Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.039716
*Article*

# MBE: A Music Copyright Depository Framework Incorporating Blockchain and Edge Computing

**Jianmao Xiao[1], Ridong Huang[1], Jiangyu Wang[1], Zhean Zhong[1], Chenyu Liu[1], Yuanlong Cao[1],* and Chuying Ouyang[2]**

[1]School of Software, Jiangxi Normal University, Nanchang, 330027, China
[2]Department of Physics, Jiangxi Normal University, Nanchang, 330027, China
*Corresponding Author: Yuanlong Cao. Email: ylcao@jxnu.edu.cn

Received: 12 February 2023; Accepted: 12 April 2023; Published: 09 November 2023

**Abstract:** Audio copyright is a crucial issue in the music industry, as it protects the rights and interests of creators and distributors. This paper studies the current situation of digital music copyright certification and proposes a music copyright certification framework based on "blockchain + edge computing mode," abbreviated as MBE, by integrating edge computing into the Hyperledger Fabric system. MBE framework compresses and splits the audio into small chunks, performs Fast Fourier Transform (FFT) to extract the peak points of each frequency and combines them to obtain unique audio fingerprint information. After being confirmed by various nodes on the Fabric alliance chain, audio fingerprint information and copyright owner information are recorded on the chain and broadcast to all participants. Blockchain technology's characteristics of being tamper-proof and traceable not only reform the trust mechanism of copyright protection but also endow edge computing with the ability to resist tampering and single-point attack, greatly enhancing the robustness of the music copyright certification system. Meanwhile, edge computing mode improves Fabric blockchain's processing speed and transaction throughput. Experimental results show that MBE's performance is better than traditional systems regarding efficiency, storage demand and security. Compared to the traditional Fabric system without edge computing mode, MBE exhibits a 53% higher deposition efficiency and a 48% lower storage space requirement.

**Keywords:** Blockchain; copyright protection; audio fingerprinting; smart contracts

## 1 Introduction

The widespread use of the Internet in recent years has resulted in an increasing number of musicians digitizing their compositions. This has reduced the costs associated with content distribution and facilitated global access to musical works. Despite these benefits, the digital age has created new avenues for music piracy [1]. Copyright disputes are widespread, and the persistent problem of music copyright infringement continues to be prohibited. The traditional processes of registering music copyrights could be more problematic, characterized by high deposit costs, complex and confusing procedures, and lengthy transaction cycles. These issues require immediate attention.

Blockchain technology has garnered widespread attention and research due to its decentralized, immutable, traceable, and smart contract-based characteristics. Utilizing cryptographic algorithms and distributed storage nodes, blockchain is a new trust mechanism that breaks from the traditional centralized bookkeeping structure [2]. As a new computing model that performs computation at the network's edge, Edge computing reduces the computational pressure on the network core and provides new node deployment options for blockchain [3]. Integrating blockchain and edge computing technologies into a single system enables reliable access and control of the network.

Existing digital copyright trading platforms need more research on integrating blockchain and edge computing technologies. Most of the literature focuses on smart contracts for copyright transactions, with few studies examining functions such as audio copyright registration and rights confirmation. In light of this, we propose MBE framework based on the "blockchain + edge computing" model, which offers rapid copyright verification, tamper-evident and traceable characteristics following deposition. The digital music created by the original musician is stored on a decentralized and transparent blockchain via an audio fingerprint recognition algorithm, which generates a unique audio fingerprint (representing a digital summary of the audio signal). The underlying blockchain adopts the Hyperledger-Fabric federated chain architecture and leverages edge computing. Results from experimental analysis and testing indicate that the MBE framework has significantly improved accuracy in audio fingerprint generation, transaction processing volume, and response time compared to traditional digital copyright platforms.

The main contributions of this paper are as follows:

1. We present a novel solution that leverages the integration of blockchain and audio fingerprint technology to tackle the challenges of centralization and piracy prevalent in current digital music copyright platforms. Our solution aims to enhance the system's reliability by addressing these pain points.
2. Building upon the Dejavu[1] project, we introduce an audio fingerprinting solution that offers greater accuracy and faster retrieval speeds than traditional PRH methods. This will enhance the reliability and efficiency of existing audio copyright deposition technology.
3. Our Fabric federated chain framework, developed under the "blockchain + edge computing" model, represents a groundbreaking approach to music copyright deposition. Through rigorous testing and analysis, our solution has been shown to improve the efficiency of the system by 53%, greatly optimize transaction throughput, and reduce response times.

This paper investigates the pain points of existing digital music copyright depository and proposes an efficient MBE framework based on "blockchain + edge computing model". The paper is organized as follows: In Section 1, we discuss the changes and advantages that blockchain technology and edge computing model can bring to audio deposition. Section 2 presents related work and the current state of audio copyright deposition. Section 3 describes the design and implementation of the MBE framework in detail and introduces the principle of the audio fingerprint retrieval algorithm as well as the process. Section 4 shows the experimental results and analysis to demonstrate the advantages of the MBE framework over the traditional model. Section 5 concludes the conclusion and future work.

[1] https://github.com/worldveil/dejavu

## 2 Related Work

### *2.1 Digital Music Copyright Depository*

The copyright system is the institutional foundation of the music industry. Digital music copyright is the right of digital music creators to protect their works under copyright law. Digital music refers to musical works that can be listened to and downloaded online in digital form through the Internet using digital information technology [4]. The integration of digital music and information technology has made digital music fast, extensive and efficient. When the digital music industry was in its infancy, music websites sprang up to attract users to form a scale. Many of them provided pirated digital music access services for free, leading to the prevalence of online piracy and chaos in the digital music copyright market.

The transaction and protection of copyright in the digital music market mainly revolve around three main parties, i.e., digital music sources (creators, record companies, music publishing companies), music service providers (digital music platform companies), and users who acquire music. The digital music copyright transaction involves many economic interests, and the intertwined and conflicting interests of multiple parties in the context of fierce competition among the major platforms lead to a complex process and a long period for digital music copyright transactions [5]. The market power gap between digital music creators, music publishing companies, and music platform companies is large. They are often in a disadvantaged position in the process of copyright trading and protection. They are easily squeezed of their original rights and interests, such as in the case of Wu Xiangfei’s lawsuit against Universal Music Copyright Company in 2021 for misappropriation of his works’ publishing fees [6]. As a result, more reliable technology is needed to ensure fairness throughout the digital music market.

### *2.2 “Blockchain + Audio” Fingerprint Retrieval Technology*

The core of audio work copyright deposition lies in audio recognition. The key is to use some feature to identify audio to quickly retrieve specific audio and perform audio similarity matching [7]. As a result, audio information retrieval technology has emerged. Audio information retrieval uses physical features such as frequency and amplitude of audio information, auditory features such as pitch, loudness and timbre. It features such as audio category and semantics to achieve content-based audio information retrieval. One of the widely used audio information processing methods is audio fingerprinting retrieval technology. Audio fingerprinting refers to the extraction of unique digital features in a piece of audio as identifiers through a specific algorithm, which can represent a content-based digital summary of the important acoustic features of a piece of music. Audio with different melodies has different audio fingerprints, which can be used to identify many sound samples or track the location of the samples in the database [8].

The earlier incarnations of centralized copyright platforms lacked features such as audio identification and detection, resulting in rampant piracy and plagiarism. To illustrate, instances of music with identical melodies being repurposed under new names for profit were common. Several extant music copyright platforms have attempted to curb these issues through the creation of a substantial quantity of audio fingerprint records to identify pirated music. However, their centralized storage methodology engenders significant covert risks and incalculable losses once data is altered or deleted. Moreover, the music copyright trading platform that is constructed on such a basis is encumbered by a complicated deposition process, a prolonged time span, transaction information that is not transparent, and a lack of traceability [9].

Blockchain technology can solve the current problems of digital copyright platforms to a certain extent due to its decentralized, non-falsifiable and traceable features [10]. By writing the audio fingerprint, which is a unique feature of audio, into the blockchain, it is possible to achieve non-tampering and the source of piracy can be determined to solidify evidence and confirm rights. This provides a high level of security and integrity for audio copyright certification systems. Blockchain is a decentralized technology with no single central authority or administrator. This allows audio copyright certification systems to operate more autonomously and efficiently without relying on a central organization or third-party trust entity. Moreover, it provides a fully transparent recording and auditing mechanism that allows anyone to view and verify the integrity and authenticity of data.

Audio fingerprint retrieval technology can extract the unique digital abstract of audio, quantify the audio similarity, and make the similarity matching speed much faster. The combination of blockchain and audio fingerprint retrieval technology for digital copyright maintenance can simplify the process of audio corroboration and deposition with the characteristics of non-comparability and high credibility, which can protect the rights of digital content creators. The literature [11–13] designed a model of a digital copyright trading system based on the federated chain technology with the help of blockchain technology, which can guarantee the comparability and traceability of copyright information, but mainly focused on copyright trading and smart contract construction without paying much attention to copyright registration. The literature [14] designed a digital copyright protection and trading system based on blockchain technology, using the federated chain technology to provide the whole process of digital content copyright registration, query and trading, but the literature did not mention how to extract and retrieve audio feature values.

### *2.3 "Edge Computing + Blockchain" Model*

Essentially, blockchain is a new application model of computer technology, an innovative distributed database system that integrates cryptographic algorithms, consensus mechanisms, data transmission and other technologies [15]. Hyperledger Fabric is a representative of the Alliance Chain. Compared to Bitcoin and Ether, the advantage of Hyperledger Fabric is that there is no mining and corresponding power loss, and there is no blockchain currency creation. At the same time, due to the limited number of nodes in the Alliance Chain, the number of transactions (TPS) is greatly increased compared to the public chain, and all read and write operations on the blockchain data in the Fabric are required to be executed by smart contracts, which is more secure [16]. Blockchain has achieved significant results in various fields, such as the blockchain-empowered security and energy efficiency of drone swarm consensus for environmental exploration [17], as well as blockchain for decentralized multi-drone to combat COVID-19 [18].

Edge computing allows end devices to migrate storage and computing tasks to network edge nodes, such as base stations (BSs), wireless access points (WAPs), edge servers, etc., which meets the computing power scaling needs of end devices while effectively saving transmission link resources for computing tasks between cloud servers and end devices [19]. Bharany et al. [20] and colleagues introduced a configuration cluster of terminal devices to reduce the overhead of load balancing and congestion management purposes. Thousands of transaction information data generated by blockchain are continuously collected into the blockchain, burdening the blockchain network's computing resources and storage space. Moreover, since the edge computing platform is close to the user side, it reduces the communication latency compared to the data transmission to the cloud, and the propagation path is more controllable from the user's perspective. Optimization strategies can also be adapted to cache frequently used data such as ledger data, account status, and business data in the edge nodes to improve communication efficiency and reduce data transmission latency.

The decentralization, tamper-proof and anonymity features of blockchain technology provide a new trusted computing paradigm for edge computing systems, enabling them to achieve transaction authentication and information recording without trusted third parties in a distributed environment, which can guarantee the security of data in the process of collection, transmission, storage and calculation [21]. Zhang et al. [22] have also proposed a storage optimization scheme for a blockchain database in their research on improving the storage efficiency of the blockchain. Liu et al. [23] attempted to design a service mechanism from the perspective of game theory for the profit optimization of cloud service providers and their multiple users. The literature [24] proposed an efficient fault-tolerant technology for cloud computing. Kaur et al. [25] described a method of real-time migration of the database layer of an application hosted on any supported cloud to any implemented cloud data storage. Xiong et al. [26] proposed a prototype for using blockchain edge computing in resource-constrained devices to facilitate blockchain application scenarios using computing resources in edge computing mode. Yang et al. [27] proposed a framework for designing fully homomorphic cryptographic smart contracts in edge computing mode and demonstrated that edge computing mode could improve the efficiency of smart contract deployment. The literature [28] proposed a model of a digital copyright trading system under the federated chain model, which implemented two functions of copyright registration and copyright trading, but did not use the edge computing model, making the system less efficient.

## 3 Our Framework

### *3.1 Architecture Design*

In order to solve the problems of opaque information circulation, complicated deposition process, time-consuming and easy to tampered with and attacked in the current centralized audio copyright platform, this paper designed the MBE framework based on blockchain and edge computing mode. MBE framework adopts Hyperledger Fabric edge computing model architecture and makes use of blockchain's non-comparability, distributed storage, traceability and other features, as well as edge computing technology to optimize storage structure and computing efficiency. The framework can realize the functions of audio copyright deposit and registration, audio copyright transaction flow, copyright query, and user asset query. Audio fingerprint extraction is based on the Dejavu project's audio fingerprint extraction and retrieval method. The copyright deposit transaction function is based on a Fabric smart contract, a decentralized deposit transaction in the federated chain.

The basic architecture is shown in Fig. 1. MBE is divided into four layers: data layer, security layer, business layer and application layer, and each layer collaborates to guarantee the availability of the framework.

#### *3.1.1 Data Layer*

The framework's data storage structure and data organization adopts Hyperledger Fabric federated chain + local Mysql database storage architecture in edge computing mode. Each channel has a separate ledger and contract; only the same channel organization can share the ledger, while other organizations do not have access to the ledger [29]. We propose a novel approach to designing the data structure of transaction information within a smart contract. Specifically, we classify most non-organizational members of Fabric as edge nodes, which are situated outside the channel. We offload the deployment of smart contracts as well as the computation of CA user access node queries to edge computing nodes. By doing so, we aim to leverage the fixed local storage capacity of these edge nodes to expand the overall data storage capacity of the Hyperledger Fabric network.

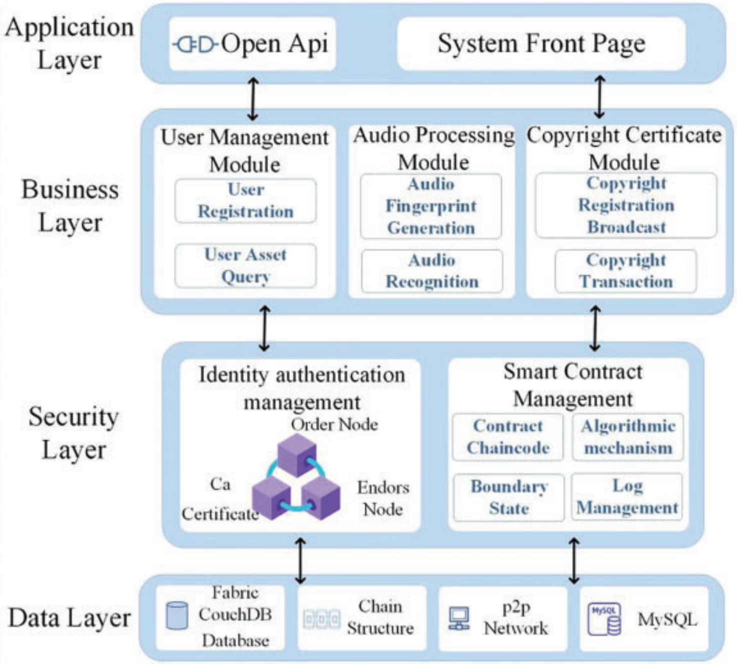


**Figure 1:** MBE hierarchy diagram

Fig. 2 shows the deployment diagram of the Fabric smart contract using the edge model. First, users can access the Fabric channels through the application layer Fabric-SDK by connecting to the Fabric with CA certificates granted by the CA nodes of the Fabric. Each Fabric channel contains three joined organizations, with a separate shared ledger and a separate smart contract. At this point, organizations 1, 2, and 3 in the same channel can be considered core nodes, and the remaining 1 to n nodes are edge nodes. The edge nodes access the local database without consensus algorithm verification and data synchronization transmission. The data inside the channel is the core data using edge computing to reduce the network burden of data transmission.

### *3.1.2 Security Layer*

The security layer is divided into an authentication module and a smart contract module. Hyperledger Fabric, a permission-based federated chain, usually uses digital certificates and other security mechanisms to enhance security, so the possibility of malicious nodes is small. The complexity and cost are reduced by using the distributed crash fault-tolerant consensus algorithm Raft, which ensures that the system can still process client requests in case of non-Byzantine failure of some nodes in the system [30]. MBE's information security, decentralization and tamper-evident characteristics are guaranteed by decentralized CA nodes, the Raft consensus algorithm and by performing modules such as system node division.

As the MBE framework adopts an edge computing mode, processing and storage of audio fingerprint information are distributed across multiple edge nodes. This ensures that even if some nodes fail or are attacked, it will not affect the normal operation of the entire system. In addition, since the MBE framework is based on the Fabric blockchain system, it also inherits Fabric's consensus mechanism and smart contract functionality, which can ensure the consistency and correctness of audio fingerprint information, as well as the credibility and verifiability of copyright ownership information. Therefore, the MBE framework can resist network failures and malicious attacks to a certain extent, improving the reliability and stability of music copyright certification systems.

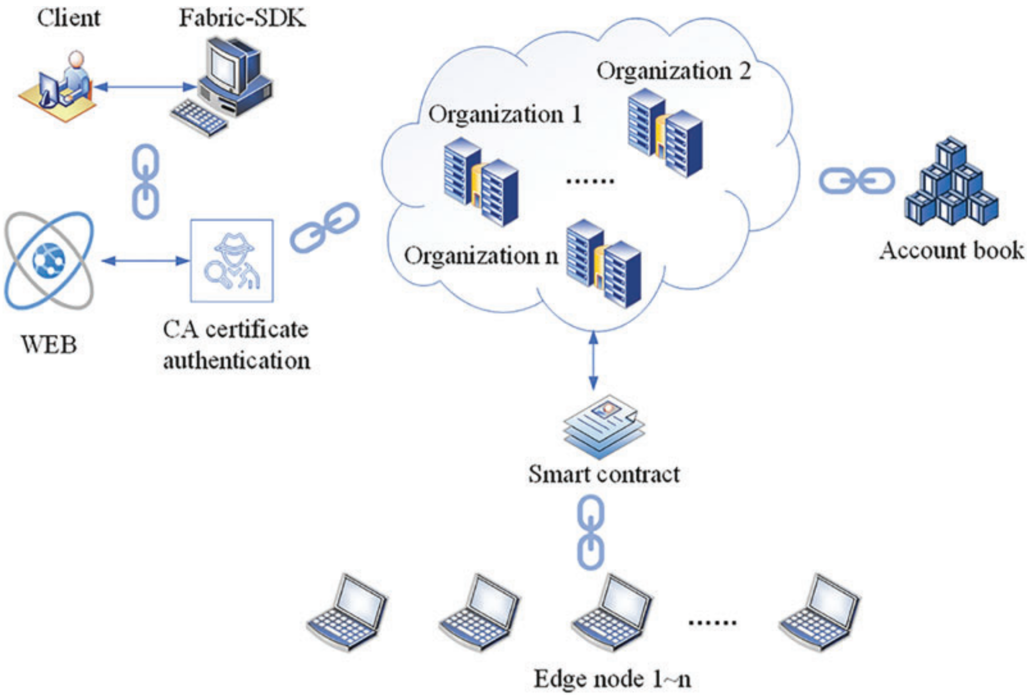


**Figure 2:** Smart contract deployment in edge computing mode

### *3.1.3 Business Layer*

The business layer is divided into three modules: user management module, audio processing module and copyright storage module, among which the audio processing module and copyright storage module are the core of MBE. The user management module is used for registering user nodes in the alliance chain, user login, issuing corresponding digital certificates to users and obtaining corresponding user rights. The audio processing module is used for music authors to upload audio and generate audio fingerprints using the Dejavu audio fingerprint extraction method. The copyright storage module invokes the Fabric smart contract to compare the uploaded audio fingerprint with the audio fingerprint in the Fabric distributed database, register and store the copyright, and trade the copyright after a successful registration.

### *3.1.4 Application Layer*

The application layer interacts with the system through front-end pages and restful service interfaces and sends user registrations, queries and other requests to the business layer modules for processing.

## ***3.2 MBE Deposition Process***

The framework operation flow is shown in Fig. 3. This framework distinguishes two types of users, namely administrators and ordinary users. The former are responsible for system management, including the deployment and review of new smart contracts, while the latter becomes user nodes upon successful registration. Ordinary users can upload original audio content to the system's audio deposition platform. To this end, the system invokes the Dejavu audio fingerprint extraction method, which stores the original audio content and extracts audio fingerprints for local Mysql database backup. Following this, the audio fingerprints are uploaded to the Fabric distributed database for fingerprint retrieval comparison. In the event that a matching fingerprint is found, the audio content is copied and registered. Conversely, if no identical fingerprint exists, the audio content is deemed original, and the system records the user information and audio fingerprint information, returning successful copyright registration information to the user, which is counted as their assets. Upon the establishment of user assets, the copyright may be traded.

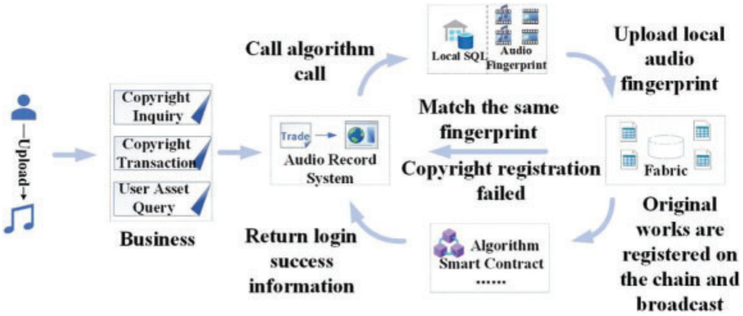

Upload
Copyright Inquiry
Copyright Transaction
User Asset Query
Business
Call algorithm call
Trade
Audio Record System
Local SQL
Audio Fingerprint
Upload local audio fingerprint
Match the same fingerprint
Copyright registration failed
Fabric
Original works are registered on the chain and broadcast
Return login success information
Algorithm Smart Contract ......

**Figure 3:** System flow chart

### *3.3 Audio Fingerprint Retrieval Technology in MBE*

The generation and retrieval of audio fingerprints are the keys to the success of audio copyright deposition. Audio fingerprinting is a technique used to identify a specific audio track by analyzing its unique acoustic features, such as the spectral shape and amplitude of its frequency components [31]. Fig. 4 shows the flowchart of audio recognition based on audio fingerprinting. The audio fingerprint retrieval algorithm consists of audio fingerprint feature extraction and audio fingerprint feature matching. Audio fingerprint feature extraction mainly includes preprocessing, windowing, filtering quantization and other processes. Audio fingerprint feature matching mainly includes a series of processes, such as hash table retrieval and matching [32].

The specific implementation process of audio fingerprint recognition technology is as follows. First, the original audio is sampled digitally. The original audio is digitally decoded to obtain multiple channels of audio signals. A first-order digital filter is used to pre-emphasize the features of the audio signal to improve the high-frequency part and make the spectrum flat for easy analysis [33]. The channel is sampled using the Nyquist-Shannon theorem (in order to recover the analog signal without distortion, the sampling frequency should be greater than or equal to two times the highest frequency in the analog signal spectrum, see Eq. (1)).

$$\text{Samples per sec needed} = \text{Highest-Frequency} * 2 = 22050 * 2 = 44100 \tag{1}$$

Commonly used symbols are given in Table 1. Framing and windowing are performed on each described audio signal to obtain multiple framed and windowed audio signals. Since the amplitude of the audio signal changes continuously with time, it is necessary to perform the framing process, by which the characteristics of the audio signal can be kept largely unchanged over time. As in Eq. (2), the framing process is a windowing function, and the windowing function w(n) is multiplied by the signal function x′(n) to form the windowed audio signal x(n).

$$x(n) = x'(n) * w(n) \tag{2}$$

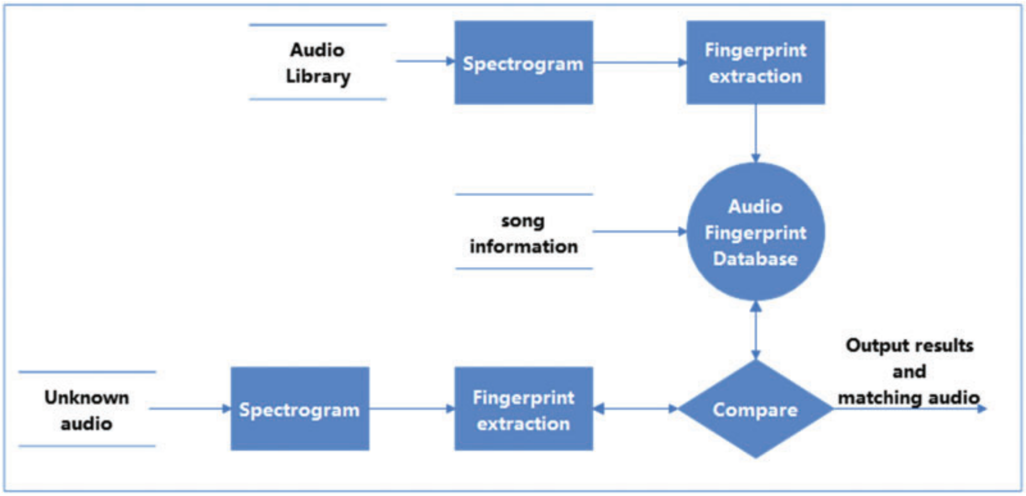


**Figure 4:** Fingerprint-based audio recognition framework diagram

**Table 1:** Commonly used notations

| Symbol | Definition |
|---|---|
| x′(n) | Signal function |
| x(n) | Windowed audio signal function |
| w(n) | Window function |
| f(x) | FFT function |
| a0 | The average value of the function f(x) over the interval [0, L] |
| an | The cosine coefficient of the function f(x) over the interval [0, L] |
| bn | The sine coefficient of the function f(x) over the interval [0, L] |

The audio signal is framed, windowed and then FFT (Eq. (3)) for each frame, after which the results of each frame are stacked along another dimension to obtain a graph (similar to a two-dimensional signal) whose amplitude is a function of time and frequency. This graph is the spectrum of audio as a two-dimensional coordinate graph, with the horizontal axis representing time(s) and the vertical axis representing frequency f(Hz), and the value of the coordinate point is the magnitude of the audio signal. The frequency and time values are discrete, while the amplitude is real-valued [34]. Suppose we color the actual value of the amplitude at the discrete (time, frequency) coordinates (higher for yellow bias and lower for green bias). In that case, an example of an audio sonogram and spectrogram is shown in Fig. 5.

The FFT can be repeated within a small time window in a song sample to create a spectrogram of the audio.

$$f(x) = a_0 + \sum_{n=1}^{\infty} \left( a_n \cos \frac{n\pi x}{L} + b_n \sin \frac{n\pi x}{L} \right) \tag{3}$$

We define a peak as a (time, frequency) pair, where the peak is the largest amplitude value in its local “neighborhood”. Other (time, frequency) pairs around it have lower amplitudes and are likely to survive in the noise. Once we have the audio spectrum, we can use the image processing toolkit to find the peaks and extract the local maxima, or peak points, that make up the maxima coordinate map. There are many peak points in the coordinate graph, and since the peak points are discrete and prone to collision, different songs can and probably will emit the same peak. So we combine each peak point with other peak points in the domain and use the hash function to obtain the fingerprint hash [35]. The fingerprint hash is generated by selecting a peak in the target domain as an anchor point in the spectrogram according to a certain density criterion, and each anchor point is sequentially paired with a peak point in its target domain.

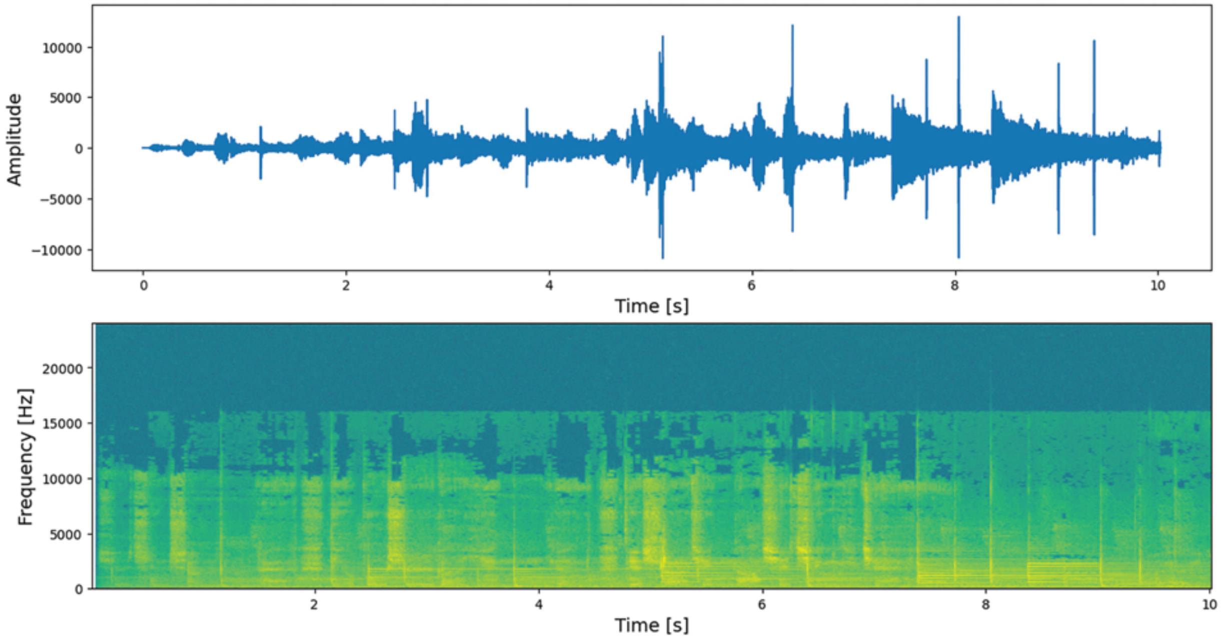


**Figure 5:** Test audio sonogram and spectrogram

The process involves utilizing the amplitude maxima of the spectrogram and amalgamating the frequencies of these maxima along with the time difference between them, where the time difference is the duration between two consecutive maxima. By generating a hash in the form of (frequencies of peaks, time difference between peaks) = fingerprint hash value, a unique fingerprint of the song can be represented over time. Each song has a different number of audio fingerprints (because the length of the audio is different and the number of peak points is different). We set a similarity threshold for audio fingerprints. If the number of fingerprints of the uploaded audio and the registered audio exceeds the threshold we set, the music is judged to be the same as the registered music, and the registration fails.

### *3.4 Copyright Depository and Trading Module in MBE*

#### *3.4.1 Copyright Registration*

After the audio fingerprint recognition algorithm gets all the fingerprints of the uploaded audio, it enters the deposition process. Fabric's smart contract code will upload the audio fingerprint information generated in the user's local MySQL database and compare it with the registered audio fingerprint information already stored in Fabric's distributed database for similarity. If the number of similarities between the user's uploaded audio fingerprint and the registered audio fingerprint does not exceed the similarity threshold we set, then it is not judged as plagiarism, and the registration is successful; on the contrary, it is judged as pirated audio and the registration fails.

Algorithm 1 is the core code of the copyright registration smart contract. First of all, we need to register the copyright information of the song: audio name, copyright owner’s name and ID, music author’s name and ID, and the space occupied by the song. The error message is output when the song copyright information is incomplete (lines 2–3). Then the song copyright information is converted to JSON transfer format. The API is called to store the song copyright information and the audio fingerprint of the song together (lines 4–7). It is worth noting that the system encapsulates the audio fingerprint of the song in the form of key-value pairs with the song ID in one-to-one correspondence, and the block information, such as copyright update time and transaction timestamp is entered by the system in a unified manner.

After the copyright registration is successfully registered in the MBE system, the system will automatically count the copyright owner’s user assets (Owner. Assets), a collection of audio copyright information owned under the copyright owner’s name.

**Algorithm 1:** Copyright Depository Smart Contract Pseudo-Code

```
Input: arguments (song_name, authorID, author_name, ownerID, owner_name, size)
Output: Transaction success or failure message
1.  begin
2.  if $len(argument) < 6$
3.    return Error(“Incorrect number of arguments.”)
4.  Json.Marshal (arguments) —> copyrightjson
5.  APIstub.putState (hash,copyrightjson) —> err
6.  if err! = nil
7.        return Error(“stub. PutState err.”)
8.  end if
9.  return message(“Registration has been successfully completed.”)
10. end
```

### 3.4.2 Copyright Transactions

The audio registered and deposited in MBE can then be transferred with others for copyright transactions. The system uses Fabric federation chain smart contracts to realize copyright transactions between users and has the characteristics of tamper-evident, traceable, and fast transaction information [36]. Compared with the traditional copyright transaction process, the MBE system has a short transaction cycle and can support cross-border transactions with high trustworthiness.

The copyright transaction process is shown in Fig. 6. The transaction is carried out between each user node without any third party, which guarantees the privacy and security of the transaction. Users can search for their favorite music to buy its copyright, and the transaction information consists of user IDs, author IDs, transaction amounts, and copyright update timestamps of both sides of the purchase, which are recorded in the Fabric smart contract. The smart contract transaction information is broadcasted through the Fabric alliance chain P2P network, and the order node will verify and sort the transaction and write it into the alliance chain block information to complete the uploading, and the copyright transaction information cannot be modified once the verification is completed and broadcasted.

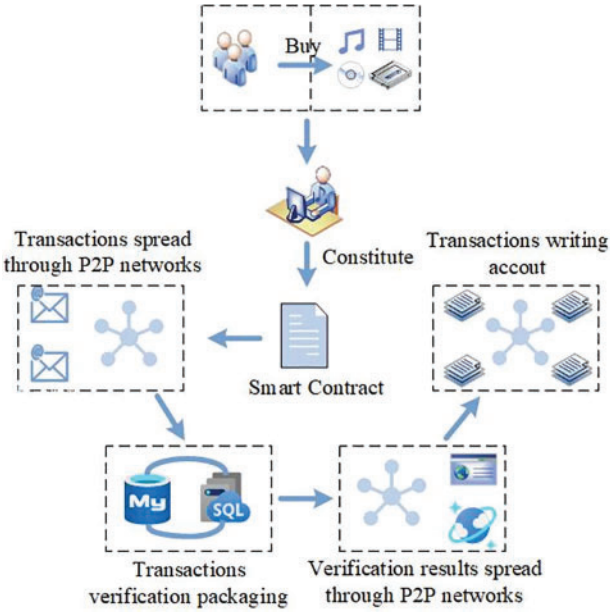

Buy
Constitute
Transactions spread through P2P networks
Transactions writing accout
Smart Contract
My SQL
Transactions verification packaging
Verification results spread through P2P networks

**Figure 6:** Flow chart of copyright transaction

## 4 Testing and Analysis

We developed a prototype system based on Hyperledger Fabric to validate the effectiveness of the proposed smart contract for audio deposition in edge mode. The system runs on an Ubuntu 20.04 (64-bit) virtual machine, i7-11370H @ 3.30 GHz processor, 16G RAM and 8 G RAM.

### *4.1 Audio Registration Time Test*

To assess the efficacy of the Dejavu-based audio fingerprint retrieval algorithm proposed in this study, we randomly selected 45 songs from the Internet to form a test set, which consisted of 971 MB of audio data in the WAV format and sequentially numbered from 1 to 45. This selection process was implemented to ensure the representativeness and diversity of the test data.

Among these 45 audio tracks, the size of space occupied by each music track and the number of extracted feature fingerprint hashes consumed storage space on the Mysql database is shown in Figs. 7 and 8. It can be seen that the number of audio fingerprint hash generated for different audio with different time length and melody is different, and the average number of hash is 13000.

We sequentially registered 45 test audios in the MBE system, and the total registration time and audio similarity audio fingerprint extraction time required for consumed storage space for each piece of music is shown in Fig. 9.

a) The average extraction time of all audio fingerprints is 4.74 s, which is basically positively correlated with the number of audio fingerprints in Fig. 10.
b) From Fig. 10, we can see that the similarity comparison between audio fingerprints is the main factor of the registration time of a piece of music, which is close to the total time spent on audio copyright registration. The length of fingerprint matching is related to the number of registered audio and shows some fluctuations.

c) As we can see, the registration time of music increases slowly with the increase of the number of registered audio, and the average registration time is 32.53 s, i.e., the total registration time of the next music increases slowly when the data in the copyright information database increases with the confirmation of one music.

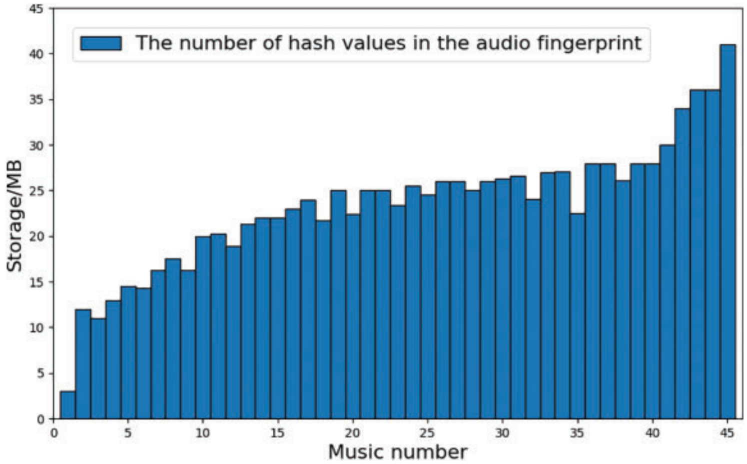


**Figure 7:** Audio storage space size

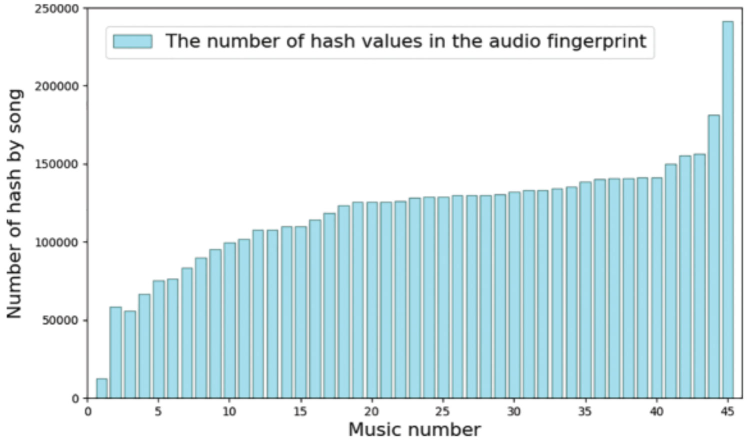


**Figure 8:** Number of audio hashes extracted

The test results show that the audio retrieval method can meet the system needs of MBE. A classical implementation method based on audio information retrieval is the global information-based method proposed by the Philips Institute in the Netherlands, namely Philips Robust Hash, or PRH. The utilization of the hash table in the Philips audio retrieval algorithm is very low, on the one hand, because the number of fingerprints is much smaller than the length of the hash table; on the other hand, because of the uneven distribution of hash values caused by [37]. We used two methods to extract 45 music tracks from the entire audio test set. It should be noted that the performance of the algorithm may be affected by the quality and quantity of different audio datasets, external factors, and environmental conditions such as noise levels. The data for this experiment was measured uniformly across the aforementioned audio datasets under the same environment and equipment. It can be clearly seen from Fig. 10 that the extraction fingerprint method used in this paper consumes substantially less time than the PRH hash fingerprint method.

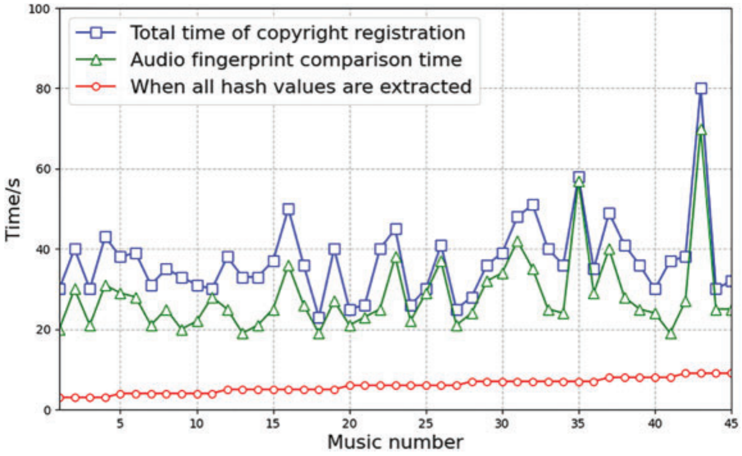


**Figure 9:** Testing audio copyright registration time consuming

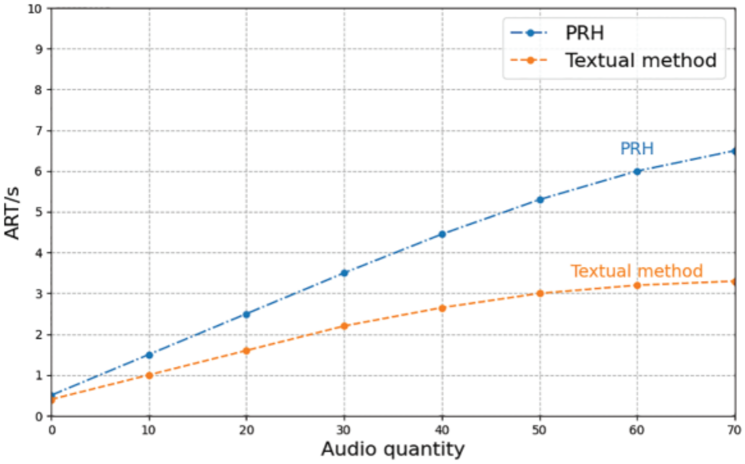


**Figure 10:** Time comparison between the audio fingerprint extraction method and the PRH method

The advantage of the Dejavu audio fingerprint retrieval method is that there is no need to keep the global information in the frequency spectrum, and the feature point storage space is less than that of PRH (Philips Robust Hash), which greatly reduces the user's waiting time and achieves the extraction of audio fingerprints with high efficiency.

### *4.2 System Performance Testing*

The main function of the edge-end node to implement cross-channel query transactions is that it has the chain code and ledger in the local and core channels and the local chain code and ledger are encrypted and operated in a system-native way. The transaction data implemented at the local node is stored locally and has high efficiency [38]. We tested the audio deposition system with and without the edge computing mode. After adopting the edge computing model, there are two organizational nodes in the channel. Each group contains a peer node (Peer0.org1.example.com and Peer0.org2.example.com), a special CA node for accessing certificates, and a CouchDB node to enhance security for compliance and data protection in the blockchain system. The blockchain network is composed of peer-to-peer nodes, each of which can keep a copy of the ledger and a copy of the smart contract. Therefore, the input and output of transactions are mainly controlled by the peer nodes, as shown in Table 2.

**Table 2:** Experimental node configuration

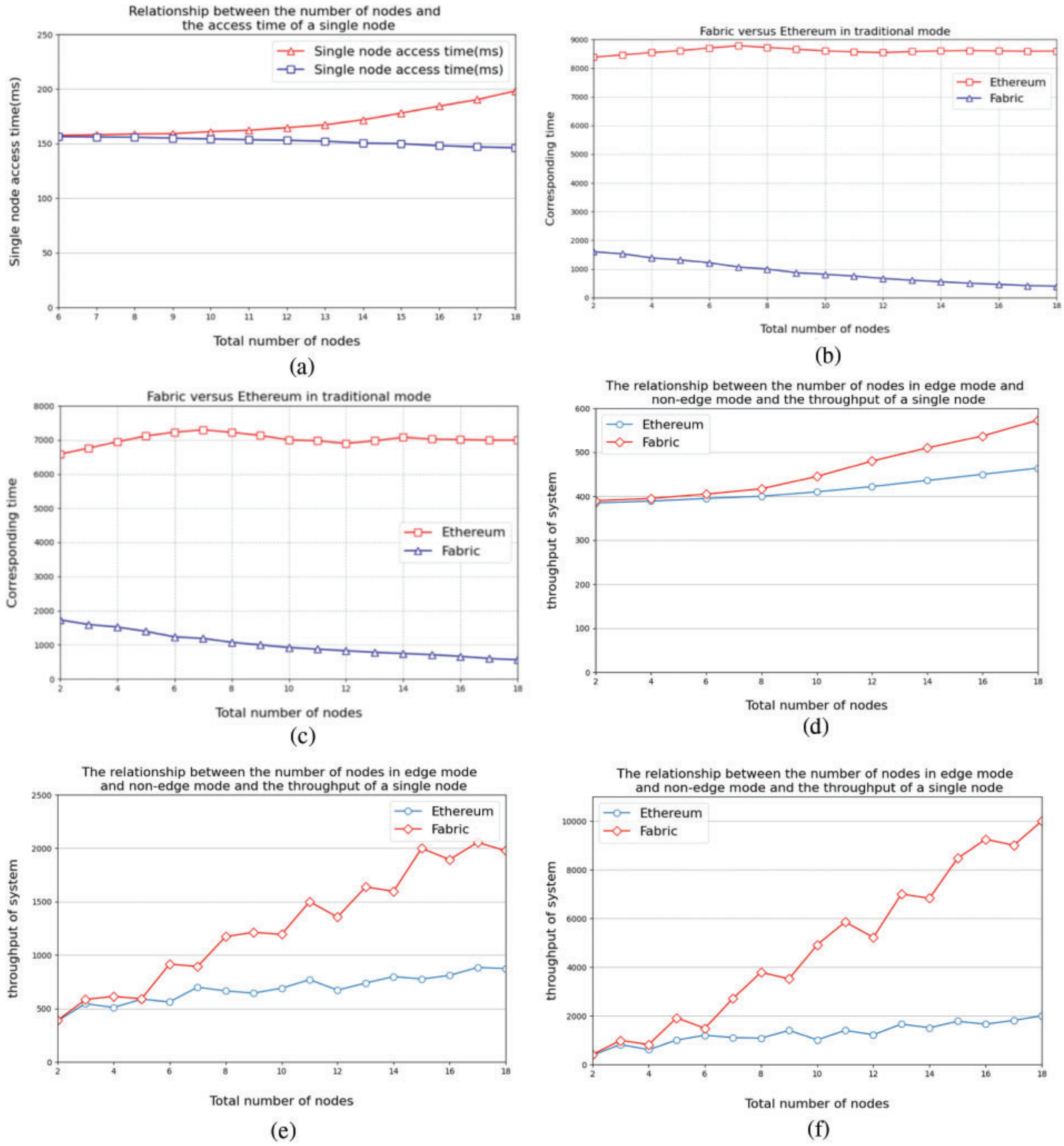
| Name | Memory (max) | Traffic in (KB) | Traffic out (KB) | Disc out (KB) | Disc write (KB) |
|---|---|---|---|---|---|
| Peer0.org1.example.com | 264.4 MB | 717.6 | 468.7 | 536.0 | 704.0 |
| Peer0.org2.example.com | 266.4 MB | 719.1 | 512.2 | 860.0 | 704.0 |
| Ca.org1.example.com | 15.5 MB | 0 | 0 | 0 | 0 |
| Couchdb.org1.example.com | 90.5 MB | 181.5 | 297.7 | 296.0 | 260.0 |
| Ca.org2.example.com | 7.9 MB | 0 | 0 | 0 | 0 |
| Couchdb.org2.example.com | 92.9 MB | 301.7 | 301.7 | 156.0 | 272.0 |
| Order.example.com | 31.9 MB | 819.1 | 819.1 | 548.0 | 508.0 |

We first store 1000 transaction information data, 200 of which are stored in the Fabric channel ledger and 800 at the edge. The number of nodes at the edge increases from 2 to 4, 6, 8, 10, 12 and 14, and then all nodes jointly initiate random access to the prototype system. The single-node access time is the total access time divided by the total number of query nodes. Controlled experiments are designed to test the single-node *vs*. multi-node response time and throughput of the Fabric federated chain with the edge computing model proposed in this paper *vs*. the non-edge computing Fabric federated chain and the three blockchain frameworks of Ether, and the experimental results are shown in Fig. 11.

Figs. 11a–11c show the experimental tests of the number of blockchain nodes *vs*. response time between the three systems. Fig. 11a shows the graphs of the number of nodes *vs*. single-node access time in edge and non-edge computing modes. When the total number of nodes is higher than 10, the access time of the Hyperledger Fabric network in non-edge computing mode increases significantly when it needs to carry more computational data volume and a larger database, and the network experiences latency and shortage of computational resources. With a total of 18 nodes and 14 edge nodes, the system's single-node access time is only 126.21 ms. However, in non-edge computing mode, the single node access time reaches 238.14 ms. This means that using edge computing mode improves efficiency by 53% compared to non-edge computing mode.

Fig. 11b shows the graph of the number of nodes *vs*. the access time of a single node under the traditional model of Hyperledger and Ether. As both use different consensus algorithms the super ledger uses the Kalfka algorithm, and the number of nodes and response time are inversely proportional, while the core problem of slow Ethernet is still PoW and the size of data blocks.

Fig. 11c shows the comparison graph of the number of nodes under the edge computing model Fabric and Ether and its system single node access time. In the case of 18 nodes and 14 edge nodes, the single node access time of the system is only 139.68 ms, while in the non-edge computing mode, the single node access time reaches 208.87 ms, which means that the efficiency of the edge computing mode is 53% higher than that of the non-edge computing mode. This is because, in edge computing mode, the edge nodes store the transaction data information occurring at the edge in the local database greatly expanding the whole system's storage space.



(a)

(b)

(c)

(d)

(e)

(f)

**Figure 11:** Response time and throughput of fabric edge computing mode *vs*. other modes

Figs. 11d–11f are the tests of single-node throughput of blockchain among the three systems. Fig. 11d shows the graphs of the number of nodes in edge mode and non-edge mode *vs*. single node to system throughput. In this equation of throughput: F = VU ∗ R/T. It shows that the throughput F is a function of the number of VUs, the number of requests R made by each user, and the time T, where R can be calculated in terms of time T, and the user thinks time TS: R = T/TS.

Fig. 11e plots the number of nodes *vs*. single node *vs*. system throughput for Fabric and Ethernet in traditional mode. The difference between the two under different consensus algorithms can be seen, and the transaction speed of the Fabric federation chain is better than that of the Ethernet public chain.

Fig. 11f shows the graph of the number of nodes *vs*. single node to system throughput under edge computing models Fabric and Ethereum. The TPS of Fabric is around 10000, and the average transaction confirmation speed is around several hundred milliseconds. The blockchain of Ether produces a block every 12 s, and the time for a transaction to be verified as valid is also about 12 s; subject to the single thread of CPU, its TPS is around 2000, which is difficult to meet the demand of some commercial scenarios of high-frequency transactions.

Based on the experimental data presented above, it is evident that the Fabric alliance chain with edge computing mode exhibits superior response time compared to the traditional Fabric alliance chain and Ethernet public chain. Moreover, with an increase in the number of nodes, the transaction throughput of the Fabric alliance chain with edge computing mode surpasses that of the other two chains. In essence, the proposed audio copyright deposit system that employs the "Fabric alliance chain + edge computing mode" blockchain architecture performs better than the traditional Fabric alliance chain and Ethernet public chain systems, as it optimizes the bandwidth utilization of each node in the alliance chain, allowing for effective transmission of information and high transaction throughput, while satisfying system requirements.

## 5 Conclusion

We present a novel audio copyright deposition framework based on integrating audio fingerprint retrieval, blockchain technology, and edge computing. Results of our experimental evaluation demonstrate that the implementation of the Fabric federated chain in this framework results in a 53% improvement in performance and meets the required transaction throughput. Our framework effectively resolves issues of unclear copyright attribution, complex deposition processes, long cycle times, and centralization present in existing audio copyright deposition systems. The proposed framework is non-comparability, traceable, and simple to use. In future research, we plan to increase the number of experiments to investigate the effects of different datasets, noise levels, and sensor layouts on the accuracy and robustness of the algorithm. We will optimize and test the performance of this framework on larger audio datasets to better adapt it to practical applications. Additionally, we would like to explore the possibility of further integrating artificial intelligence techniques, such as machine learning and deep learning, into the framework to improve its performance and accuracy.

**Acknowledgement:** We thank the editors and reviewers for their comments, which have helped a lot to improve the quality of the manuscript.

**Funding Statement:** This work is supported by Jiangxi Provincial Natural Science Foundation under Grant Nos. 20224BAB212015, 20224ACB202007, Jiangxi Province Science and Technology Project (03 Special 5G Project) under Grant No. 20224ABC03A13, the Foundation of Jiangxi Educational Committee under Grant No. GJJ210338, the National Natural Science Foundation of China (NSFC), under Grant No. 61962026.

**Author Contributions:** The authors confirm their contribution to the paper as follows: conception and design of the framework: Jianmao Xiao, Ridong Huang; experimental design: Jianmao Xiao, Jiangyu Wang; data collection: Ridong Huang, Zhean Zhong; analysis and comparison of results:

Jianmao Xiao, Chenyu Liu, Yuanlong Cao; fund support: Yuanlong Cao, Chuying Ouyang. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** As the research is supported by a third-party organization, we are currently unable to provide access to the data and materials due to security concerns and constraints imposed by confidentiality agreements.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] M. Y. Fan, G. B. Zhang and T. C. Yao, “Exploring the copyright protection of digital music under the perspective of blockchain,” *Industry and Technology Forum*, vol. 21, no. 10, pp. 28–31, 2022.

[2] Y. F. Lv, X. J. Shen, J. I. Yang and W. Q. Zang, “A review of digital copyright protection based on blockchain technology,” *Remote Sensing Science: Chinese and English Edition*, vol. 7, no. 1, pp. 10, 2019.

[3] N. A. Sulieman, L. R. Celsi, W. Li, A. Zomaya and M. Villari, “Edge-oriented Computing: A survey on research and use cases,” *Energies*, vol. 15, no. 2, pp. 15, 2022.

[4] X. Wang, “Observation and thinking of digital music industry—analysis based on streaming music,” *Arts Studies and Criticism*, vol. 3, no. 1, pp. 41–43, 2022.

[5] Frabboni and M. Mecedes, “Collective management of music rights: A test of competition and industrial organisation theories,” Ph.D. Dissertation, Queen Mary, University of London, England, 2009.

[6] S. Bilonikar, C. Mendonca, D. Phadakale and M. Shetty, “Blockchain based model for royalty payments of artists and RemixMakers,” in *Proc. of ICSMDI*, India, pp. 121–132, 2021.

[7] Y. Zeng, “Digital music resource copyright management mechanism based on blockchain,” in *Proc. of the 2020 3rd Int. Conf. on Smart BlockChain (SmartBlock)*, Zhengzhou, China, pp. 158–162, 2020.

[8] Y. D. Liu, W. Li, X. Q. Li, Z. R. Wang and R. Feng, “Compression domain robust music fingerprinting algorithm study,” *Journal of Electronics*, vol. 38, no. 5, pp. 5, 2010.

[9] I. D. León and R. Gupta, *The Impact of Digital Innovation and Blockchain on the Music Industry*. US: Inter-American Development Bank, 2017.

[10] A. Gervais, G. O. Karame and K. Wüst, “On the security and performance of proof of work bockchains,” in *Proc. of the ACM SIGSAC Conf. on Computer & Communications Security*, New York, NY, USA, 2016.

[11] C. Li, B. R. Dai, H. J. Wang and X. Q. Wang, “Blockchain-based digital copyright protection and transaction system,” *Modern Computing: Midterm Journal*, vol. 1, no. 10, pp. 5, 2018.

[12] Z. Chen, Q. Li, J. Gan, C. Zhang and Z. R. Li, “VC chain: A federated audio and video copyright blockchain system,” *Computer Engineering and Science*, vol. 41, no. 11, pp. 10, 2019.

[13] D. K. Hu, Z. I. Li and W. Zhou, “Blockchain-based digital copyright authentication model,” *Computer Applications and Software*, vol. 38, no. 2, pp. 311–317, 2021.

[14] L. Li, S. Q. Zhou, Q. Liu and D. B. He, “Blockchain-based digital copyright trading system,” *Journal of Network and Information Security*, vol. 4, no. 7, pp. 8, 2018.

[15] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[16] E. Androulaki, Y. Manevich, S. Muralidharan, C. Murthy and G. Laventman, “Hyperledger fabric: A distributed operating system for permissioned blockchains,” in *IEEE Symp. on Security and Privacy Workshops (SPW)*, Porto, Portugal, 2018.

[17] J. Li, “Incentivizing resource cooperation for blockchain empowered wireless power transfer in UAV networks,” *IEEE Transactions on Vehicular Technology*, vol. PP, no. 1, pp. 1, 2020.

[18] Z. Xiao, Y. Chi and F. Liu, “The application of blockchain technology in the national emergency management system under COVID-19,” *Social Science Electronic Publishing*, vol. 1, no. 1, pp. 1, 2021.

[19] J. I. Zhang, Y. C. Zhao, B. Chen, F. Hu and Z. Kun, “A review of research on data security and privacy protection in edge computing,” *Journal of Communication*, vol. 39, no. 3, pp. 21, 2018.

[20] S. Bharany, S. Sharma, N. Alsharabi, T. E. Elsayed and N. A. Ghamry, “Energy-efficient clustering protocol for underwater wireless sensor networks using optimized glowworm swarm optimization,” *Frontiers in Marine Science*, vol. 10, pp. 6945, 2023.

[21] C. Esrosito, A. Castiglione, F. Pop and K. Choo, “Challenges of connecting edge and cloud computing: A security and forensic perspective,” *IEEE Cloud Computing*, vol. 4, no. 2, pp. 13–17, 2017.

[22] J. Zhang, S. Zhong and J. Wang, “A storage optimization scheme for blockchain transaction databases,” *International Journal of Computer Systems Science & Engineering*, vol. 1, no. 1, pp. 36, 2021.

[23] C. Liu, K. Li and K. Li, “A new service mechanism for profit optimizations of a cloud provider and its users,” *IEEE Transactions on Cloud Computing*, vol. 1, no. 1, pp. 1, 2017.

[24] S. Bharany, S. Badotra, S. Sharma, S. Rani, M. Alazab *et al.,* “Energy efficient fault tolerance techniques in green cloud computing: A systematic survey and taxonomy,” *Sustainable Energy Technologies and Assessments*, vol. 53, no. 2, pp. 102613, 2022.

[25] K. Kaur, S. Bharany, S. Badotra, K. Aggarwal, A. Nayyar *et al.,* “Energy-efficient polyglot persistence database live migration among heterogeneous clouds,” *The Journal of Supercomputing*, vol. 79, no. 1, pp. 265–294, 2023.

[26] Z. Xiong, Y. Zhang, D. Niyato, Z. Han and P. Wang, “When mobile blockchain meets edge computing,” *IEEE Network*, vol. 32, no. 1, pp. 192–197, 2018.

[27] Y. T. Yang, T. X. Lin and J. Y. Chen, “Design of fully homomorphic cryptographic smart contracts in edge computing mode,” *Journal of Information Security*, vol. 7, no. 2, pp. 150–162, 2022.

[28] G. F. Zhao, Y. He and J. H. Zhou, “Blockchain-based digital copyright registration technology,” *Information Technology and Network Security*, vol. 38, no. 4, pp. 5, 2019.

[29] H. Sukhwani, J. M. Martinez, X. Chang, K. S. Trivedi and A. Rindos, “Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric),” in *Proc. of the 2017 IEEE 36th Symp. on Reliable Distributed Systems (SRDS)*, Hong Kong, China, 2017.

[30] C. Ma, X. Kong and Q. Lan, “The privacy protection mechanism of hyperledger fabric and its application in supply chain finance,” *Cybersecurity*, vol. 2, no. 1, pp. 9, 2019.

[31] M. L. Miller, M. A. Rodriguez and I. J. Cox, “Audio fingerprinting: Nearest neighbor search in high dimensional binary spaces,” *Journal of VLSl Signal Processing Systems*, vol. 1, no. 3, pp. 285–291, 2005.

[32] M. Zhang, J. Q. Ouyang, Z. Z. Li and W. Liu, “A fast method for specific audio fingerprint extraction,” *Computer Engineering*, vol. 36, no. 2, pp. 211–213, 2010.

[33] N. Jing, Q. Liu and V. Sugumaran, “A blockchain-based code copyright management system,” *Information Processing & Management*, vol. 58, no. 3, pp. 102518, 2021.

[34] C. Ouali, P. Dumouchel and V. Gupta, “A spectrogram-based audio fingerprinting system for content-based copy detection,” *Multimedia Tools & Applications*, vol. 75, no. 15, pp. 45–65, 2016.

[35] P. Cano, E. Batle, T. Kaler and J. Haitsma, “A review of algorithms for audio fingerprinting,” in *2002 IEEE Workshop on Proc. of the Multimedia Signal Processing*, VL, USA, 2003.

[36] A. Fc, B. Tkd and A. Cp, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and Informatics*, vol. 36, no. 7674, pp. 55–81, 2019.

[37] Y. Liu, K. Cho, H. Yun, J. Shin and N. Kim, “DCT based multiple hashing technique for robust audio fingerprinting,” in *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, Taipei, pp. 61–64, 2009.

[38] K. I. Wright, M. Martinez, U. Chadha and B. Krishnamachari, “SmartEdge: A smart contract for edge computing,” in *Proc. of the 2018 IEEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, pp. 1685–1690, 2018.