iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.61507

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Global Copyright Consortium: Empowering Decentralisation with Authority - Backed Blockchain

A. Vadivelu[1], T. Charu Vickraman[2], A. Koushik[3], V. Rohith[4]
[1]*Assistant Professor, Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India*
[2, 3, 4]*B.Tech, CSE with Specialization in Cybersecurity, SRM Institute of Science and Technology, Chennai, India*

Abstract: Digital images are transferred with ease through the network. Many users are using the images without the knowledge of the owners. Zero watermarking does not alter the original information contained in vector map data and provides perfect imperceptibility. The use of zero watermarking for data copyright protection has become a significant trend in digital watermarking research. However, zero watermarking encounters tremendous obstacles to its development and application because of its requirement to store copyright information with a third party and its difficulty in confirming copyright ownership. However, traditional digital image generation methods have high operational requirements for designers due to difficulties in collecting data sets and simulating environmental scenes, which results in poor quality, lack of diversity, and long generation speed of generated images, making it difficult to meet the current needs of image generation.

I. INTRODUCTION

This paper proposes a new image verification mechanism based on the Merkle tree technique in the blockchain. The Merkle tree root in the blockchain mechanism provides a reliable environment for storage of image features. In image verification, the verification of each image can be performed by the Merkle tree mechanism to obtain the hash value of the Merkle tree node on the path. The main purpose of this paper is to achieve the goal of image integrity verification. The proposed method can not only verify the integrity of the image but also restore the tampered area in the case of image tampering. Since the proposed method employs the blockchain mechanism, the image verification mechanism does not need third party resources. The verification method is performed by each node in the blockchain network. The experimental results demonstrate that the proposed method successfully achieved the goal of image authentication and tampered area restoration.

The popularity of cloudedge collaboration has led to the explosive development of the Internet of Things, and the collection of multimedia data is occurring more widely. Multimedia data, especially high-definition data, has obvious value attributes and can transfer value through transactions. Attention has been widely paid to how high-definition multimedia data can achieve secure transactions . High-definition multimedia data can be used in many fields. For example, vector maps are widely used in the fieldof geographic information, and remote sensing maps can effectively identify forest fires. In addition, high-definition multimedia data have also been effectively applied in the supply chain field. For example, in supply chain service and deployment tasks, high-definition video can be used to monitor the arrival of materials, ascertain whether the trucks are driven and delivered according to the prescribed routes, and effectively monitor the bid evaluation process through high-definition video. If the highdefinition video is not clear enough, the efficiency of these works will be greatly reduced. Despite the many benefits of trading high-definition multimedia data, there is still an inevitable security issue. For example, vector graphics store a small amount of data and are easy to copy and distribute. In addition, in the process of centralized trading, the transaction security of the data owner is not guaranteed, and the problem of data leakage and user privacy leakage cannot be effectively avoided (for example, data and transaction information can be obtained on the Internet). No matter who the leakage affects, the whole process of the transaction should be tracked and the copyright should be bound. Once the responsible person can be traced, punishment is required, namely accountability. To some extent, solving problems effectively can increase the activity of the market.

Recently, with the development of long-range informal communication on the web, the capacity and dissemination of interactive media content have become extremely simple. On the other hand, this simplicity has led to the need for copyright protection, blocking information theft, and data genuineness. To handle the above issues, digital watermarking has emerged as an appropriate solution. Digital watermarking is a way of embedding a watermark into a significant image/media.

©IJRASET: All Rights are Reserved

A watermark acts as copyright data, shielding advanced information from illicit replication and conveyance. A watermark is a sort of marker clandestinely inserted in a signal (audio, video, or image information). A watermark embedded into media may or may not relate to it. Watermarks are utilized to check the realness or uprightness of the watermarked signal. With the continuous improvements in computer technology and the development of image processing technology, digital image generation methods have undergone tremendous changes, and new image generation methods are emerging one after another. From traditional graphics to automatic encoding technology and then to deep learning technology, image generation methods are developing towards diversification, flexibility, and efficiency. Although using existing traditional digital image technology can achieve good results in image generation, the use of professional software to create and edit the effects of virtual environments in the face of image generation tasks is directly related to the operational ability of designers. Especially for the creation of environmental scenes, in order to simulate every aspect clearly, it is necessary to accurately simulate objective conditions such as the shape, material, and light of the object. Compared with the traditional digital image generation methods, this paper intends to use the virtual interaction design method under blockchain technology to establish a universal generation model, and train it and adjust it appropriately, so as to achieve effective extraction of different types of data and self-adaptation to various application scenarios. In the case of the same generation of images, the use of virtual interaction design under blockchain technology for digital image generation can improve the generation quality and diversity of generated images. Therefore, this paper focuses on the analysis of virtual interaction design under blockchain technology, hoping that this method can improve the existing image generation methods, make up for their shortcomings, and improve the quality and diversity of generated images. According to the advanced development of information technologies, the internet has become an indispensable part of data delivery in our daily life. The creation of content such as digital images is getting easier than before. It can be produced by a digital camera, scanner, computer software, etc. The image might be stolen, have tampered content, or even be misappropriated by an unexpected user.

Thus, how to organize, store, and deliver the images becomes an important issue because the internet is not a secure environment. Digital image content integrity has been an important research topic of digital image management in recent years. Digital images are easy to copy and transmit anywhere over public computer networks, and can be spread across the world very fast. Also, it could easily be tampered with and transformed by the unexpected user. Thus, the integrity of a digital image is determined by checking whether an image has been tampered with or not. Generally speaking, the integrity is not only checking the difference from the original image but also to point out the area of the tampered part, in the case of an image that has been tampered with. For example, the correctness of license plate information on a vehicle violation photo is quite important. That means the vehicle violation image cannot be tampered with. Normally, the tampered area detecting can be done by comparing the difference between original image and tampered image. This is not an efficient way to authenticate the integrity of an image. Many researchers use an information hiding technique to embed the features of a digital image into the image to achieve the goal of image integrity protection.

II. LITERATURE SURVEY

Blockchain has become an unavoidable future in enterprise finance, particularly enabling and securing crosscompany transactions. By introducing a comparable notion of smart contract, the trusted sub-ledger operation (TSLO), this article will propose a complete architecture based on the Blockchain to solve the traceability and validity of accounting data by assets groupement. TSLO is a more flexible and adaptable method for asset management in the corporate accounting system and the enterprise resource planner. This method is built on a decentralized microservices tree (DMST) and is an extendable E-Bidding form of TEA (Triple Entry Accounting). Instead of using a multi-ledger architecture, the Hyperledger Fabric skeleton, limited to participant channels inside one entity or organization, our approach uses decentralized sub-ledgers with an implementation tree (DMST) for an assets-driven transactions. Furthermore, the governments audit and taxation procedures for financial groups are more accessible by combining Proof of Authority and Proof of Stake to assure the logic of More stake more reputation to preserve. The auditing profession must accept and lean in to the advantages and challenges that widespread blockchain adop- tion will offer. Advances in blockchain technology present opportunities for CPA auditors and assurance providers to grow, learn and exploit their proven ability to adapt to the needs of a rapidly changing corporate world. We have estab- lished a complete architecture that offers a solution to the challenges mentioned above, and we have illuminated the solutions major components in this paper. To be able to pose the nal chain, we investigated numerous blockchain archi- tectures, and blockchain integration approaches to ERP-type N. Fikri et al.: Blockchain Architecture for TSLOs and Financial Audit Using Decentralized Microservices information systems. Weve claried the general and indi- vidual components that make up our blockchain architecture. We are sure that integrating our technique is a rst step toward integrating blockchain technology into the nancial audit- ing industry and that we can now move on to studying the developing limits of this union.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

We have already implemented a Java API with pivotal microservices, which can be easily decentralized. Our approachs next stage and vision will cover some enhancements to the current architecture then propose a according to governmental standards and policies

Blockchain is attracting attention as a new solution for problems such as illegal copying, profit distribution, and forgery and falsification in the digital content trading environment, which has become an essential asset in the information age. However, one problem is that it is difficult to propagate digital content to the blockchain network because of a limited capacity to upload to the blockchain.

The integrity and transparency of blockchain are also considered as weak points in terms of privacy. In this paper, we propose a new blockchain system, the secret block-based blockchain (SBBC), to address the problems with the blockchain system in the digital content trading environment. SBBC is composed of off-chain and on-chain network components. Off-chain is the part that allows trading digital content through the authentication phase. The digital content that is traded has a digital fingerprint inserted, so if an illegal leak occurs, the destination can be tracked. In addition, the content is encrypted and traded, and only the rightful user can use the digital content, thus ensuring income for the legitimate content author. Next, the on-chain network is licensed to use digital content, and a verification process using a consensus algorithm is performed.

The licensed consumer creates a secret block of their transaction and records it only on their ledger. In a private part, secret block creation ensures privacy and solves the network overload that can occur when uploading digital content to the blockchain.

III. RELATED WORK

A. Problem Statement

Currently, the challenges facing digital copyright protection include the proliferation of copyright infringement, loopholes in copyright registration, difficulties in enforcing rights, and low public awareness of copyright protection. These problems are particularly evident in digital recipes, as numerous chefs and food enthusiasts share and upload their unique works on various apps, making the task of copyright protection increasingly arduous. Therefore, we need to find an innovative way to address these issues, protect the rights of creators, and promote the healthy development of the digital recipe field.

B. Domain Overview

The Blockchain is an encrypted, distributed database that records data, or in other words it is a digital ledger of any transactions, contracts - that needs to be independently recorded. One of the key features of Blockchain is that this digital ledger is accessible across several hundreds and thousands of computer and is not bound to be kept in a single place. Blockchain chain has already started disrupting the financial services sector, and it is this technology which underpins the digital currency- bitcoin transaction. With Blockchain technology in financial sector, the participants can interact directly and can make transactions across the internet without the interference of a third party. Such transactions through Blockchain will not share any personal information regarding the participants and it creates a transaction record by encrypting the identifying information.

The most exciting feature of Blockchain is that it greatly reduces the possibilities of a data breach. In contrast with the traditional processes, in Blockchain there are multiple shared copies of the same data base which makes it challenging to wage a data breach attack or cyber-attack. With all the fraud resistant features, the block chain technology holds the potential to revolutionize various business sectors and make processes smarter, secure, transparent, and more efficient compared to the traditional business processes.

C. Drawbacks of Existing System

Cannot handle hundreds of transactions per second. Tough to crack violently, the risk of a data breach still exists. Lacks of transaction data protection in their Ethereum module during the whole process. Requires large amount of resources in mining phase. The current implementation can only be considered to guarantee liveness for one failure.

D. Proposed System

Blockchain faithfully records each new data generation and puts an indelible record of the time of each new data generation, just like a steel stamp. As new data keep increasing, each newly generated data block is linked to the previous data block by an encryption algorithm and passed to the next data block, and the new data of the latter data block are also confirmed and recorded by the previous one, which forms a nearly infinite blockchain with first and last links, and one timestamp also forms an uninterrupted continuous time record, and this record is distributed and recorded in all.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

This record is distributed in the data blocks of all participants so that all participants can trace the whole process of data changes. Each transaction record of the digital copyright information will be timestamped and recorded throughout the entire process.
By querying the public blockchain or requesting the private key from the copyright owner to query the nonpublic blockchain at the time of transaction, the entire traceability of the information from creation to several transactions can be realized. The term smart contract originated from cryptographer Nick Szabo, which means the organic combination of computer computing and contract, by setting the starting conditions of the computer computing code in advance; once the trigger occurs, the computer can automatically execute the contents of the contract. The most common form of this model is the vending machine, where the seller sets the price of each item in the vending machine in advance and sets that once the product is selected and the corresponding amount of currency is invested, then the vending machine will automatically ship the product, and if the corresponding amount is not reached, then the coins will be automatically refunded.

E. Advantages of Proposed System

Consistent with the traceability requirements of information. Become inherently resilient to single points of failure and are less vulnerable to hacking attempts.It is highly scalable, making it suitable for a variety of applications. Speed: Provides faster processing of transactions. Efficiency: Consumes less energy. Can balance robustness and vulnerability.

IV. IMPLEMENTATION

A. Key Features

1) *Decentralized:* The basic structure of blockchain, the network is decentralized, meaning it has no need to rely on any server or node. The data can be recorded, stored, and updated by a group of nodes.
2) *Transparency:* When data is transmitted on the blockchain, records on each node are open and transparentthis is the reason that blockchain can be trusted.
3) *Open Source:* The records of blockchain systems are publicly verifiable for any user, and the user can also use the blockchain system to develop any application.
4) *Autonomy:* Based on the consensus mechanism, each node in the blockchain can transmit or update data to each other in a secure situation. This idea is from a single entity to the entire system so that no one can interfere with it.
5) *Immutable:* Any records will always be kept and stored and will not be altered unless the remaining nodes have a record where greater than 51% of the record will be changed.
6) *Anonymity:* The blockchain technology solves the problem of trust on the node-to-node, so the data transmission or the transaction can be hidden, and only when the traders blockchain address is known will it be exposed.

B. Blockchain Data Upload and Download

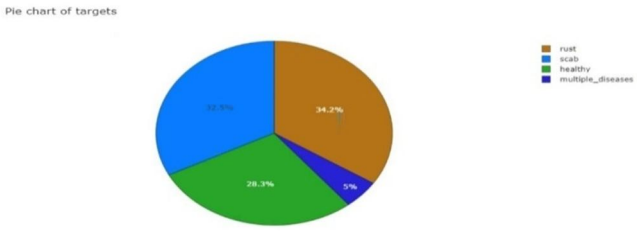
The user interaction of a digital copyright protection system consists of two main aspects: uploading and downloading data. In our Ethereum-based digital copyright protection system for blockchain recipes, first, a user registers, and the system automatically generates a public/private key pair. The public key is used for external data encryption, while the private key, known only to the user, is employed to decrypt received data. Furthermore, the private keys storage on the server is encrypted, offering dual-layer protection. The system also allows users to easily update or revoke their keys if they suspect their keys security is compromised.
Through this method, we ensure the integrity and security of user credentials.A creator (e.g., Alice) uploads their recipe by invoking a smart contract.When an unauthorized use event occurs, Alice can quickly retrieve all transaction records related to her in the side chain through the smart contract TransactionQueryContract using the recipe ID and her public key as input.
This has important implications for copyright protection because the information on the side chain can be used as legally valid evidence to prove her ownership if there is any dispute. All transactions are timestamped with the involved parties public keys, confirming that at a particular point in time, Alices recipes were downloaded by a specific user. In addition, because these records are on the blockchain, they are immutable, which provides strong evidence for resolution of copyright disputes.

C. System Design

Our proposed digital copyright protection system is a multilayer, multirole network system initially designed to fulfill the needs of digital recipe copyright protection in a distributed network environment. The system, as a whole, is divided into a user layer, application service layer, node layer, contract layer, consensus layer, and data layer.

The user layer is mainly composed of creators and customers, which interact with the system through the client. Users can switch roles according to their needs to complete the uploading and downloading of recipes. The service layer contains four main modules: copyright application, audit, transaction, and traceability. It is primarily responsible for accomplishing the overall functional requirements. The node layer is divided into interaction nodes and processing nodes. Interaction nodes represent user interaction nodes, which are primarily involved in user interaction, including creating, uploading, downloading, and decryption of recipes. Processing nodes are responsible for data processing, validation, and storage. The contract layer mainly realizes the modules used by the server side. Transactions are quickly agreed upon between nodes in a distributed system.

To ensure the security and integrity of transactions, we introduce an authentication system. Each node that participates in the consensus needs to go through an authentication process that ensures that it is a registered and trusted node. In addition, we design a credential management system to store, update, and revoke the credentials of nodes. This ensures that only nodes with valid credentials can participate in the consensus process, enhancing the security of the system. The data layer is divided into the main chain and side chain. The main chain stores the hash address of the users data. It ensures that the creators work is public and cannot be tampered with. The side chain holds the users copyright transaction information, which is convenient for later rights holders to trace the copyright.



V. CONCLUSION AND FUTURE WORK

A. Conclusion

The existing zero watermarking algorithm has the disadvantages of a long audit cycle, easy copyright loss, and difficult copyright ownership confirmation due to the requirement of copyright authentication we proposed a zero watermarking algorithm based on the angular features of concentric circles with strong robustness. This algorithm constructs concentric circles with angular information from many inflection points in the line and area vector elements and generates multiple sequences of zero watermarking. The experiments show that the proposed algorithm reflects strong robustness under common watermark attacks, such as rotation, cropping, and compression, with different intensities and satisfies the requirement of uniqueness. This article fully combines zero watermarking and blockchain technology to achieve a lossless data protection scheme. When a copyright dispute occurs, the copyright information can be extracted with a public algorithm and compared with the same information stored on the blockchain to achieve copyright protection for the lossless vector map. This provides a new way of thinking about zero watermarking copyright authentication.

B. Future Works

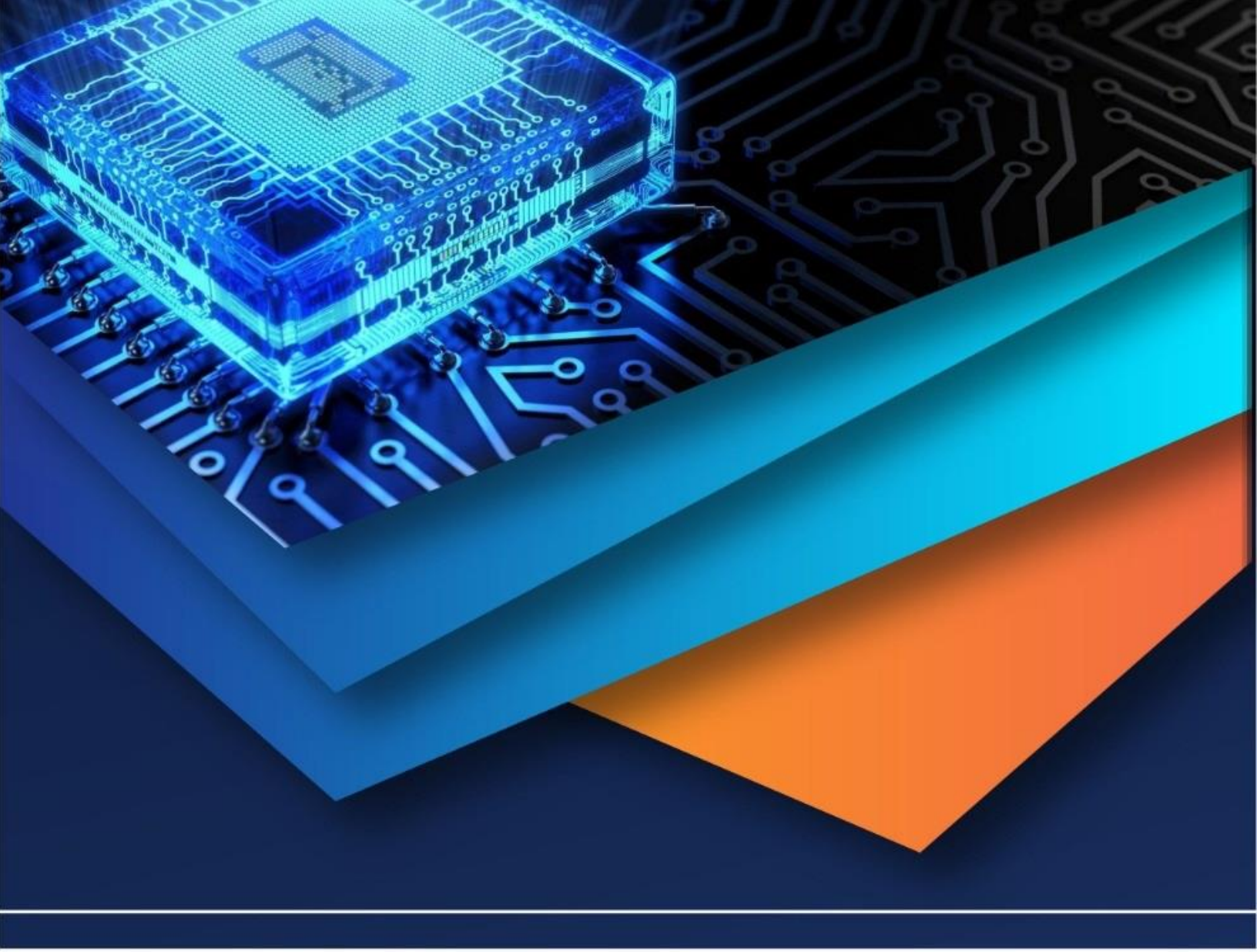
In future work, we will fully combine the trusted execution environment SGX enclave to ensure the security of smart contract. Specifically, we will put the calculation with high complexity into the enclave for execution and use RSA encryption mode to securely transmit the calculation results. One can also securely block an enclave in order to control the calling rights of the smart contract. In addition, we believe it makes more sense to use non-fungible tokens (NFTs) for copyright protection because NFTs are in the system from the creation of the work, the entire transaction process is recorded through smart contracts, and each work has a unique ID that makes it impossible to pirate.



REFERENCES

[1] Zhini Cai Usage of Deep Learning and Blockchain in Compilation and Copyright Protection of Digital Music IEEE Access, 2020
[2] Lijun Xiao,Weihong Huang,Yong Xie,Weidong Xiao,Kuan-Ching Li A Blockchain-Based Traceable IP Copyright Protection Algorithm IEEE Access, 2020
[3] Emanuele Bellini,Youssef Iraqi,Ernesto Damiani Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey IEEE Access, 2020
[4] Gabin Heo,Dana Yang,Inshil Doh,Kijoon Chae Efficient and Secure Blockchain System for Digital Content Trading IEEE Access, 2021
[5] Jun Lin,Wen Long,Anting Zhang,Yueting Chai Blockchain and IoT-based architecture design for intellectual property protection International Journal of Crowd Science, 2020
[6] S. Johar,N. Ahmad,A. Durrani,G. Ali Proof of Pseudonym: Blockchain-Based Privacy Preserving Protocol for Intelligent Transport System IEEE Access, 2021
[7] Kentaroh Toyoda,Koji Machi,Yutaka Ohtake,Allan N. Zhang Function-Level Bottleneck Analysis of Private Proof-of-Authority Ethereum Blockchain IEEE Access, 2020
[8] Yan Yang,Xingyuan Chen,Hao Chen,Xuehui Du Improving Privacy and Security in Decentralizing Multi-Authority AttributeBased Encryption in Cloud Computing IEEE Access, 2018
[9] Noussair Fikri,Mohamed Rida,Nourredine Abghour,Khalid Moussaid,Amina El Omri,Mounia Myara A Blockchain Architecture for Trusted Sub-Ledger Operations and Financial Audit Using Decentralized Microservices IEEE Access, 2022
[10] Yao-Tsung Yang,Li-Der Chou,Chia-Wei Tseng,Fan-Hsun Tseng,Chien-Chang Liu Blockchain-Based Traffic Event Validation and Trust Verification for VANETs IEEE Access, 2019
[11] E. Fiordalisi, The tangled web: Cross-border conflicts of copyright law in the age of internet sharing, Loy. U. Chi. Int. L. Rev., vol. 12, no. 2, pp. 197-213, 2015.
[12] L. Ruth Okediji, The limits of international copyright exceptions for developing countries, Vanderbilt JETLaw, vol. 21, no. 3, pp. 689, 2019.
[13] F. Cantatore, Publishing and the Law: Copyright and Globalisation, Newcastle Upon Tyne, U.K.:Cambridge Scholars Publishing, pp. 41-64, 2019.
[14] A. Savelyev, Copyright in the blockchain era: Promises and challenges, Comput. Law Secur. Rev., vol. 34, no. 3, pp. 550-561, Jun. 2018.
[15] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad and N. C. Debnath, Blockchain for smart cities: A review of architectures integration trends and future research directions, Sustain. Cities Soc., vol. 61, Oct. 2020.
[16] S. H. Didwania, Copyright protection and cumulative creation: Evidence from early twentieth-century music, J. Legal Stud., vol. 47, no. 2, pp. 235-268, Jun. 2018.
[17] C. Guo, J. Lu, Z. Tian W. Guo and A. Darvishan, Optimization of critical parameters of pem fuel cell using tlbo-de based on elman neural network, Energy Convers. Manage., vol. 183, pp. 149-158, Mar. 2019.
[18] D. Herremans and C.-H. Chuan, The emergence of deep learning: New opportunities for music and audio technologies, Neural Comput. Appl., vol. 32, no. 4, pp. 913-914, Apr. 2019.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)