ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Scheme Design of Blockchain Technology for Copyright Protection and Cyber Threat Defense in Music Performance Industry

Xingnuo Du[1,*]

[1] Department of Performing Arts Management, The Graduate School of Culture Technology, Sangmyung University, Seoul, 110-744, Republic of Korea

SUMMARY: *The conventional copyright safeguarding system for digital music suffers from a variety of issues. These include susceptibility to assaults, an extended duration of copyright protection, and a lack of data storage security. As a result, this study utilizes blockchain technology for music copyright protection. It devises a plan for copyright safeguarding and network threat defense within the music performance sector. In this article, the music copyright protection and transaction system is established via the consortium chain, IPFS, and the Shazam algorithm, DWT digital watermarking technology and improved consensus algorithm. The music copyright registration time increase of this system is about 1.948s, and the space occupied by the feature fingerprint of each piece of music on IPFS is about 8.05MB, and the improved consensus algorithm shows better fault tolerance and throughput, and the average value of throughput reaches 1251TPS, which is higher than that of the comparison consensus algorithm. The experiments show that the proposed music copyright protection and transaction system has good performance and high security, Moreover, it can achieve the reliable verification of digital music copyright and the safe preservation of transactions.*

KEYWORDS: *blockchain; Shazam algorithm; IPFS; consensus algorithm; music copyright protection*

1 Introduction

In the wake of the digital age, the music performance sector has undergone substantial transformations. Copyright safeguarding has long stood as the fundamental concern within the music performance industry. This matter is significant as it pertains not only to the lawful claims and interests of composers but also to the long - term viability of the entire industry [1, 2]. However, under the current wave of digitization, the issue of music copyright appears to be particularly complex and severe. The widespread adoption of the Internet and digital technologies has led to an incredibly swift and far - reaching dissemination of musical works. However, it has also given rise to a high frequency of copyright infringements and cyber threats [3]. Therefore, the exploration of solutions for copyright protection and network threat defense to safeguard the legitimate rights and interests of music creators has become an immediate issue that needs to be addressed in the present day.Blockchain technology, founded on the concept of decentralization, stores and validates information in the form of a distributed ledger. It is characterized by resistance to tampering and the elimination of intermediaries[4-6], These features endow it with significant potential in the areas of copyright protection and cyber threat defense within the music performance industry.

*duxingnuo1992@163.com
https://doi.org/10.65102/is2026602
Published: 30 April, 2026

To begin with, the non - alterability of copyright data can be guaranteed by blockchain technology. In traditional copyright protection methods, the storage and verification of copyright information mainly rely on authoritative organizations or third-party platforms, which are susceptible to the threat of tampering and forgery [7, 8]. The decentralized nature of the blockchain's distributed ledger causes the storage and verification of copyright information to be spread across multiple nodes within the network, and no one can modify the information in the ledger individually, which realizes the network threat defense and ensures the security and authenticity of copyright information [9-11]. Secondly, blockchain technology can realize the automatic distribution and tracking of copyright proceeds [12]. With the help of technologies like intelligent contracts, the sales and utilization data of works can be documented on the blockchain. Additionally, the allocation of copyright revenues can be automatically achieved in accordance with the pre - set regulations [13, 14]. This approach not only significantly cuts down the expenses associated with distributing copyright earnings but also boosts the income level of copyright holders and stimulates creation and innovation.When it comes to the implementation of blockchain technology in copyright safeguarding and cyber threat countermeasures within the music performance sector, reference[15] delves into the utilization of deep generative adversarial networks in single - note melody composition and multi - instrument concerto arrangement. It also devises a digital music copyright protection system founded on blockchain and enhanced Byzantine fault - tolerant algorithms. Experimental results indicate that the proposed model surpasses the baseline in several performance indicators. Moreover, the system demonstrates a 0% error rate under high - concurrency conditions and exhibits outstanding transaction throughput. The fact that the system has a 0% error rate under high concurrency and excellent transaction throughput validates its practical application worth.Reference[16] highlights that the existing digital copyright protection systems suffer from issues such as centralization, time - consuming processes, high costs, and data isolation. To address these problems, it puts forward a secure and efficient copyright protection system based on blockchain and IPFS, which encompasses the entire process of rights verification, transactions, and traceability, and ensures security automation through encryption algorithms and smart contracts, and the test shows that the system can effectively solve the existing pain points. Reference [17] stressed that blockchain technology can offer legal and moral backing to the music industry in the areas of composition, dissemination, and copyright safeguarding, and sorted out 11 blockchain-driven industry functions by analyzing 89 resources, finding that 79.4% were based on the traditional blockchain and 28.2% focused on digital rights management, and pointing out that the trend is to reduce third-party dependence and increase revenue transparency. Literature [18] indicates that the current digital information piracy problem is serious, digital music copyright protection research is less, for its storage security is low, the right to confirm the cycle is long and other pain points, combined with blockchain technology to propose credible right to confirm the program, the experiment shows that the DPBFT algorithm used in the fault tolerance rate is higher, the average throughput reaches 1,249, which can satisfy the management system requirements and has practical value. Literature [19] argues that the deepening dependence of music creators on the Internet highlights the digital copyright protection problem, and proposes an efficient protection scheme that combines AI, Blockchain technology and cryptographic methods present an innovative model founded on Hyperledger Fabric and incorporating quantum homomorphic encryption, and converts music files into NFTs in order to activate the smart contract, and experiments show that this technique can effectively deal with the realistic copyright protection challenges. Reference [20] puts forward a music distribution model founded on blockchain and smart contracts. This model safeguards the integrity, confidentiality, and non - repudiation of assets by encrypting

music assets and disseminating them across nodes. It also mitigates the risk associated with a single point of failure. As a result, musicians can easily handle copyrights, and right - holders can automatically and immediately receive royalties. This ensures the security and transparency of music market transactions.Reference [21] points out that with the swift advancement of the Internet, online music has enriched people's spiritual lives. However, it has also presented a challenge to the safeguarding of intellectual property rights. To address this, it proposes a decentralized music copyright operation and management system based on blockchain technology. This system makes use of the shared ledger mechanism and smart contracts to effectively protect copyrights and balance the interests of multiple parties. It also promotes the sound development of the music industry and enhances the user experience. The suggested system leverages the shared ledger mechanism and smart contracts to achieve efficient copyright protection and the coordination of multiple interests, foster the healthy growth of the music industry, and improve the user's experience.

Moreover, the research in literature [22] puts forward a reliable music copyright safeguarding system that is founded on Ethernet, which generates content fingerprints through signal chunking and singular value decomposition, and queries the comparison in blockchain to achieve the dual goals of anti-attack and cross-platform protection, and the simulation results verify its superiority. Literature [23] reveals that music copyright protection in multimedia distribution networks is extremely challenging, Moreover, the majority of current watermarking techniques do not offer multi - layer embedding capabilities and require reliance on intermediate entities, based on this, a novel privacy protection mechanism combining blockchain and watermarking is proposed, which associates copyright information through specific watermarks and utilizes smart contracts to ensure the compliance of each entity, and simulation verifies its efficiency and scalability. Reference [24] presents a digital music copyright management system founded on the VNT chain. This system makes use of blockchain technology to guarantee data integrity. It employs the Shazam algorithm for originality verification and secures transaction safety via smart contracts. Experimental results indicate that the registration time of this system is extended by approximately 1.9 seconds, and the fingerprint data amounts to around 8MB, which achieves the expected performance of security, efficiency, and scalability. Literature [25] shows that the music industry has made significant technological progress, but the royalty payment system is lagging behind, and the existing improvements are fragmented and difficult to implement, and proposes an exploratory royalty distribution system, TARP, which covers the whole process of identity management, work registration, and authorization payment, and allows external interfaces, and the prototypes of Ether and SGX show that it can provide tangible improvements at a moderate cost. Literature [26] describes how unauthorized use of songs on digital platforms causes huge losses to creators every year due to weak tracking systems and data fragmentation,furthermore, it constructs an integrated data model relying on blockchain, application programming interfaces (APIs), and audio fingerprints. It fills regulatory loopholes via jurisprudential analysis and explores real - time tracking technologies to enhance the transparency of royalty distribution, achieving an accuracy rate of 85%,and strengthens the enforcement of digital evidence. Literature [27] points out that music blockchain platforms are changing the online music landscape, aiming to enable copyright holders to bypass intermediaries and transact directly with users in order to solve the historical problem of intermediary dominance, and analyzes the advantages and limitations of its application to improve the understanding of its actual potential in the industry. Reference [28] creates an end - to - end service spanning from copyright contracting to distribution. This is achieved by devising a blockchain - based technology for copyright contracting and distribution. The technology makes use of fundamental techniques like large - scale data

storage and rapid real - time transaction processing, aiming to provide creators and producers with a copyright protection and trust guarantee system that is transparent and reliable, and that supports secure personal transactions.

This research project focuses on the development of a system for safeguarding music copyright and facilitating its transactions. To enhance the security and efficiency of this system, a modified version of the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm is employed. Specifically, a reputation model is instituted, and a Pre - Commit stage is incorporated. This modification helps the system counteract Sybil attacks, curtails the communication volume among consensus nodes, and upholds the integrity of data.When it comes to the authentication and trading of digital music copyrights, the Shazam algorithm serves a crucial role. It is utilized to obtain music feature fingerprints, which are then stored in the InterPlanetary File System (IPFS), so as to realize the non-tampering and traceability of music copyrights, and to provide credible credentials for creators to defend their rights by utilizing the robustness and hiddenness of discrete wavelet transform watermarking technology. Subsequently, On VMware virtual machines, experimental trials are conducted to assess the fault tolerance and throughput of the enhanced consensus algorithm. Additionally, investigations are carried out to explore the system's time required for music copyright registration and the storage space utilized by the feature fingerprint on IPFS. The research on the music copyright protection and transaction system presented in this paper helps to clarify the issue of copyright attribution, improving the efficiency of copyright transaction, and simplifying the infringement proof procedure.

2 Key technologies

2.1 Blockchain technology

Blockchain is an ever - expanding distributed database that is collaboratively maintained by multiple participants within a distributed shared ledger (DSL). It is a novel application paradigm that integrates various computer technologies such as distributed data storage, peer - to - peer communication, consensus protocols, and encryption algorithms. Based on the level of openness and access rules of the blockchain, it can be classified into three types: public blockchain, consortium blockchain, and private blockchain.Blockchain technology is characterized by decentralization, immutability, and traceability. These technical features enable blockchain to have broader application prospects in the copyright protection of the music performance industry. Specifically, it can offer comprehensive protection for digital music copyright works across the entire lifecycle, including rights registration and verification, rights trading, as well as evidence gathering and rights defense.

2.2 Star File System

The Interstellar File System, known as IPFS, is a network communication protocol. It establishes a long - lasting and decentralized system for storing and sharing files. This protocol is crafted to rectify the limitations of the current Hypertext Transfer Protocol (HTTP).IPFS stores files in equal-sized chunks, then constructs hash values for each chunk and builds a file lookup table, which allows files to be stored in chunks on distributed servers. When searching for a file, you only need to enter the hash value returned when storing the file, and IPFS will automatically search and merge the file blocks to form the original file according to the file search table and the internal routing table.

2.3 Shazam's algorithm

The fingerprint of Shazam algorithm is based on the matching of energy peak points of the speech spectrogram and the whole algorithm is split into two segments:

The initial stage involves the extraction of features from the audio fingerprint. First these peak points (also called feature points) are found over the entire time-frequency length of the recording, which are converted to a set of sparse peak coordinates of the constellation, The horizontal axes represent the values of the audio in the time domain, while the vertical axes represent the values of the audio in the frequency domain. This is then followed by a fast combination of hashes. Each feature point and a subsequent peak point in the target rectangular region construct a feature point pair, and the current feature point is called an anchor point. Each anchor point corresponds to a rectangular target region, and the number of peak points within the target region and the anchor point constructing feature point pairs is called the number of outer links. Every anchor point is systematically paired with the apex points within the target area. This pairing yields two frequencies along with a time disparity. The dimensions of the target area can be modified in accordance with the real - world circumstances. Additionally, the quantity of external connections in the target area can be restricted to regulate the number of combined hash values. The combined hash produced in this way is highly reproducible, even if the noise is strong or the audio has been compressed.

The second part is audio fingerprint matching retrieval. All the hashes and time offset information need to be extracted from the recording samples before retrieval. The hashes extracted from the samples are matched with the hashes in the index, and when all the fingerprints extracted from the samples have finished matching, the time is scanned to get the correct song.

2.4 DWT Watermarking Algorithm

Based on the disparities in the embedding position of digital audio watermarking, it can be classified into two main types: time - domain digital audio watermarking and transform - domain digital audio watermarking. Time - domain digital audio watermarking involves directly altering the value of the sampling point within the time domain, so as to superimpose the watermarking information, the information embedded in this method is relatively large, but its robustness is poor, the typical algorithms are LSB algorithm and echo hiding algorithm. Transform domain digital audio watermarking algorithm refers to the original audio signal transformed to other domains, and then embed the watermark information into the transformed domain, common transforms include DFT, DCT, DWT. When comparing transform - domain digital audio watermarking algorithms with time - domain audio watermarking algorithms, the former demonstrate distinct advantages in terms of algorithmic robustness. The principle of discrete wavelet transform (DWT) is as follows:

Let $\varphi(t)$ be a square productable function, i.e., $\varphi(t) \in L^2(\mathbb{R})$, if its Fourier transform $\hat{\varphi}(\omega)$ satisfies Equation (1):

$$\int \frac{|\hat{\varphi}(\omega)|^2}{\omega} d\omega < \infty \tag{1}$$

where $\varphi(t)$ is a fundamental wavelet or wavelet mother function, and Eq. (1) is the admissibility condition for the wavelet function.

The scaling and translation of the wavelet mother function $\varphi(t)$, let its scale factor be α and its translation factor be τ, and let the function after it has been subjected to scaling and

translation be $\varphi_{\alpha,\tau}(t)$ as shown in Eq. (2):

$$\varphi_{\alpha,\tau}(t)=\alpha^{-\frac{1}{2}}\varphi\left(\frac{t-\tau}{\alpha}\right),\alpha>0,\tau\in\mathbb{R} \tag{2}$$

where $\varphi_{\alpha,\tau}(t)$ is a wavelet basis function that depends on the parameters α, τ. Since the values of the scale factor α as well as the translation factor τ are continuously varying, $\varphi_{\alpha,\tau}(t)$ is said to be a continuous wavelet basis function.

The scale factor α and translation factor τ in Eq. (2) are discretized by taking $\alpha=2^j$ and $\tau=2^kT_s$, then Eq. (2) can be expressed as Eq. (3):

$$\frac{1}{\sqrt{2^j}}\varphi\left(\frac{t-2^jT_s}{2^j}\right)=\frac{1}{\sqrt{2^j}}\varphi\left(\frac{t}{2^j}-kT_s\right) \tag{3}$$

Denote equation (3) as $\varphi_{j,k}(t)$, where $j,k\in\mathbb{Z}$. Then the t-axis is normalized by T_s, and we have the discrete wavelet function as shown in equation (4):

$$\varphi_{j,k}(t)=2^{-\frac{j}{2}}\varphi\left(2^{-j}t-k\right) \tag{4}$$

For any function $f(t)$, its discrete wavelet transform is Eq. (5):

$$WT_f(j,k)=\int_R f(t)\overline{\varphi_{j,k}(t)}dt \tag{5}$$

where $WT_f(j,k)$ is the discrete wavelet transform.

Assuming that the discrete wavelet sequence $\{\varphi_{j,k}(t)\}_{j,k\in\mathbb{Z}}$ forms a frame, so that the upper and lower boundaries of this frame are A and B, respectively, the inverse transform equation of the discrete wavelet transform is shown in equation (6) when $A=B$:

$$f(t)=\frac{1}{A}\sum_{j,k}WT_f(j,k)\varphi_{j,k}(t) \tag{6}$$

Specifically, the discrete wavelet sequence is an orthogonal basis when $A=B=1$, when the formula for the discrete wavelet inverse transformation is shown in (7):

$$f(t)=\sum_{j,k}WT_f(j,k)\varphi_{j,k}(t) \tag{7}$$

Through DWT decomposition, a one-dimensional signal can be divided into two parts: The signal is divided into a high - frequency sub - band and a low - frequency sub - band. The low - frequency sub - band can be further broken down into a high - frequency portion and a low - frequency portion. Once the discrete wavelet transform (DWT) decomposition is carried out, the energy of the signal is predominantly concentrated in the low - frequency portion, while the high - frequency portion contains a very small amount of energy. Since the low - frequency component can effectively withstand various attacks, to achieve better robustness,

the watermark can be inserted into the low - frequency component after DWT decomposition. Moreover, the original signal can be reconstituted from the high - frequency component and the low - frequency component, which is known as the discrete wavelet inverse transform (IDWT).

3 Programming

3.1 Overall idea

As a unique technical means, blockchain can provide brand-new solutions for copyright protection, registration of rights and transaction of digital music works, This is anticipated to create a more extensive development scope for copyright safeguarding within the music performance sector. Blockchain technology possesses the traits of decentralization, transparency, immutability, and traceability. These features render it highly appropriate for music copyright protection and network threat mitigation. Decentralization means that music copyright protection no longer needs to rely on centralized institutions or platforms, thus reducing the risk of being attacked. The characteristics of openness and non - alterability can guarantee the transparency and genuineness of copyright information, safeguarding it against being modified or fabricated. In addition, the traceability feature can provide strong evidence support to help solve difficult problems such as rights defense and rights confirmation. Overall, the attributes of blockchain technology render copyright safeguarding within the music performance sector more secure, transparent, and dependable.

In this research paper, we leverage blockchain technology to achieve copyright safeguarding and network threat mitigation within the music performance sector. We put forward a music copyright protection and transaction framework founded on the coalition chain. This system is designed to perform functions in validating, utilizing, and defending the rights of digital music. Additionally, we present an enhanced consensus algorithm aimed at countering the Sybil attack. Through this algorithm, nodes across the entire network can reach an agreement and collaborate to uphold the secure and stable operation of the blockchain network.

3.2 System architecture

Figure 1 depicts the architecture of the music copyright protection and transaction system founded on blockchain technology. On the client side, users go through the registration process. The registration results in the creation of an account using the public key of the certificate. Through the PKI certificate system, every user acquires a distinct digital certificate that serves as an identity identifier.The server side consists of four layers: the contract layer, the network layer, the consensus layer, and the storage layer. The contract layer is responsible for identity verification, examination of music works, and the recording of both music copyright data and transaction details. The network layer enhances efficiency by separating the execution of smart contracts from the consensus mechanism.The transaction procedure involves three types of nodes: endorsement nodes, sorting nodes, and bookkeeping nodes. The endorsement node conducts verification, simulates the execution, and provides an endorsement for the transaction. The sorting node arranges the transactions and determines their sequence. The bookkeeping node examines the sorted transactions and records the legitimate ones into the ledger.Given that blockchain is not well - suited for storing large files, this paper adopts a combined on - chain and off - chain approach. Copyright information and transaction data are stored in the blockchain, music is stored in the local database, and music feature fingerprints are stored in IPFS. The consensus layer is mainly an abstract embodiment

of the consensus communication between the blockchain nodes, and adopts the modified PBFT algorithm to achieve consistency of data storage, defend against blockchain Sybil attack, and at the same time make the whole system can ensure the efficiency and speed of consensus even in the case of a large amount of business.

In this paper, we adopt Fabric platform and use the coalition chain with Kafka consensus mechanism to implement a system for protecting and transacting music copyrights, and leverage the features of blockchain technology to render the registration, trading, and verification of digital music copyrights more efficient and reliable.

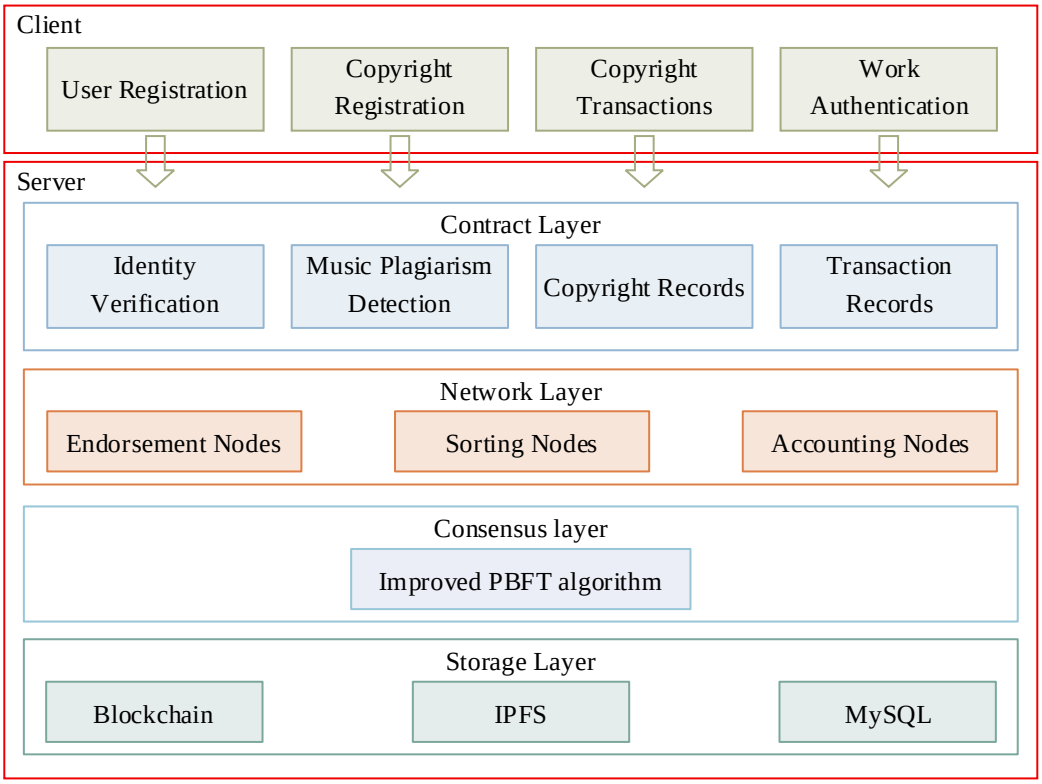


Figure 1: Music version power protection and trading system architecture

3.3 Improvement of consensus algorithm

Blockchain is a non - centralized, distributed record - keeping system. In this system, a consensus mechanism is needed to select the sole node that has the "right to record transactions". so that nodes can establish trust and maintain the consistency of the system together under the environment of no central node control and the possible existence of malicious nodes. Therefore, The music copyright protection and transaction system founded on blockchain requires an effective and suitable consensus algorithm to ensure the data consistency of this system. At the same time, the network structure of blockchain is vulnerable to Sybil attacks. A Sybil attack takes place when malevolent nodes fabricate numerous fake node identities to enter the blockchain network. In this article, we put forward a plan to counter Sybil attacks in the blockchain. This is accomplished by enhancing the Practical Byzantine Fault Tolerance Algorithm (IPBFT). Through the establishment of a blockchain consensus mechanism, this algorithm conducts data integrity verification and protects the security of the music copyright protection and transaction system.

3.3.1 System model

There are N consensus nodes $S=\{S_0,S_1,\cdots,S_{N-1}\}$ in the music copyright protection and trading system, and there exists a master node S_p in each round, and all the consensus nodes will cache the information of the incoming transactions to them locally for storing first, and at the same time the master node S_p will receive a valid transaction transaction from the client packed into a block.

When the majority of the consensus nodes validate the new block, it is deemed valid and will be incorporated into the blockchain. Conversely, if not validated, this block will be jettisoned.In the blockchain system, an enhancement has been made to the PBFT algorithm. Specifically, the voting weight of each consensus node is correlated with the reputation value it holds. Moreover, in this system, every consensus node is responsible for maintaining and updating a consensus - node information table.

3.3.2 Reputation modeling

In the improved consensus algorithm, the established reputation value, denoted as R is a real - valued quantity that lies within the range of 0 to 1. As the reputation value increases, the level of credibility rises accordingly.

(1) S_i is the master node

For the master node, if a new block is generated during t rounds of consensus, then the reputation value of the master node will increase, and with more and more rounds of consensus the reputation value will increase more and more slowly but the maximum value will not be more than 1.In the event that no new block is produced, the standing value of the master node will decline. The rate at which this decline occurs is dictated by the value of x. Should the primary node transmit a distinct set of node details to the other nodes, the credibility score of the primary node will plummet to zero, and it will be excluded from the existing consensus node details list. Let $R_i(t)$ be the reputation value of node S_i after the t th round of consensus in the blockchain, then $R_i(t+1)$:

$$R_i(t+1)=\begin{cases}\min\left(1,R_i(t)\left(1+\dfrac{1}{t+1}\right)\right),\text{A new block has been generated}\\ xR_i(t),\text{No new block has been generated}\\ 0,\text{Sending differentmessage lists to different nodes}\end{cases} \tag{8}$$

(2) S_i is a replica node

In the context of a replica node, during the consensus process in round t, if it transmits an identical list of messages (CNIL) to other nodes and the voting outcome aligns with the final result, the reputation score of the replica node will gradually rise, yet it will not exceed 1. In the event that the node abstains from participating in the consensus process within the current round, the reputation score of that particular node will decline.Alternatively, if the node takes part in the consensus process but the voting outcome does not match the final result, the reputation score will also drop. The rate of this decrease is determined by the value of y.Should it be detected that the same consensus node sends a dissimilar list of node information to other nodes, the node will be classified as a Sybil node. Consequently, its

reputation score will be immediately reduced to zero, and it will be removed from the current consensus node information list. As shown in equation (9):

$$R_i(t+1)=\begin{cases}\min\left(1,R_i(t)\left(1+\dfrac{1}{t+1}\right)\right), \text{Nodes send}\\ \text{identical message lists and agree to the majority}\\ xR_i(t), \text{Nodes did not send messages in this round}\\ yR_i(t), \text{Nodes did not agree to}\\ \text{the majority in this round}\\ 0, \text{Send different message lists to different}\end{cases} \tag{9}$$

Among them, $0<x<1, 0<y<x<1, 0<z<0.05$.

3.3.3 Master Node Update Algorithm

Within the Practical Byzantine Fault Tolerance (PBFT) algorithm, the replacement of nodes is carried out by $p=v \bmod |R|$, where v is the view number. In the enhanced PBFT algorithm, the replacement of the primary node is carried out according to the reputation score of the nodes. As depicted in the equation of the view number, during the primary node update procedure, the greater the reputation score of a node, the higher the likelihood that the node will be selected as the primary node (10):

$$\forall S_i, S_j \in S: R_{(S_i)} \geq R_{(S_j)} \Rightarrow P_{(S_i,D)} \geq P_{(S_j,D)} \tag{10}$$

where S is the set of consensus nodes, P is the probability that a consensus node is elected as the master node, and D is the exponential distribution. Where the probability density function $F(x)$ of the exponential distribution:

$$F(x)=\begin{cases}\lambda e^{-\lambda x}, & x\geq 0\\ 0, & x<0\end{cases} \tag{11}$$

where, $\lambda=-\ln^{\left(0.05^{\mu^2}\right)}\!\!\diagup_{N}$, the values of 1, 2, and 3 for μ correspond to the first three trustworthy states of the consensus node, respectively,When the credibility value of the consensus node drops below the initially set threshold of 0.5, the consensus node is removed. Additionally, the possibility of substituting the master node is taken into account. The trusted state $TS=I$ of the consensus node is shown in equation (12) when $t=1$:

$$\int_0^N F(x)=1-e^{-\lambda x}\Big|_0^N=0.95 \tag{12}$$

That is, the consensus node with trusted state TS=I has a 95% chance to be elected as the master node. By analogy, consensus nodes with TS=II and TS=III have 80% and 55% chances to be elected as master nodes, respectively.

The specific steps for changing the master node algorithm are as follows:

(1) In the course of the consensus procedure, when the reputation score of the primary

node falls below the predefined threshold or reaches zero precisely, every secondary node is required to select the node boasting the highest reputation score among the existing nodes as the primary node. Subsequently, the secondary node disseminates a primary - change message to the other nodes, with the following content $< primary-change, S_q, R_{\max} CNIL_{S_i}, S_i >$, where S_q is the serial number of the newly elected master node, $R_{\max}$ is the reputation value of the newly elected master node, and S_i is the replica node serial number.

(2) The other replica nodes collect and calculate whether there are $2f$ different replica nodes (excluding themselves) sending the priamry-change message updating the master node to S_q, if there are $2f$ then execute (3), otherwise end.

(3) The newly elected master node N sends a new-primary message to the other replica nodes as $<$new-primary$, S_q, O, CNIL_{S_q} >$, where O is the set of primary-change messages.

Completion of the above steps of the change-master node algorithm leads to the process of consensus with node S_q as the master node.

3.3.4 PBFT Algorithm Improvement

During the enhancement of the consensus algorithm, the reputation score of each node is computed to allocate distinct speaking privileges to every node. The criterion for a consensus node i to update its consensus status is that the total of the reputation scores R_v of the consensus nodes sending messages to it is sufficiently high. The calculation of the total reputation scores R_v received from other nodes is as follows.

Supposing that the blockchain network is a directed graph $G(N, E)$, in which N represents the collection of nodes and E is the set of directed edges with weights. This network can be employed to forecast the potential results of the negotiation among the consensus nodes and to ascertain the influence of the nodes during the consensus - building process.

Within the blockchain network, the present reputation score obtained by a node i is collaboratively decided by the reputation scores of its adjacent nodes. That is to say, the reputation score acquired by a node i in a particular round t is as described in equation (13):

$$R_v(t) = R_i(t) + \sum_{j=1}^{N} \left[R_j(t) - R_i(t) \right] \left(\varphi^T \right)_{ij} \tag{13}$$

where $R_i(t)$ is the reputation value of node i at t round of consensus, the matrix $\varphi = (\varphi_{ij}) \in R^{N \times N}$ consists of the network topology and the reputation values on the links, and φ^T is its transpose matrix.

If node i is influenced by more than one neighboring consensus node, then the reputation value received by node i is the sum of all influences acting on i, as shown in equation (14):

$$\Delta R_i(t) = \sum_{j=1}^{N} \left[R_j(t) - R_i(t) \right] \varphi_{ij} \tag{14}$$

The state equation can be expressed as $\Delta R(t) = L \cdot R(t)$, where L is the Laplacian matrix of φ^T. Therefore the updated rule is Eq. (15):

$$R(t+1) = R(t) + L \times R(t) = (I + L)R(t) \tag{15}$$

where the matrix $T = I + L = (T_{ij}) \in R^{N \times N}$, and T_{ij} denotes that node i is influenced by node j.The current node's consensus process is affected by the connected consensus nodes, enabling the consensus node to compute the present reputation value that can vary dynamically as time progresses.

The sum of the received reputation values of other nodes R_v has to be not less than a set threshold $R_{threshold}$. Where the value of $R_{threshold}$ is set as equation (16):

$$R_{threshold} = \frac{1}{N} \times \left(2 \times \left\lfloor \frac{N-1}{3} \right\rfloor + 1 \right) \tag{16}$$

The enhanced PBFT algorithm consists of six stages, with four of them being the most significant: pre - preparation, preparation, pre - submission, and submission. Moreover, it integrates a reputation - based model. This model is designed to identify Sybil nodes within the blockchain. It does so by assessing the standing of each node according to their actions during the consensus procedure.

The following are the detailed procedures of the enhanced PBFT algorithm.

(1) Client C initiates transaction tx and broadcasts the transaction to the master node 0. The master node 0 receives the sent transaction tx and first verifies whether the transaction transaction tx is valid or not, if the transaction is invalid it directly deletes the transaction. If the transaction is valid, it packages the transaction tx into the block and generates the block header B_{head} based on the information in the block body.

(2) Master node 0 broadcasts a Pre-Prepare message to each replica node, where the content of the Pre-Prepare message is $<<\text{PRE-PREPARE}, h, d, t, P_0, CNIL_0>_{\sigma 0}, B_{head}>$, where h is the height of the current new block, d is the summary of the block head B_{head}, t is the current timestamp, P_0 is the identity id of the current master node 0, and $CNIL_0$ is the list of node information of the master node 0.

(3) Replica nodes 1, 2 receive the Pre-Prepare message sent by master node 0, firstly, they have to check the validity of the new block, and after passing the validation, then they send Prepare messages to other nodes respectively $<<\text{PRE-PREPARE}, h, d, t, P_i, CNIL_i>_{\sigma i}, B_{head}>$.

(4) Replica nodes 1,2 receive Prepare messages from other replica nodes received from nodes with different reputation values. First the replica node has to calculate the reputation value of the node that currently sends a message to it R_v, and if $R_v \geq R_{thershold}$ then it updates the consensus status of the transaction message and sends the Pre-Commit message $<<\text{PRE-COMMIT}, h, d, t, P_i>_{\sigma i}, <CNIL>_{\sigma i}>$.

(5) Master node 0 will receive the Pre-Commit message sent by replica nodes for comparison, calculate the current reputation value of each node according to the reputation model, update the local consensus node information list at the same time feedback the consensus result to the client and all replica nodes, and send the Commit message $<<\text{PRE-COMMIT}, h, d, t, P_0>_{\sigma 0}, <CNIL>_{\sigma 0}>$.

(6) After completing the commit state, the replica nodes in the blockchain update the local

consensus node information list and feedback the consensus result to the client to prepare for the next round of consensus process.

3.4 Music copyright protection design

3.4.1 Copyright in music

Upon successful registration, users are transformed into user nodes. Subsequently, these user nodes have the ability to submit their original musical works for copyright registration through the following procedure:

The system employs the Shazam algorithm to extract the musical fingerprints of the uploaded pieces:

$$S\left(music\right) \rightarrow fingerpr\,\mathrm{int} \tag{17}$$

The initial audio data is transformed into mono format. Subsequently, a first - order digital filter is employed to accentuate the features of the audio signal. This process aims to enhance the high - frequency component, resulting in a smooth spectrum that is more conducive to analysis. The relevant operation is described by equation (18):

$$y(n) = x(n) - ax(n-1) \tag{18}$$

The value of the audio sampling at time n is denoted as $x(n)$, and a represents the pre - emphasis factor.

As the audio signal varies over time, its amplitude is continuously altered. Thus, it is essential to perform framing on it. Through the process of splitting the audio into frames, the characteristics of the audio signal within a certain time period can be kept largely stable. The frame - splitting process is, in fact, a windowing operation. In this operation, the windowing function $w(n)$ is multiplied by the signal function $x'(n)$ to generate a windowed audio signal:

$$x(n) = x'(n) \times w(n) \tag{19}$$

The windowing function used in this system is the Hamming window which is commonly used in frequency domain analysis:

$$w(n) = \begin{cases} 0.54 - 0.46\cos\left[2\pi n/(N-1)\right] & 0 \le n \le N-1 \\ 0 & others \end{cases} \tag{20}$$

A brief - duration Fourier transform (STFT) is applied to the windowed audio signal. This process serves to transform the initial time - domain audio signal into the frequency domain, thereby generating a spectrogram. As shown in equation (21):

$$X(m,w) = \sum_{n=-\infty}^{\infty} x(n)w(m-n)e^{-jwn} \tag{21}$$

(2) Compare the extracted music fingerprint with the feature fingerprint library in IPFS to determine whether the work is original or not. Construct a backward index with the keyword music fingerprint $(f_1, f_2, \Delta t)$ and the value corresponding to the keyword is the ID of the

music and the position of f_1 in the music, i.e., the fingerprint time offset *offset*:

$$key\left(f_1, f_2, \Delta t\right) \rightarrow value\left(musicID, offset\right) \tag{22}$$

Compare the audio fingerprints of the music to be uploaded with the keywords in the hash table to get all the audio fingerprints mapped by the same keywords, and then find out the similar music based on the audio fingerprints, which are obtained by *musicID*. For each similar music, find the time offset difference between each matched music fingerprint and the corresponding music fingerprint of the music to be uploaded:

$$\Delta t_k = t_k' - t_k \tag{23}$$

where: t_k is the time offset of the music to be uploaded, t_k' is the time offset of the similar music, and Δt_k is the time offset difference between the fingerprints of the two music. From all the calculated time offset differences, find the value with the largest difference of the same time offset in each music as the number of fingerprint matches for that music. If the number of fingerprint matches between the music to be uploaded and the similar music exceeds the set threshold, the music is determined to be identical to the similar music.

(3) When the matching algorithm identifies the music as original, the system saves the extracted fingerprints of the music characteristics into the InterPlanetary File System (IPFS) and gets the IPFS hash address of the fingerprint database:

$$fingerpr\,\mathrm{int} \xrightarrow{upload} IPFS \xrightarrow{get} hash \tag{24}$$

(4)Trigger the copyright registration intelligent contract to submit the IPFS hash address along with the copyright details and timestamp as a transaction within the blockchain.

$$\left(IPFS_{hash}, musicID, author, Ts\right) \rightarrow TX \rightarrow blockchain \tag{25}$$

(5) Add the platform watermark to the original music file and then store it in the local database MySQL to provide effective credentials for the creators to protect their rights. Since the audio is a one-dimensional vector and the platform watermark is a two-dimensional binary image, the image should be downscaled and converted into a one-dimensional vector, i.e., $M = M_1 \times M_2$. The original audio signal S of length N is segmented, and the length of each segment is set to N_1, the original audio signal is divided into $K = fix(N / N_1)$ segments, and each segment is embedded with a watermark information. The Haar wavelet basis is used, defined as shown in equation (26):

$$\psi(t) = \begin{cases} 1 & 0 \le t \le \dfrac{1}{2} \\ -1 & \dfrac{1}{2} \le t \le 1 \end{cases} \tag{26}$$

After taking the Haar wavelet basis, denote S as:

$$S(n) = \sum_{j,k \in Z} C_{j,k} \psi_{j,k}(n) \tag{27}$$

where: $C_{j,k}$ is the discrete wavelet coefficients. The watermarked signal is embedded in the low-frequency approximation part, and after embedding the watermarked information, then after IDWT, the audio is transformed into a time-domain signal.

3.4.2 Music rights trading

Figure 2 depicts the process of music copyright transactions. Leveraging the immutable and traceable properties of blockchain technology, smart contracts are triggered to facilitate copyright exchanges between users, thus guaranteeing a secure environment for such transactions. Users have the ability to search for music that piques their interest, listen to it, and subsequently make a purchase.Upon the successful completion of each transaction, the blockchain automatically generates a corresponding transaction record. Once inscribed on the blockchain, this record remains unalterable. The transaction record encompasses several key elements: the identifier of the purchaser, the identifier of the music creator, the transaction amount, the IPFS hash address of the music fingerprint, and the timestamp.

$$(hash, user, author, amount, Ts) \rightarrow TX \tag{28}$$

Every single transaction gets disseminated across the peer - to - peer network. After that, it undergoes verification by a consensus process. Ultimately, it is added to the ledger.

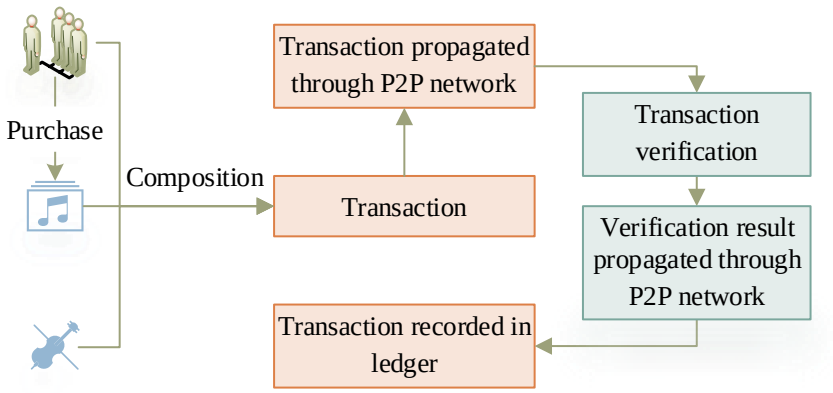


Figure 2: Music copyright transaction model

3.4.3 Authentication of musical works

Users can upload music files suspected of being pirated to the system, which will detect whether the files contain the platform's watermark, and determine whether the uploaded music is pirated based on the copyright information of the work and the copyright transaction information. Users can also upload music to determine whether there is plagiarism or similarity, and the system will match the files based on their feature fingerprints to give similarity results. After the originator uploads the music feature fingerprint to IPFS, the returned hash value, The details of the work and the time - stamp are uploaded onto the blockchain. Subsequently, users have the ability to track the copyright details of the work by referring to the hash value.

4 Experiments and their validation analysis

4.1 Experimental setup

To validate the system's performance, the system in this paper employs a test environment. This environment is equipped with an Intel Core i7 - 14700KF CPU clocked at 5.60GHz, 32GB of RAM, and runs the Windows 11 operating system. Additionally, a VMware virtual machine with the Ubuntu 16.04 system installed is attached.In the music copyright protection and transaction system founded on blockchain technology, the copyright registration module is the most fundamental and central functionality. It is also the most time - and storage - intensive part. This is because it requires the application of the Shazam algorithm to handle music files and the storage of music feature fingerprint data. Thus, in this paper, the copyright registration module of the system will undergo testing.Moreover, within the blockchain network of the established music copyright protection and transaction system, the enhanced consensus algorithm (IPBFT) will be evaluated in terms of node fault tolerance and transaction throughput. During the experiments, transactions are continuously fed into the system. The IPBFT consensus algorithm is then executed to achieve an agreement on these transactions. Subsequently, the transactions are grouped into new blocks and recorded on the blockchain.

4.2 IPBFT algorithm testing

4.2.1 Fault Tolerance Analysis

In the music copyright protection and trading system, fault tolerance is a crucial objective that reflects the system's reliability and availability. To be more specific, when the music copyright protection and trading system encounters a failure or has a certain number of nodes with Byzantine problems, the system can still operate normally without breaking down.As described in this paper regarding the improved PBFT algorithm, namely the IPBFT consensus algorithm, the maximum number of faulty nodes that this algorithm can tolerate is $f=(N-1)/3$ (f is the number of Byzantine problem nodes). (where f represents the number of nodes with Byzantine problems). Subsequently, the system's fault tolerance is tested with the number of faulty consensus nodes set as f_1=0,1,2,3,4,5,6, and 7 respectively. The test results are presented in Figure 3.

In the consensus node set, when the quantity of malfunctioning nodes is fewer than 3, there are sufficient normal nodes to guarantee the proper execution of the blockchain network's consensus requests. At this juncture, the system's throughput hovers around 1700 - 1800 TPS. Conversely, once the number of failed nodes in the consensus node set hits 3, the blockchain network malfunctions, and each request fails to execute as intended. As a result, the system throughput drops to 0.Based on the experiments, it can be deduced that the IPBFT consensus algorithm can tolerate a maximum of no more than $(N-1)/3$ [the specific number is missing in the original] failed nodes. Its fault - tolerance ability of the algorithm meets the requirements, enabling it to be applied smoothly in the music copyright protection and trading system.

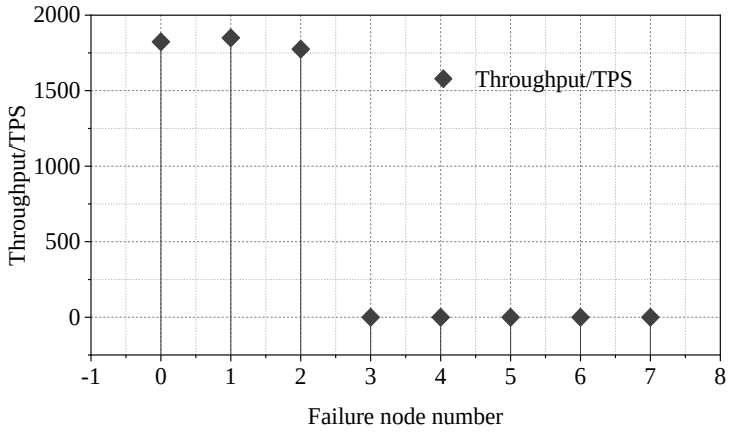


Figure 3: IPBFT algorithm fault tolerance test

4.2.2 Throughput analysis

Throughput acts as a measure to evaluate a system's ability to handle the volume of requests within a specific time period. To some extent, it demonstrates the system's performance. In this chapter, the number of transactions per second (TPS) is used to represent the throughput of the algorithm. A throughput evaluation is carried out on the proposed IPBFT consensus algorithm, as well as the PBFT consensus algorithm and the DPBFT consensus algorithm does not take into account the problem of network bandwidth, the script simulates 1200 simultaneous user requests, each user initiates a request twice a second, 25 consecutive experiments and each time the request is initiated continuously for ten seconds. Algorithm throughput comparison is shown in Figure 4. The throughput of IPBFT consensus algorithm is 1251TPS on average, which is larger than that of PBFT algorithm and DPBFT algorithm, which are 898TPS and 1050TPS, respectively.Across a multitude of experiments, the throughput of the IPBFT consensus algorithm shows only slight variations, and its performance is far more stable. This trait is highly compatible with the practical demands of the music copyright protection and trading system. That is to say, it meets the actual requirements of this system.

To substantiate the effectiveness of the IPBFT algorithm, a selection of well - known blockchain platforms is made for comparison. In Figure 5, a contrast is shown between the throughput of the IPBFT algorithm and that of other blockchain platforms. The throughput of the IPBFT consensus algorithm attains 1,250 TPS. This shows a notable enhancement when contrasted with several established and well - developed blockchain platforms. Evidently, it showcases that the performance of the IPBFT consensus algorithm proposed in this paper can fulfill the requirements of the application environment for music copyright protection and trading systems.

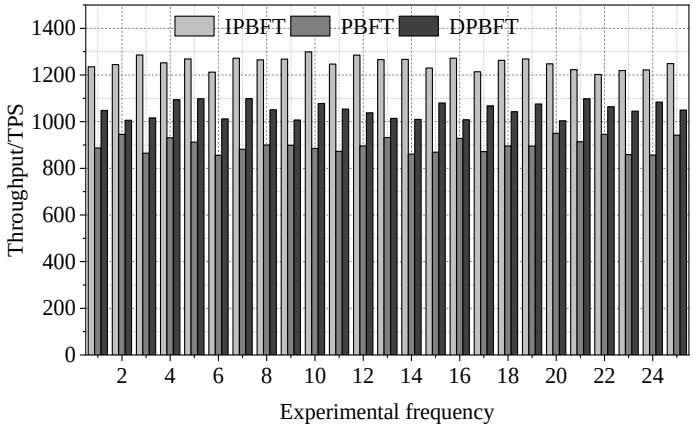


Figure 4: Algorithm throughput comparison

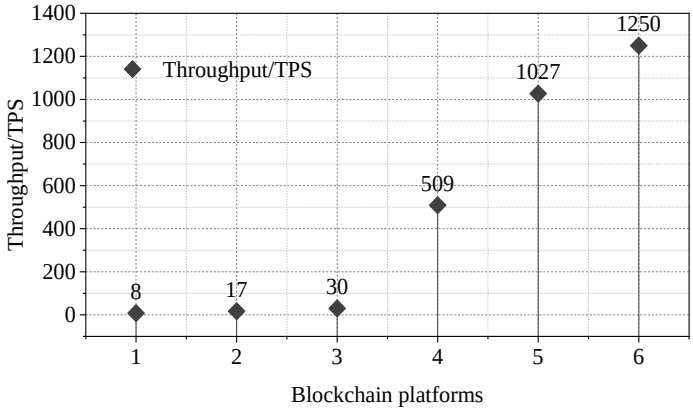


Figure 5: Comparison of throughput between IPBFT algorithm and other blockchain platforms

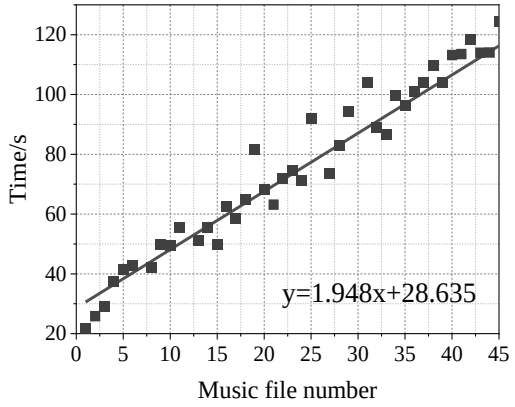
4.3 System Performance Testing

4.3.1 Timing of copyright registration

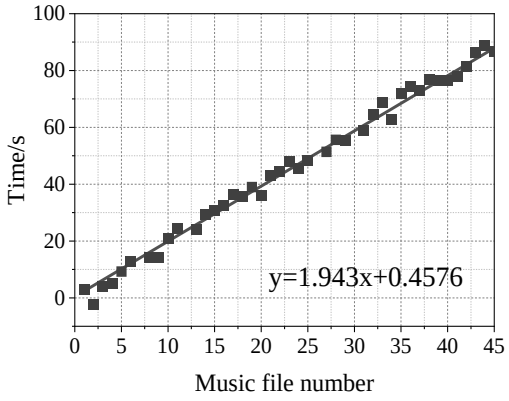
In this research paper, the system is engineered to acquire the distinctive fingerprint data from 10 - second portions of the music files intended for comparison. At the same time, the characteristic fingerprint database set up by the system must extract the characteristic fingerprint data of the whole music. In this paper, the system registers the copyrights of 45 different music files randomly downloaded from the Internet, 41 of these 45 music files are successfully registered, with a success rate of 91.11%, and the 4 music files that fail to be registered have file numbers 7, 12, 26, and 30, respectively. The reasons for the failure of the registration are that the system is not able to allocate enough memory in the stage of extracting the fingerprints of the whole music file, which leads to a system error. The reason for the failure of copyright registration is that not enough memory can be allocated during the extraction of the characteristic fingerprint of the whole music file. Analyzing these four music files, we can see that the length of the music is about 5 minutes, and extracting all the music fingerprints will be very large, which will trigger the system's over-processing mode, prohibiting the creation of memory space for variables of this size. The memory problem can be solved by modifying the system configuration to expand the virtual memory and storing the fingerprint data in batches.

During this test, a total of 41 music tracks were successfully registered for copyright

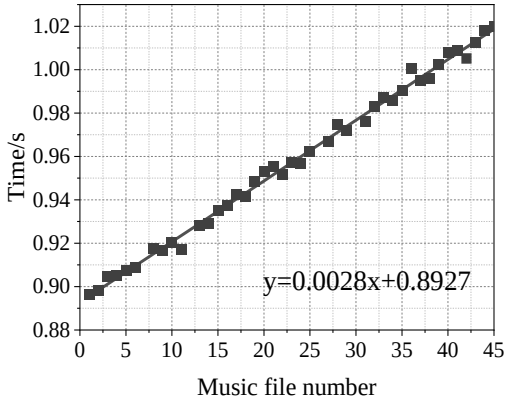
within the system described in this paper. The registration time for each track is presented in Figures 6(a) through (e). The gradient of the total time dedicated to copyright registration is approximately 1.948. This indicates that for every additional music piece registered by the system, the copyright - registration time for subsequent music will rise by around 1.948 seconds.The gradient of the time the system expends on extracting 10 - second - long fingerprints from music files is 0.0028. This is primarily attributed to the variability in the system's performance. The system spends roughly 0.9 seconds on extracting these 10 - second - long fingerprints.The gradient of the time required by the system to extract all the feature fingerprints of the music files is about - 0.0251. This is also a result of the system performance fluctuations. In other words, it takes approximately 21 seconds to extract all the feature fingerprints of each music piece.The gradient of the time taken by the system to conduct similarity matching is approximately 1.943, which is nearly equal to the gradient of the total time for copyright registration. This implies that the increase in the time for similarity matching leads to the increase in the overall time for copyright registration.Lastly, each music piece demands about 6.8 seconds for other auxiliary processing. In addition to the fluctuation of system performance, some music files require more processing time because the system checks whether the sampling rate of the music file is 44.1kHz and MP3 format before extracting the music feature fingerprints, and if it is not, it will utilize the FFmpeg tool to transform the music file before If not, then FFmpeg tool will be used to convert the music file before extracting the fingerprint.



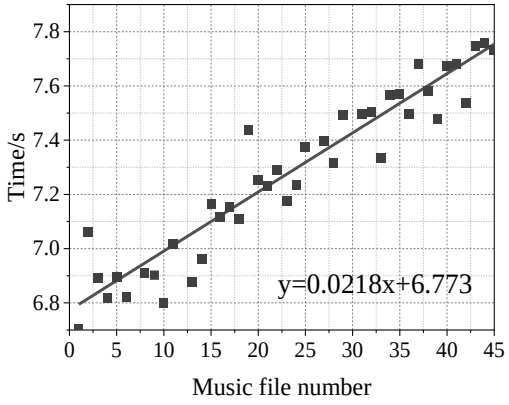
(a)The total time of copyright registration



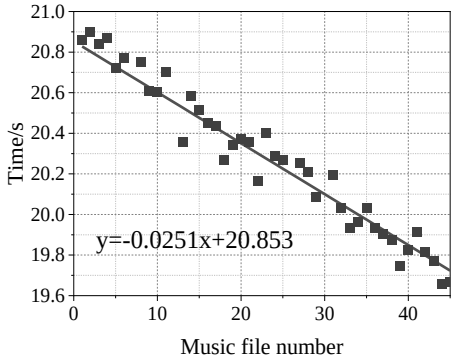
(b)The time of similarity contrast



(c)Extract 10s feature fingerprint time



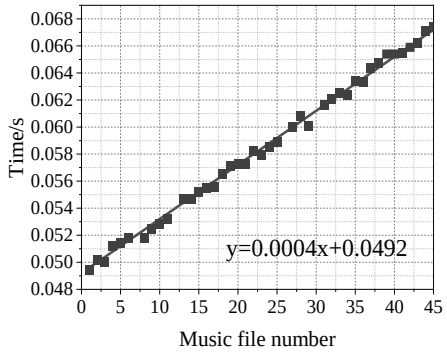
(d)The time of other processing



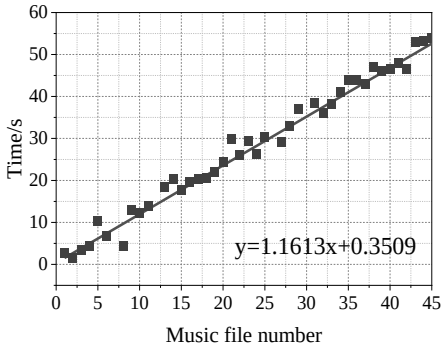
(e)The time of extracting all feature fingerprint

Figure 6: Time spent on copyright registration

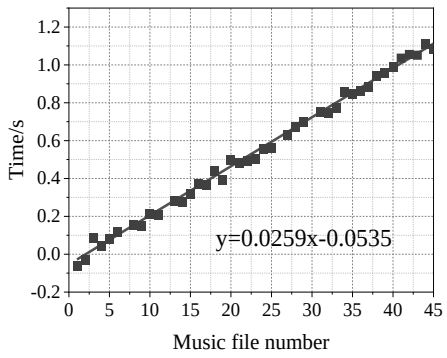
An elevation in the duration dedicated to similarity matching results in an augmentation of the total copyright registration time. The elements contributing to the rise in the time allotted for similarity matching are presented in the figures.7(a)~(d). The slopes of the four lines in the figure are 0.0004, 1.1613, 0.0259, and 0.7571, which add up to about 1.945, This value represents the gradient of the line depicting the time dedicated to similarity matching in Figure 6. The increment in time between retrieving the address of the feature fingerprint on IPFS from the copyright registration contract and sorting the hash value of the feature fingerprint is comparatively minor,and the most significant of these four factors is actually obtaining all of the feature fingerprint data from IPFS.



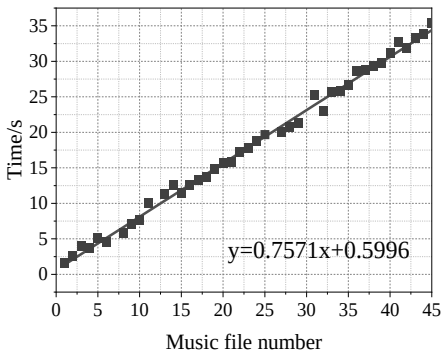
(a)Get IPFS from the contract



(b)Get all the feature fingerprints from IPFS



(c)Sorting feature fingerprint Hash value



(d)Matching feature fingerprint Hash value

Figure 7: Factors of copyright registration time increase

4.3.2 Music copyright depository

Among the 41 pieces of music that have successfully obtained copyright, the storage space occupied on IPFS by the extracted feature fingerprint data of each piece of music is presented in Figure 8, and the quantity of hash values within each feature fingerprint is depicted in Figure 9. On average, each of these 41 music tracks consumes approximately 8.05 MB of IPFS space. Even though 8.05 MB is two to three times the size of the original music file, this exemplifies the concept of the Shazam algorithm trading space for time. By augmenting the storage space, it enhances the speed of the feature fingerprint similarity comparison.

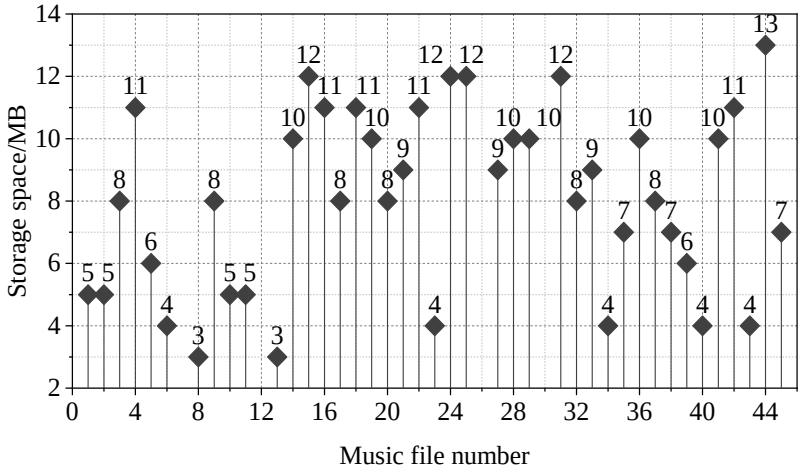


Figure 8: The cost of storage space occupied by each feature fingerprint on the Inter Planetary File System (IPFS)

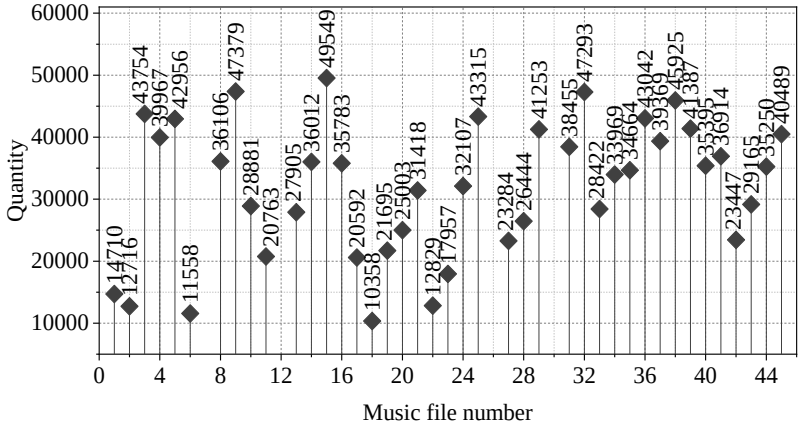


Figure 9: Quantity of Hash values within each feature fingerprint

5 Conclusion

The challenge of safeguarding music copyrights acts as a hindrance to the progress of the music industry. This paper integrates blockchain technology, the InterPlanetary File System (IPFS), the Shazam algorithm, Discrete Wavelet Transform (DWT) digital watermarking technology, and an enhanced consensus algorithm to put forward a music copyright protection and transaction system. This system is beneficial for the copyright protection of the music performance industry and its defense against cyber threats. The system realizes digital music

copyright protection through copyright registration confirmation, copyright usage transaction and musical work authentication, and guarantees the security of blockchain network by defending Sybil attack in blockchain through the improved practical Byzantine fault-tolerant algorithm. The experimental test on VMware virtual machine found that (1) when the number of failed nodes ≥ 3, the system throughput is 0, which satisfies that the number of malicious nodes does not exceed $(N-1)/3$, which indicates that the improved PBFT algorithm has a good fault-tolerance, and its throughput is higher than the comparative consensus algorithm, with a mean value of 1,251 TPS, This implies that the algorithm can guarantee the security and vitality of the music copyright protection and transaction system. (2) For each piece of music, the growth in copyright registration time is approximately 1.948 seconds. Moreover, on IPFS, the average storage of feature fingerprint data for each piece of music uses around 8.05 megabytes. which can satisfy the practical needs of managing and protecting the copyright of music works. There is still much room for improvement for the existing research work, such as optimizing the time spent on copyright registration and expanding virtual memory.

References

[1] Panjaitan, H., Betlehn, A., Situmeang, T., Khan, M. Z. K., & Miraz, M. H. (2024). Music copyright protection in the digital era: Legal framework and strategies for enforcement. Jurnal Hukum UNISSULA, 40(2), 235-257.

[2] Herlihy, D., & Zhang, Y. (2016). Music industry and copyright protection in the United States and China. Global Media and China, 1(4), 390-400.

[3] Atanasova, I. (2019). Copyright infringement in digital environment. Economics & Law, 1(1), 13-22.

[4] Michael, J., Cohn, A. L. A. N., & Butcher, J. R. (2018). Blockchain technology. The Journal, 1(7), 1-11.

[5] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

[6] Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. PeerJ Computer Science, 9, e1705.

[7] Santiago, J. M. (2017). The Blurred Lines of Copyright Law: Setting a New Standard for Copyright Infringement in Music. Brook. L. Rev., 83, 289.

[8] Mopas, M., & Curran, A. (2016). Translating the sound of music: forensic musicology and visual evidence in music copyright infringement cases. Canadian Journal of Law and Society/La Revue Canadienne Droit et Société, 31(1), 25-46.

[9] Fang, Q. (2024). Designing of music copyright protection system based on deep belief network and blockchain. Soft Computing, 28(2), 1669-1684.

[10] Chen, X., Yang, A., Weng, J., Tong, Y., Huang, C., & Li, T. (2023). A blockchain-based copyright protection scheme with proactive defense. IEEE Transactions on Services Computing, 16(4), 2316-2329.

[11] Qureshi, A., & Megias Jimenez, D. (2020). Blockchain-based multimedia content protection: Review and open challenges. Applied Sciences, 11(1), 1.

[12] Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. Computer law & security review, 34(3), 550-561.

[13] Gürfidan, R., & Ersoy, M. (2021). Blockchain-based music wallet for copyright protection in audio files. Journal of Computer Science & Technology, 21.

[14] Ciriello, R. F., Torbensen, A. C. G., Hansen, M. R. P., & Müller-Bloch, C. (2023). Blockchain-based digital rights management systems: Design principles for the music industry. Electronic markets, 33(1), 5.

[15] Cai, Z. (2020). Usage of deep learning and blockchain in compilation and copyright protection of digital music. Ieee Access, 8, 164144-164154.

[16] Xu, Z., Wei, L., Wu, J., & Long, C. (2020, December). A blockchain-based digital copyright protection system with security and efficiency. In CCF China Blockchain Conference (pp. 34-49). Singapore: Springer Singapore.

[17] Wijesekara, P. A. D. S. N. (2025). A Survey on Blockchain-driven Music Industry: Trends, Gaps, and Future Directions. Science, Engineering and Technology, 5(2).

[18] Wen, X. (2023). Application of blockchain technology in copyright protection of digital music information. International journal of grid and utility computing, 14(2-3), 136-145.

[19] Li, N. (2022). Combination of blockchain and AI for music intellectual property protection. Computational intelligence and neuroscience, 2022(1), 4482217.

[20] Kim, A., & Kim, M. (2020, October). A study on blockchain-based music distribution framework: focusing on copyright protection. In 2020 International conference on information and communication technology convergence (ICTC) (pp. 1921-1925). IEEE.

[21] Li, Y., Wei, J., Yuan, J., Xu, Q., & He, C. (2021). A decentralized music copyright operation management system based on blockchain technology. Procedia Computer Science, 187, 458-463.

[22] Zhao, J., Zong, T., Xiang, Y., Gao, L., & Beliakov, G. (2020, October). Robust blockchain-based cross-platform audio copyright protection system using content-based fingerprint. In International Conference on Web Information Systems Engineering (pp. 201-212). Cham: Springer International Publishing.

[23] Natgunanathan, I., Praitheeshan, P., Gao, L., Xiang, Y., & Pan, L. (2022). Blockchain-based audio watermarking technique for multimedia copyright protection in distribution networks. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 18(3), 1-23.

[24] Shi, Q., & Zhou, Y. (2025). Application of blockchain technology in digital music copyright management: a case study of VNT chain platform. Frontiers in Blockchain, 7,

1388832.

[25] Jiang, Y., Matsumoto, S., & Bischof, T. (2024). Towards a blockchain-based music royalty system. International Journal of Student Project Reporting, 2(2), 174-201.

[26] Marseda, A. T., Rosidah, E., & Lany, A. (2025). Blockchain-Based Data Bank for Music Royalty Protection in Indonesia. Research Horizon, 5(3), 921-932.

[27] Tam, T. N. L. (2019). Music copyright management on blockchain: Advantages and challenges. Alb. LJ Sci. & Tech., 29, 201.

[28] Lee, J. J. (2021, October). A Study on the Influence on Intention to Use Blockchain-Based Copyright Contract: Focusing on Blockchain-Based Digital Copyright Exchange Core Platform. In International Conference on Computer and Information Science (pp. 96-106). Cham: Springer International Publishing.