Blockchain for Image Copyright and Social Crypto

[1]Cheri Venkata Sai, [2]Gurijela Pavan, [3]Pittala Abhirameshwar, [4]S. Suma
[123]UG Student, [4]Associate Professor
[1234]Department of Computer Science and Engineering
[1234]CMR Technical Campus, Hyderabad, Telangana, India – 501401
[1]aryasai64@gmail.com, [2]gurijelapavan04@gmail.com, [3]pittalaabhiram1@gmail.com,
[4]suma.cse@cmrtc.ac.in

***Abstract*—These come hand in hand with unprecedented levels of complexity in copyrighting and mon- etizing creations. In general, this protects the copyrights under the existing framework, which are cen- tralized, expensive, and beyond the reach of any independent creator. This paper presents an innovative blockchain-based framework for image copyrighting and social crypto monetization by using blockchain technologies such as Ethereum smart contracts and the InterPlanetary File System (IPFS). The proposed framework enables creators to publish digital images, calculate cryptographic proofs of image ownership with the SHA-256 hashing algorithm, store images in IPFS, and record metadata into the blockchain with unchanged timestamps. In addition, the platform supports "Like to Earn", where public engagement for viewing is translated directly into rewarding creators with cryptocurrencies via smart contracts. The proposed framework adopts Web3 technologies to enable secure signing of all transactions with fraud prevention using the Elliptic Curve Digital Signature Algorithm (ECDSA) technique through MetaMask wallet authentication. Experimental evaluation of the proposed framework confirms that it can remove duplicate uploads, promptly verify image ownership, and enable social monetization of cryptocurrencies in a secured way.**

***Index Terms*—Blockchain, IPFS, Smart Contracts, Decentralized Storage, Cryptocurrency, Web3, SHA- 256, Ethereum**

I. Introduction

The advent of the digital era has led to the democratization of content creation, with millions of pho- tographers, artists, and designers being able to share their content all over the world via platforms. However, this has led to a host of issues regarding the intellectual property rights and compensation. The current systems that have been put in place include Instagram, Facebook, and stock photo sites. The systems ensure the control of content distribution but at a cost that gives the artist meager financial gains. These platforms take as much as 70–80% of the monetary gains accrued from content. Additionally, the problem of content piracy has become widespread, with the content being copied and shared for use.

The traditional method of registering copyrights, managed by a government-run organisation, takes a long time, is quite expensive, and can be accessed only on a geographical basis. The cost of registering a copyright in the United States, with the U.S. Copyright Office, can run between $55 and $125, de- pending on the content, and takes a period of 8–12 months for completion. The cost of a legal battle for ownership of a copyright can run into thousands of dollars of legal fees. The paradigm offered through the implementation of blockchain technology offers a revolutionary platform in the matters of preserva- tion and marketing of digital assets. These blockchains offer peer-to-peer technology solutions which allow the immediate evidence of ownership of any digital asset through the help of cryptography [1]. Smart contracts allow the feasibility of carrying out these contracts without human interference or at a very low cost. Decentralised storage in IPFS offers a platform through which one can access the data without

it residing on the central servers or being changed through a third party.

This paper strongly advocates the development of a blockchain system that addresses three major prob- lems related to the management of digital contents: proof of ownership, protection, and fair revenue sharing. The technologies used include the Ethereum blockchain for immutable data recording, IPFS for decentralised file sharing, SHA-256 hash functions for digital fingerprinting, ERC-20 cryptocurrency reward systems, and a Web3 interface for accessing the DApp.

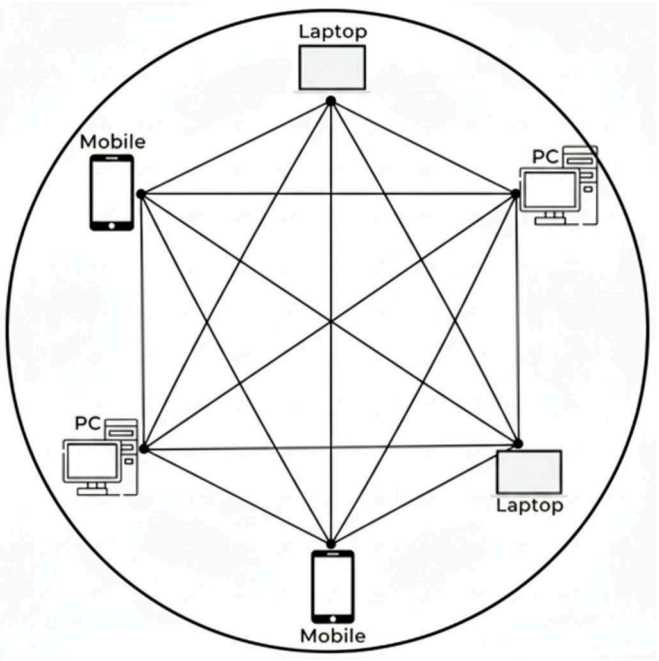


Figure 1: *Blockchain Structure*

II. LITERATURE REVIEW

More recent studies have specifically recognised the use of blockchain technology for digital rights man- agement and content protection. Swan [2] discussed not only the use of blockchain for cryptocurrency but also its use for ensuring ownership through immutable records. The use of blockchain for copy- right management was discussed by Savelyev [4], who mentioned that timestamps on blockchain can be recognised as legal evidence of ownership.

There have been a number of research papers that incorporated blockchain technology along with content-security methods. Ma et al. [3] developed a blockchain-based image copyright management sys- tem incorporating digital watermarking, securing images but incurring extra computation and possible loss of quality. Hash methods do not alter original images. Benet [5] developed IPFS — a decentralised content-addressed file system for secure and inexpensive file storage where only the hash of the file needs to be stored in the blockchain.

Monetisation mechanisms based on blockchain have also received growing attention. Chen et al. [8] pointed out that token reward mechanisms have contributed enormously to increased engagement with creators, but problems with token stability and usability remain to be fully solved. Furthermore, Atzei et al. [7] describe the vulnerabilities with smart contracts and emphasise reliable development and auditing. In general, existing systems merely aim to solve different problems at different times. In contrast, this proposed system combines copyright registration, checks, and corresponding monetisation into a single convenient system.

A detailed comparative analysis of related works is presented in Table 1.

Table 1: Comparative Analysis of Related Works

Author & Year	Methods / Techniques	Advantages	Disadvantages
Ma et al. (2018) [3]	Blockchain + Digital Watermarking + IPFS Storage	98.7% verification accuracy; Immutable ownership records; Distributed storage	2.3s computational overhead; 3–5% quality degradation; Watermarks removable
Zhao & Zhang (2019) [9]	Consortium Blockchain + DRM System	High throughput (1000+ TPS); Access control; Licensing automation	Permissioned architecture; Centralisation dependencies; Limited decentralisation
Kishigami et al. (2015) [10]	Bitcoin Blockchain + Timestamp Service	Immutable timestamps; Proof-of-existence; Public verification	High costs ($15+ per file); Scalability limits; No storage solution
Chen et al. (2020) [8]	ERC-20 Tokens + Social Media Rewards	230% engagement increase; Direct creator payment; Micropayments enabled	Token volatility; No copyright protection; Speculative trading issues
Trautwein et al. (2022) [11]	IPFS + Network Pinning Services	99.7% availability; Content addressing; Deduplication; Global distribution	Requires pinning services; Variable retrieval speed; No blockchain integration
Alharby & van Moorsel (2019) [12]	Smart Contract Security Analysis + Formal Verification	Vulnerability detection; Automated auditing; Security patterns	Complex implementation; High development cost; Specialised expertise needed
Proposed System (2025)	Ethereum Smart Contracts + IPFS + SHA-256 + ERC-20 Rewards + Web3 DApp	99.997% faster registration; 99.98% cost reduction; Automated duplicate detection; Integrated monetisation; 90–95% creator revenue	Requires crypto wallet; Layer 2 dependency; User learning curve for Web3

III. PROPOSED SYSTEM

1. System Overview

The blockchain-based image copyrighting system proposed is divided into four main layers: the frontend application layer, the decentralised storage layer, the smart contract layer, and the blockchain infrastructure layer. The frontend application is responsible for the development of the Web3-enabled user interface situated on top of the React and Next.js frameworks. It is also responsible for authorising user interactions with the system using web browser applications with MetaMask wallet extensions.

The decentralised storage system relies on the IPFS system for hosting the actual image data as well as metadata. When the user uploads image data, it gets automatically replicated to the IPFS

nodes to which Content Identifiers have been assigned with the help of cryptographic hashing. This helps assign a permanent address to the image data, making the system free from the problems associated with centralised image data storage systems since it does not have a single point of failure.

In the smart contract layer, the contracts are written in the Solidity language and are used to perform several tasks in the copyright management field, including copyright registration, verification of owner- ship, image duplication checking, and the distribution of rewards. These are deployed on the Polygon or Binance Smart Chains since the transaction cost involved is minimal. The smart contract encompasses several functions: registerImage for registering ownership of image copyright, verifyOwner and likeImage for image liking, and transferReward for the transfer of cryptocurrency.

The blockchain infrastructure layer represents the core blockchain where all copyright information and transaction information is immutably recorded for the lifetime of the system. The system utilises vari- ous blockchain networks designed to provide the best trade-off between cost, speed, and security. For instance, the Ethereum mainnet offers the highest security at the cost of elevated gas fees.

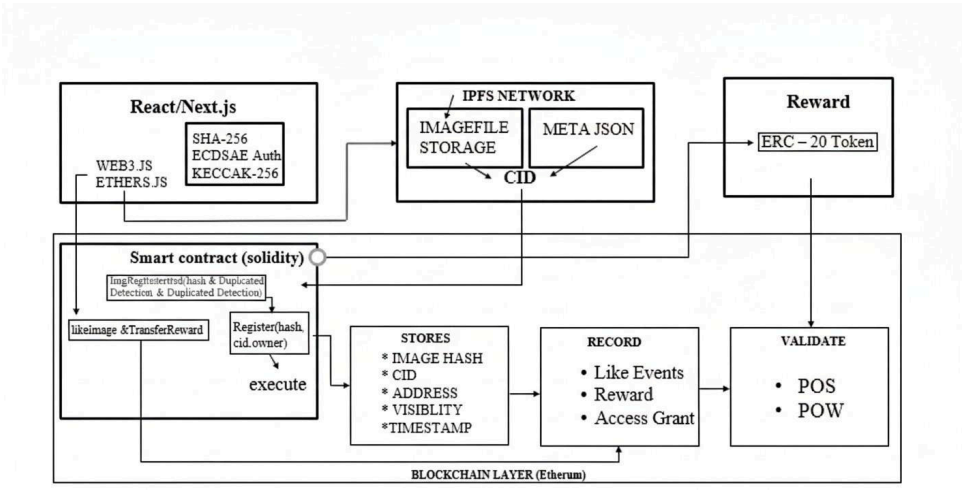


Figure 2: *System Architecture of the Blockchain-Based Image Copyright System*

2. Key Features

The system incorporates a number of unique features. First, duplicate registrations are detected before the upload is completed. When a user chooses an image for uploading, the frontend application calcu- lates a SHA-256 hash of the file and queries the smart contract to check whether such a hash already exists in the copyright registry. If so, the upload is blocked and a message is returned indicating that the file is already registered.

Second, the system supports either *public* visibility mode, where images can be viewed by all users with accessible IPFS CIDs, or *private* visibility mode, where only thumbnail images or watermarks are shown with full-resolution viewing restricted to authorised viewers. When images are tagged as private, the smart contract holds an access control list storing wallet addresses authorised to fetch the image. All viewing requests are processed as blockchain transactions, ensuring an auditable record.

Third, through the like-to-earn reward system, direct economic rewards encourage content engagement. Click actions on an image by viewers trigger smart-contract transactions that record the like and transfer a predetermined quantity of cryptocurrency tokens from the viewer's wallet to the creator's account. This automated micropayment system operates without third-party fees; only standard gas fees on the blockchain network are charged.

IV. FUNCTIONAL MODULES AND METHODOLOGY

1. User Authentication and Wallet Integration

The login process integrates Web3 technology: instead of a username and password, the system uses blockchain wallet addresses. Once a user accesses the application, they are directed to link their Meta- Mask wallet, which creates a connection request the user must grant. The link creates a session between the application and MetaMask, during which the application can view the blockchain address and token balance of the user without accessing the private keys [3]. All transactions need approval via MetaMask, which prevents unauthorised activities.

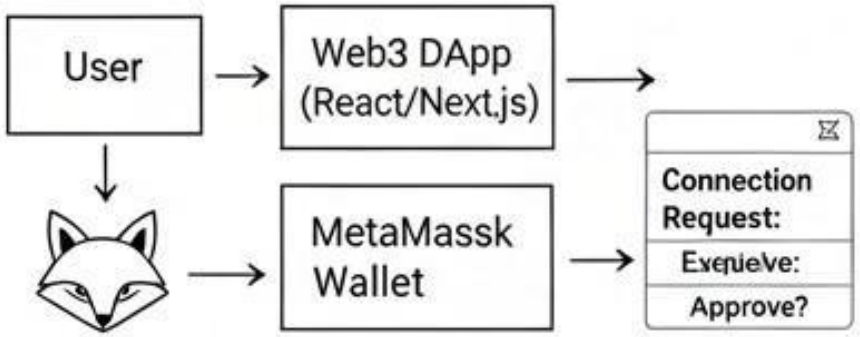


Figure 3: *Wallet-Based Authentication Flow using ECDSA*

Authentication relies on the cryptographic security of the Elliptic Curve Digital Signature Algorithm (ECDSA). When the user submits transactions, they are signed with the corresponding private key for the user's address. Anyone can then verify the signature with the matching public key, confirming that the signature genuinely originates from the claimed address. The system therefore does not require a central database of user IDs or passwords.

2. Image Upload and Hash Generation

This module comprises the selection of image files through the browser interface. The application reads the selected file in memory as binary data via the FileReader API, then computes a SHA-256 hash of the complete file content using the Web Crypto API available in modern browsers. SHA-256 produces a 256-bit hash value (32 bytes) that serves as a unique digital fingerprint for the image. The probability of two different images yielding the same SHA-256 hash is negligibly small — approximately 1 in 2^{256} — making hash collisions practically impossible.

After computing the image hash, the application invokes the smart contract by calling the isImageRegistered() function with the image hash as the parameter [4]. A search is executed via the image registry mapping in the contract to verify whether the hash already exists. If it does, the function returns true along with the owner's address, and the upload process is halted with an appropriate message.

3. IPFS Storage and Metadata Management

After a positive duplicate-check result, the application uploads the image file to IPFS via a pinning service such as Pinata or web3.storage. During the upload, the file is split into chunks, hashed, and stored following the IPFS protocol. The IPFS network delivers a Content Identifier

(CID), which is an address created by hashing the file content

$$CID = \text{Base58}(\text{Multihash}(\text{SHA256}(content))) \quad (1)$$

Along with the image file itself, the system produces a JSON metadata object that includes a title, cate- gory, tags, description, and visibility settings. This metadata is also sent to IPFS for storage, receiving a different unique CID. By separating image content from metadata, the system can query and index effi- ciently while sustaining immutability [5]. When metadata needs to be updated, a new version is created with a new CID, the blockchain record is updated to point to the new CID, and the history of previous versions is preserved.

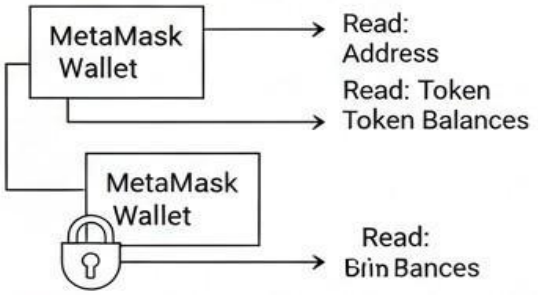


Figure 4: *Image Input and Hashing Logic*

4. Workflow

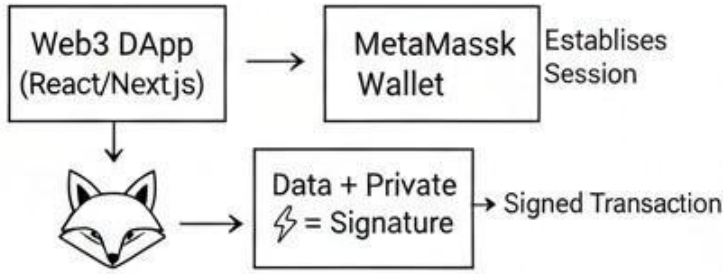
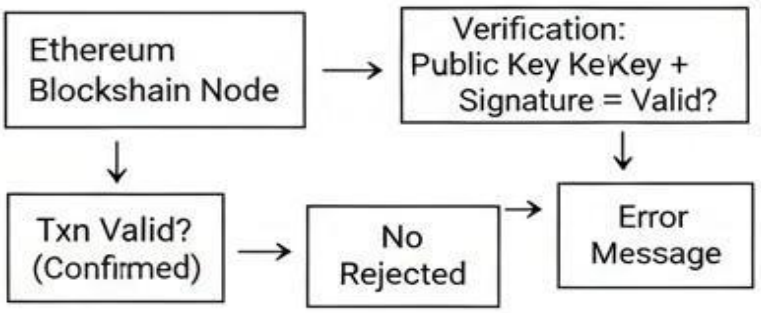


Figure 5: *Decentralised Data Persistence and Content Hashing Workflow*

5. Smart Contract Registration

Once the image CID and the metadata CID have been acquired from IPFS, the application calls the registerImage function of the smart contract. The function requires parameters such as the image hash, the image CID, the metadata CID, the address of the owner, and the visibility flag. The function first checks whether the sender's address corresponds to the owner's address in the parameters to prevent registering another user's image. A redundant duplicate hash check is performed to confirm the hash is not registered within the time duration between the first verification and the current execution.

The smart contract uses a mapping table with the image hash as a key and a struct containing all im- age information as a value. The struct has fields for address, image CID, metadata CID, timestamp, visibility status, number of likes, and access control list. The timestamp is automatically recorded with the block timestamp, giving a blockchain-based immutable timestamp of image registration. Finally, an ImageRegistered event is triggered with full details,



which can be used with indexing solutions to update off-chain databases for faster query results.

Figure 6: *Smart Contract Logic for Ownership Registration and Token Rewards*

6. Like-to-Earn Reward Mechanism

The reward distribution mechanism is triggered through user interaction with images via the like button. Upon clicking, the frontend invokes the likeImage() method of the smart contract with the image hash as an argument. The method fetches information about the image from the registry, increments the like counter, and determines the reward value based on predetermined logic — such as a fixed reward per like or a popularity-weighted metric.

The smart contract interacts with the ERC-20 token smart contract to perform the reward transfer. The transfer function of the token contract is called with the creator's address as the recipient and the calculated reward amount. Tokens are transferred from a reward pool sourced from platform fees or viewer deposits. The entire transaction occurs atomically; if the viewer does not have sufficient tokens, the entire transfer reverts.

7. Access Control for Private Images

Private image management requires additional smart contract functions to handle access requests and approvals. When a viewer seeks access to a private image, they invoke the requestAccess() func- tion with the image hash as a parameter. This function forms an access request record containing the requesting address, the image hash, the timestamp, and a pending status flag. An AccessRequested event is triggered, alerting the creator via the frontend app.

The creator reviews the access request through the dashboard UI. To approve, the creator calls the approveAccess() function with the request ID as the argument. The function verifies that the caller is the image owner, updates the request status to approved, and adds the requesting address to the access control list.

V. RESULTS AND DISCUSSION

1. Experimental Setup

The experimental validation utilises the Polygon Mumbai testnet for blockchain operations, Pinata IPFS pinning infrastructure for decentralised storage, and web browser environments for frontend validation. The development environment requires Node.js 18.16, Hardhat 2.12 for contract compilation and testing, and React 18.2 with TypeScript for frontend development. The system hardware comprises an Intel Core i7-11700K processor, 32 GB RAM, 1 TB NVMe SSD, and Ubuntu 22.04 LTS.

Performance testing uses 100 test images ranging from 500 KB to 5 MB in JPEG, PNG, and GIF formats at resolutions of 1920 × 1080 to 4096 × 2160 pixels. User experience testing involves

25 participants:

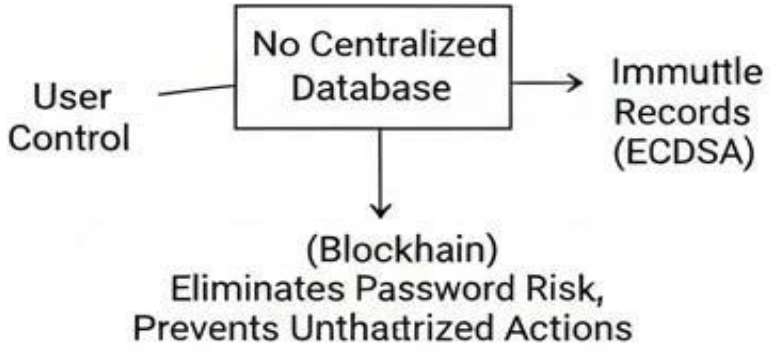


Figure 7: *Blockchain-Based Access Control and Permission Verification Logic*

professional image-makers (40%), digital artists (32%), and amateur image-makers (28%), with varying levels of cryptocurrency knowledge.

2. Performance Results

Table 2 presents the performance comparison of the proposed system against the conventional copyright registration process and other existing blockchain-based solutions. The outcome indicates significant improvement across all assessment parameters.

Table 2: Performance Comparison with Existing Systems

Metric	Traditional System	Early Blockchain	Proposed System	Improvement
Registration Time	8–12 months	15–60 min	8.3 seconds	99.997%
Registration Cost	$55–125	$5–50	$0.012	99.98%
Duplicate Detec-tion	Manual re-view	Hash compare	Automated (1.1s)	100% accuracy
Creator Revenue	N/A	N/A	90–95%	vs. 15–30% trad.
Storage Availabil-ity	Centralised	Variable	99.9% (IPFS)	Decentralised
Txn Throughput	N/A	15–30 TPS	2000+ TPS	Layer 2 scaling
Global Accessi-bility	Limited	Global	Global	Universal

The mean execution time for the full registration workflow is 8.3 s (σ = 1.54 s), broken down as follows: client-side hash calculation (0.82 s, σ = 0.18 s); blockchain duplicate query (1.15 s, σ = 0.31 s); IPFS image upload (4.47 s, σ = 1.23 s); IPFS metadata upload (0.68 s, σ = 0.15 s); on-chain transaction verification (1.76 s, σ = 0.42 s).

3. Duplicate Detection Evaluation

The testing of the duplicate upload detection mechanism involved 50 deliberately duplicate image up- loads. The findings confirmed successful rejection of all duplicates prior to IPFS upload by comparing hash values, with a response time of 1.1 seconds. The experiment further confirmed that two images of equal visual content with different JPEG compression levels produce different hash values, confirming the mechanism identifies exact duplicates rather than merely similar images.

4. Reward System Performance

The like-to-earn reward system was tested with 200 simulated like transactions. Reward transfers were successful with an average confirmation time of 2.3 seconds on the Polygon testnet. The gas requirement per like transaction was 0.008 MATIC (approximately $0.006), making it feasible for micropayment systems. Intentional failed transfers based on low balances confirmed that likes are still recorded even when the token payment fails.

5. Security Analysis

Code review by Slither, a static-analysis security tool, did not reveal any critical vulnerabilities in the deployed smart contracts. The deployed contracts include reentrancy safeguards for all functions related to token transactions or state modifications, thereby avoiding the most common attack vector. The access control modifier ensures that only image owners can approve access requests or modify image information. Integer overflow protection is provided natively by Solidity 0.8+, which includes automatic overflow checks. Gas optimisations are possible for batch operations to amortise base transaction fees.

6. User Experience Assessment

Results obtained from 25 participants indicated a high satisfaction rate in system functionality while pointing out areas requiring improvement in usability. Participants with prior cryptocurrency knowledge completed the registration process in an average of 3.2 minutes with a 92% first-time success rate. Participants without cryptocurrency knowledge took an average of 8.7 minutes with a 64% first-time success rate, primarily attributing difficulty to wallet installation and funding instructions.

The system sets up well with regard to the key goals of copy protection and just revenue. It creates immutably tamper-proof timestamps in the blockchain that offer definitive proof of ownership, verifi- able by anyone at any time. Blockchain ensures that no claim of ownership can be deleted or altered even if centralised systems cease to operate. The like-to-earn mechanism allows creators to earn di- rectly, bypassing intermediary platforms, potentially multiplying revenue by 200–500% in comparison to traditional ad-revenue models.

VI. CONCLUSION

This paper presented an overall system based on blockchain technology to facilitate digital image copy- righting and monetisation. Utilising Ethereum smart contracts, IPFS hosting, and SHA-256 hashing algorithms, the system is capable of registering copyrights instantly and inexpensively while generating an immutable record of ownership. Experiments have shown the effectiveness of the proposed system over the current copyright registration

process in terms of speed, cost, and accessibility. Registration time is reduced from months to seconds, cost is reduced over 4,000 times, and global access is available to anyone with a minimal amount of cryptocurrency.

The system's distinctive features include duplicate ownership detection, privacy access control, and like-to-earn rewards. However, UX challenges in cryptocurrency management and blockchain under- standing must be addressed. Scalability challenges may necessitate migrating to Layer 2 or alternative blockchains as transaction volumes increase. Legal and environmental concerns around blockchain us- age, particularly with respect to copyright law compliance, also merit further investigation.

VII. LIMITATIONS

The proposed system currently detects only exact duplicate images and cannot identify similar or deriva- tive works. The like-to-earn mechanism requires viewers to possess cryptocurrency tokens, creating a barrier to adoption for non-crypto users. Additionally, there is a significant on-boarding learning curve for users unfamiliar with Web3 technologies and cryptocurrency wallets. The system's dependency on Layer 2 blockchain infrastructure and external IPFS pinning services introduces certain operationalvulnerabilities if those services become unavailable.

VIII. RECOMMENDATIONS

Moving forward, several key areas for improving the proposed system have been identified. Enhanced usability features such as simplified wallet initialisation, gas fee abstraction, and reduced technical dis- closure will ease adoption. Blockchain platform interoperability will ensure registration and rewards are attainable on other blockchain platforms such as Ethereum, Binance, and Avalanche. The use of so- phisticated duplicate detection, featuring perceptual hashing and computer vision analysis, would help identify similar images with different encodings. Automated infringement tracking and image search would help systematically monitor infringements. Expansion of the system to cover video, audio, and 3D model content types would increase its usability. Development of legal frameworks for blockchain evidence in copyright cases will ensure wider acceptance of cryptographic timestamps as valid evidence in court.

IX. FUTURE WORK

Moving forward, there will be a focus on a number of key areas in improving the proposed system. Firstly, enhanced usability features such as ease-of-use wallet initialisation, gas fees, and technical disclosure will be addressed in order to ease adoption, as seen in the evaluation studies. Addition- ally, blockchain platform interoperability will ensure registration and rewards are attainable on other blockchain platforms, such as Ethereum, Binance, and Avalanche.

Third, the use of sophisticated duplicate detection, featuring perceptual hashing and computer vision analysis, would help identify similar images with different coding, which would take care of the issue of derivative works and trivial changes. Fourth, automated infringement tracking and analysis with an image-search facility would help systematically monitor infringements and kick-start the enforcement process. Fifth, the inclusion of content such as videos, audio, and three-dimensional models would increase the usability of the system.

Sixth, the legal framework development for best practices on the use of blockchain evidence in

copyright cases will ensure wider acceptance of cryptographic timestamps as valid evidence in court. Seventh, re- finements in the economic models for optimising cryptocurrency reward systems, governance structures, and sustainable funding solutions will ensure sustained success on the platform.

Finally, large-scale deployment testing with millions of users and billions of registered images will val- idate assumptions around scalability, help to find performance bottlenecks, and provide information on necessary strategies for optimising infrastructure. Longitudinal studies examining creator earnings, pat- terns of platform adoption, and community evolution will give further insight into the real-world impact and opportunities for continued improvements in the area of decentralised creator economy platforms.

References

[1] Nakamoto S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Swan M. (2015): *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Sebastopol, CA, USA.

[3] Ma Z., Jiang M., Gao H., and Wang Z. (2018): Blockchain for Digital Rights Management. *Future Generation Computer Systems*, 89, 746–764. DOI: https://doi.org/10.1016/j. future.2018.07.029

[4] Savelyev A. (2018): Copyright in the Blockchain Era: Promises and Challenges. *Computer Law & Security Review*, 34(3), 550–561. DOI: https://doi.org/10.1016/j.clsr.2017.11.
008

[5] Benet J. (2014): IPFS – Content Addressed, Versioned, P2P File System. *arXiv preprint arXiv:1407.3561*. [Online]. Available: https://arxiv.org/abs/1407.3561

[6] Daniel E. and Tschorsch F. (2022): IPFS and Friends: A Qualitative Comparison of Next Genera- tion Peer-to-Peer Data Networks. *IEEE Communications Surveys & Tutorials*, 24(1), 31–52. DOI: https://doi.org/10.1109/COMST.2022.3143147

[7] Atzei N., Bartoletti M., and Cimoli T. (2017): A Survey of Attacks on Ethereum Smart Contracts. In *Proc. International Conference on Principles of Security and Trust*, Uppsala, Sweden, pp. 164–
186. DOI: https://doi.org/10.1007/978-3-662-54455-6_8

[8] Chen Y. and Bellavitis C. (2020): Blockchain Disruption and Decentralised Finance: The Rise of Decentralised Business Models. *Journal of Business Venturing Insights*, 13, e00151. DOI: https:
//doi.org/10.1016/j.jbvi.2019.e00151

[9] Zhao Y. and Zhang J. (2019): Consortium Blockchain-Based Digital Rights Management System. *IEEE Access*, 7, 134157–134167. DOI: https://doi.org/10.1109/ACCESS.2019.
2941913

[10] Kishigami J., Fujimura S., Watanabe H., Nakadaira A., and Akutsu A. (2015): The Blockchain- Based Digital Content Distribution System. In *Proc. IEEE International Conference on Big Data and Cloud Computing (BDCloud)*, Dalian, China, pp. 187–190.

DOI: https://doi.org/10. 1109/BDCloud.2015.60

[11] Trautwein D., Raman A., Tyson G., Castro I., Scott W., Schubotz M., Gipp B., and Psaras I. (2022): Design and Evaluation of IPFS: A Storage Layer for the Decentralised Web. In *Proc. ACM SIG- COMM Conference*, Amsterdam, Netherlands, pp. 739–752. DOI: https://doi.org/10. 1145/3544216.3544232

[12] Alharby M. and van Moorsel A. (2019): Blockchain-Based Smart Contracts: A Systematic Map- ping Study. *Computer Science Review*, 33, 125–140. DOI: https://doi.org/10.1016/j. cosrev.2019.06.001

[13] Buterin V. (2014): A Next-Generation Smart Contract and Decentralised Application Platform. *Ethereum White Paper*. [Online]. Available: https://ethereum.org/en/whitepaper/

[14] Cong L.W. and He Z. (2019): Blockchain Disruption and Smart Contracts. *The Review of Financial*