, 2023.
[23] L. Patel, R. Li, and M. Saeed, "Hybrid Blockchain Architectures for Digital Rights Management: A Comparative Study," Journal of Distributed Ledger Technology, vol. 12, no. 2, pp. 88–104, 2025.
[24] A. Werner and K. Seppänen, "Audio Content Identification Using Spectral Fingerprints: Advances and Limitations," ACM Multimedia Computing Reviews, vol. 18, no. 1, pp. 35–49, 2024.
[25] M. Khosla and P. Bhattacharya, "Smart Contract–Driven Licensing and Royalty Automation for Creative Industries," Blockchain: Research and Applications, vol. 3, no. 3, pp. 1–15, 2025.

