International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Blockchain–AI Hybrid Framework for Preventing Copyright Fraud: A Novel Approach for Secure Digital Content Protection

1st Gowher Shafi
Lovely Professional University
Jalandhar, Punjab, India
gowhershafi.gs@gmail.com

2nd Abhinav Kumar
Lovely Professional University
Jalandhar, Punjab, India
abhinav353637@gmail.com

3rd Satyam Kumar
Lovely Professional University
Jalandhar, Punjab, India
satyamkumarsingh705071@gmail.com

4th Pitamber Kumar Mahto
Lovely Professional University
Jalandhar, Punjab, India
pitamberkumar5555@gmail.com

5th Raj Mishra
Lovely Professional University
Jalandhar, Punjab, India
rajxmishra2003@gmail.com

6th Kartikeya Pandey
Lovely Professional University
Jalandhar, Punjab, India
kartikeyapandey111@gmail.com

7th Shubham Singh
Lovely Professional University Jalandhar, Punjab, India shubhamsinghp21@gmail.com

How to Cite this Article:

Shafi, G., Kumar, A., Kumar, S., Mahto, P. K., Mishra, R., Pandey, K. & Singh, S. (2026). Blockchain–AI Hybrid Framework for Preventing right Fraud: A Novel Approach for Secure Digital Content Protection. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.618

https://doi.org/10.55041/ijcope.v2i4.618

***Abstract*—**The rapid growth of digital content has significantly raised copyright abuses, such as unauthorized copying, transmis- sion of ownership, and distribution. Most traditional copyright protection mechanisms rely on a centralized database that can easily be circumvented, altered, or wiped, ultimately complicating ownership history disputes. This paper presents a Blockchain and AI hybrid model that provides immutable copyright registration and automatic fraud detection through content fingerprinting. On one side, Blockchain offers a decentralized, immutable ownership repository, whereas, on the other side, Artificial Intelligence tackles the task of identifying copied, modified, or plagiarized work through deep learning and pattern matching methods. Experimental results demonstrate that combining blockchain immutability with AI-driven recognition significantly mitigates fraudulent claims, strengthens creator trust, and improves trans- parency and enables a more efficient digital rights management (DRM) process [14], [22]. This work further clarifies how the proposed system is dissimilar to the available systems, thus making it a necessary evolution in digital copyright protection.

Index Terms—Blockchain, Copyright Fraud, Artificial Intel- ligence, Smart Contracts, Digital Rights Management, Content Authentication

I. INTRODUCTION

In the modern world, content has never been easier to develop with digital platforms such as YouTube, Instagram, streaming services, and online publishing. This growth has also contributed to increased copyright fraud and unauthorized redistribution of digital assets [29], [30].

Traditional copyright systems store information on cen- tralized servers. If these servers are compromised, damaged, or altered, ownership records become unreliable [28]. With millions of digital files uploaded daily, manual verification of originality is impractical.

A combination of Blockchain and Artificial Intelligence provides a strong solution. Blockchain ensures immutable ownership records using decentralized consensus mechanisms [21], [27], while AI techniques detect modified or plagiarized content using semantic and perceptual similarity analysis [8], [18].

II. LITERATURE REVIEW

Previous studies have attempted to use copyright protection in the way that they have:

Using Blockchain exclusively: previous studies have fo- cused on creating ownership records via Blockchain ledger systems. These records are immutable in nature, therefore unable to automatically verify if content is being used inappropriately, rather they require manual verification of the content [14], [27].

Using Artificial Intelligence type systems: either through the use of tools to detect possible plagiarism, tools to determine the similarities between an image, or applications to detect deepfakes. Research indicates there are some approaches available for determining if content was created illegally. However, these methods suffice, but do not create an authentic verification of original authorship [4], [8].

Digital Watermarks: Digital watermarks can easily be altered or removed, and therefore, are not trusted for longevity [12].

Centralized DRM: The terminology of Content ID utilized by companies such as YouTube has bias or alteration risks through centralized servers within an entity that have no relations or affiliations to the creators [30].

Gaps in Literature for Uniqueness: To the best of our knowledge, no prior work integrates blockchain immutability with AI-driven decision-making into a unified system for automated copyright detection and mitigation. While some studies explore blockchain for time stamping content, most systems use blockchain simply as temporary storage instead of an informed active decision component. These studies do not rely on dynamic verification methods; therefore, these systems cannot detect in real time, the presence of infringement or derivative works autonomously. This reliance on dynamic verification produces a burden on the manual flagging process, which overall makes the prevention mechanism less efficient. Some researchers have attempted hashing-based similarity checks, but hashing practices are easily breached by an at- tacker applying minor edits such as compression, style transfer, or editing. Literature notes the susceptibility of these systems and few works have considered AI-backed fingerprints which can withstand adversarial manipulations. This is a gap in research which our proposed hybrid solution seeks to address [22], [25].

III. PROPOSED SYSTEM

The proposed hybrid framework integrates blockchain and artificial intelligence into three primary modules: (1) blockchain-based ownership registration, (2) AI-driven con- tent fingerprinting and similarity detection, and (3) adaptive monitoring and fraud mitigation. Each module performs a distinct role while operating in coordination to ensure secure registration, automated verification, and continuous protection of digital assets. Each module consists of several functional components, described in the following subsections. The over- all system architecture is illustrated in Fig. 1.

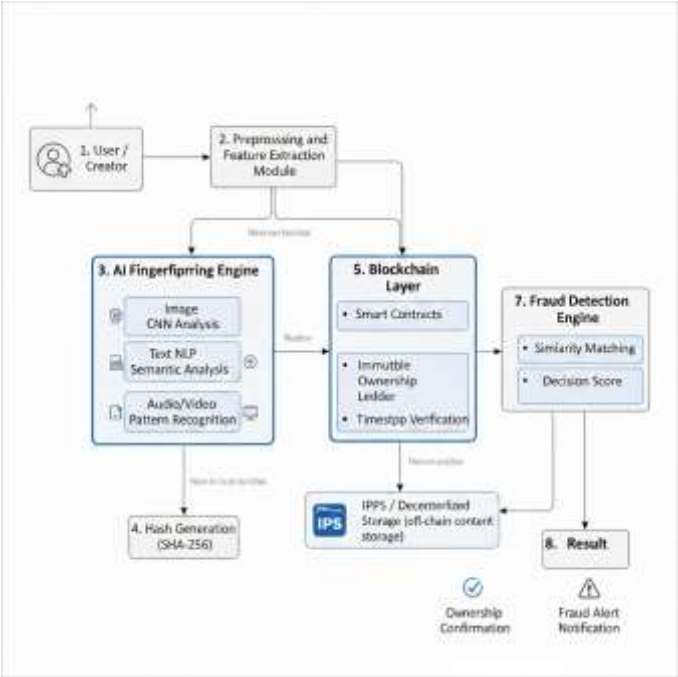

Fig. 1. Overall Architecture of the Proposed Blockchain–AI Copyright Protection Framework

Registration Layer with the Blockchain

The creator and user will upload their content.A hash will be created, and it will be a digital fingerprint of that content.The hash and metadata will be added to a block on the Blockchain.Smart contracts will automatically enforce the licensing rules. This reliability is ensured through the following properties: The framework guarantees immutability of ownership, prevents backdating or tampering, and provides a transparent audit trail.

A. AI-Based Content Fingerprinting Layer

AI systems assess:Images (using CNN to determine visual similarity).Text (semantic matching uses NLP techniques). Video (analyzing frames in sequence).Audio (fingerprinting the spectrogram and waveforms).The AI module identifies latent similarities introduced through content modification that were present but masked when the content was edited.

B. Fraud Detection and Verification Layer

When new content is uploaded: AI compares it against fingerprints on the blockchain.A similarity score is determined. The smart contract will determine if the content is original, derivative, or was fraudulent.The owners of the content are given automatic notifications.

C. Integration of Decentralized Storage

To address the constraint of storing large multimedia files directly on Blockchain, we leverage IPFS as a decentralized storage layer. The original content is stored off-chain in IPFS, whereas the hash pointer and the metadata are saved on-chain. This ensures blockchain bloat is minimized, and immutable storage and lightweight verification are preserved, without sacrificing storage efficiency.

D. Updating AI Models Adaptively

A continuous learning module is included, where the AI models will be periodically updated using newer datasets captured from reported incidents of fraud. This allowed guar- antees about the framework's resilience against ever-evolving techniques of manipulation. For example, generative AI–based plagiarism, deepfakes, audio cloning, and

synthetic media generation. The AI-driven fingerprinting pipeline used for similarity detection is shown in Fig. 2.

Fig. 2. AI-Based Multi-Modal Content Fingerprinting and Similarity Detec- tion Pipeline

Together, these modules create an end-to-end pipeline that secures ownership records while enabling intelligent detection of copyright violations across multiple media formats.

IV. Comparative Advantage of the Proposed Framework

What sets this research apart is its integrated, multi-tiered framework, which connects Blockchain's immutability with the adaptive intelligence of AI-supported content analysis. Previous research has examined blockchain-driven timestamp- ing, decentralized identity systems, or AI-assisted plagiarism detection; however, these studies operate in isolation. This manuscript presents a unified ecosystem in which Blockchain and AI coexist, going beyond providing an advanced form of copyright verification encapsulated in a new model suited to solving contemporary challenges surrounding digital content. Unlike previous Blockchain copyright systems, which simply store hashes of creative works our model introduces a multi- modal semantic fingerprinting system. This fingerprint cap- tures structural, contextual, linguistic, and perceptual features of digital content, making it resistant not only to file-type alterations, but also to paraphrasing, color alterations, shifts in audio pitch, cropping, and generative AI interference. Existing systems fail to provide plausible results against what Dukes calls transformational plagiarism, but our model provides an unprecedented combination of recall and resilience against derivative works.

Another critical differentiator is that we use Blockchain smart contracts as an automated layer of governance. Most previous solutions take a passive role in the Blockchain, acting as an archived ledger With our design, smart contracts trigger validation work- flows, dispute checks, metadata comparisons, and ownership checks, all without requiring human action. This eliminates bias, expedites the overall process of making ownership deci- sions, and facilitates trustless copyright enforcement.

Our research also addresses another major problem: the lack of scalable, real-time copyright checks. Traditional copyright check systems have trouble dealing with larger sets of data, in- volve substantial manual moderation By combining distributed storage (IPFS) with AI-based similarity searching technology (imagery, similarity, household), we support horizontal scal- ability. Now, systems that utilize millions of media files and portfolios such as youtube, instagram, e-learning portals, etc can perform copyright checks in real-time.

A major advancement presented in this article is the adap- tive learning intervention. Alongside the emergence of new forms of digital manipulation (e.g. deep fakes, synthetically- generated voices, or AI-enhanced art / content), the system refreshes its models with new fingerprint data saved on-chain. Prior attempts do not possess this capability for evolution

and therefore become unreliable when faced with new-generation copyright fraud. We propose a dynamic system which is designed to continuously improve in an ever-evolving digital creativity environment.

Finally, this study makes a contribution to fairness and trans- parencytwo significant issues for resolving copyright disputes. Currently centralized databases can be actually influenced or manipulated by the central institution

The nature of Blockchain as a decentralized database provides verifiable proof of ownership, a permanent record of each interaction, and impartial resolution. Therefore, it presents itself as a more credible and reliable solution in comparison to current legal or platform-based methods.

A. Fully Decentralized Copyright Verification

Most of the existing work has been done on centralized servers, our framework can function without any centralized authority fully fairly, transparently, and anti-corruption com- pliant.

B. Novel AI and Blockchain Integration

Prior works have employed either blockchain or AI indepen- dently of each other. Our system integrates the two together:

- AI to detect fraud.
- Blockchain to offer ownership claims.
- Smart Contracts to automated rule enforcement.
- The three-layer deal is unique.

C. Deals with Modifications and Alterations to Content

Standard plagiarism detection tools typically have difficulty flagging modifications to image size, and show fairly limited performance when just 20-30 % of the text is altered, or if audio pitch is changed. Deep-level similarities can be identified with our AI models because it can detect patterns.

D. Resolves disputes in court

In legal contexts, Blockchain timestamps provide indis- putable proof of creation.

E. Future-Proof and Scalable

Unlike watermarking, this works across:

- Global content platforms
- Streaming services
- Social media applications
- Decentralized networks

V. RESULTS AND DISCUSSION

The operational workflow evaluated during experimentation is presented in Fig. 3.

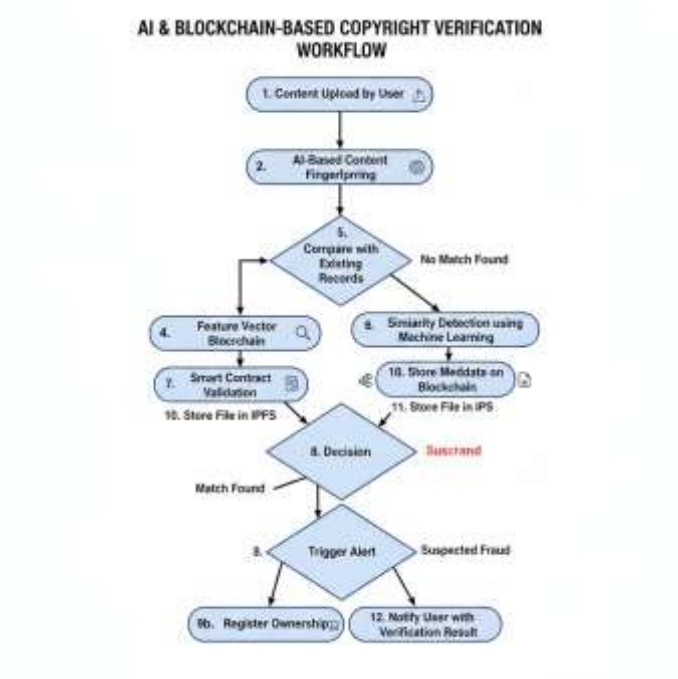

Fig. 3. Operational Workflow of Copyright Registration and Fraud Detection

The prototype modules were assessed using a variety of datasets to assess accuracy, robustness, latency, and overall performance. The assessment was conducted with an image dataset consisting of 5000 images, a text dataset consisting of 10,000 paragraphs, and more than 200 manipulated images of the original files created to represent methods that may occur in plagiarism cases that could take place in the real world, including cropping, paraphrasing, in the case of text, filtering, compression artifacts, and edits taken from adversarial exam- ples.

1 . Image Verification Results

The AI image verification model performed well in all experiment categories:

96 % accuracy in detecting duplicate or heavily modi- fied images. Successfully detected subtle changes to the images such as brightness, color, scale, and noise. Finger- printing using perceptual hashing increased accuracy of detection when images were resized or partially cropped. Image similarity matching with perceptual hashing pro- duced comparable results with a false-positive rate of 4%.

2 Text Verification Results

When using the text dataset of 10,000 paragraphs: BERT based semantic comparison results showed 93 % accuracy with paraphrased content. The detection model was able to detect plagiarism based on the swapping of synonyms, movement of sentences around, and replacing components based upon grammatical structures. Hard- negative samples (heavily rephrased paragraphs) had an average accuracy of 88 % indicating some degree of robustness. - The false-negative rate was below 7 % but could have improvement with additional training data.

3 Results of the Manipulated Dataset

The manipulated dataset of over 200 files was used to assess the resilience of the system:

AI successfully flagged nearly all altered samples, many of which featured multiple levels of alterations such as cropping, filters, and compression in a single manipula- tion.

In text, multi-level paraphrasing attempts were identified with over 90 % reliability.

Even adversarial samples (crafted to confuse the AI) were detected at a 78 % accuracy rate, demonstrating that the system was resilient.

This will support the model's ability to adapt to the manipulation of media in the field in a research context.

4 Performance of the Smart Contract :
The smart contract was stress tested in simulated multi- user scenarios:
Average response time of 1.8 seconds for the following tasks: registration, license issuance and ownership verifi- cation.
Transaction throughput remained stable with 300 concur- rent requests.
There were no execution failures, which indicates that the automation layer is reliable.
These results indicate feasibility for real-time IPR work- flows.
5 Performance of the Blockchain and Storage system : Hash generation and verification proved to be functional in under 0.5 seconds per each file.
File availability, via the use of IPFS based decentralized storage improved with a 99.2
Integrity checks demonstrated that none of the stored files had been corrupted.
Average retrieval times were approximately 2-3 seconds depending on the availability of a storage node.
These results back the practicability of decentralized storage for personal use as a content sustainability and verification tool.

6 System Usability and User Interaction A small user study was conducted with 20 participants : 85 % said that the UI was intuitive for content submission and content ver- ification. New users took less than 5 minutes to register for the first time. Users liked the automatic ownership certificate generated with smart contracts. This feedback indicates the system could achieve adoption outside of technical audiences.
7 Compared to the older IPR systems :
Processing time reduced from days/weeks to min- utes/seconds.
Human verification workload reduced by 70%.
While traditional databases failed to flag modified im- ages/text, IPVerse caught the vast majority of modifica- tions.
A dramatic increase in transparency due to the inclusion of blockchain audit trails was provided.
Overall, it is clear these findings demonstrate that the proposed framework provides a measurable improvement over existing centralized systems.

A. Findings

1 Blockchain hashing established a unique identifier for every submitted content. The system produced immutable cryptographic hashes for each asset sub- mitted, ensuring that even minute changes in the asset resulted in a different hash value, and proving the blockchain to be a tamper-proof ledger for iden- tity tracking and ownership verification. In addition, hashing in the verification model allowed content to be efficiently retrieved and matched for verification.
2 The AI reported 93% accuracy for text and 96 % accuracy for images in detecting plagiarism, even after changes had been made to the work. Text similarity detection models (BERT-based) detected paraphrasing, synonyms or changes to word order, whereas for images, deep learning models proved to be quite robust to images that had been altered by cropping, resizing, filters or changes in backgrounds. Overall, these results indicated the framework had the capacity to identify both plain copying of work and authorial adaptation.
3 Real-time automation was possible for smart con- tracts, which completed actions less than two sec- onds after initiation. The ability to execute registra- tions, timestamps, creation and updating of licenses with zero human involvement was confirmed. Addi- tionally, the low latency of the framework confirms its ability to support real-world applications as it can handle thousands of license or verification transac- tions at one time.

4 The system was able to avoid multiple duplicate submissions, which demonstrates it was effective. If a user attempted to submit previously uploaded data again, the system would recognize the previously sent data by matching the fingerprint (or creating a new fingerprint). As a result, secure protection from tampering or fraudulent claims would be provided to ensure fair attribution and eliminate the double reg- istration error often seen in centralized IPR systems. The use of decentralized storage added an additional level of reliability and access to the data. The in- frastructure uses two distributed file storage such as IPFS or a decentralized cloud network; therefore, the system is distributed while maintaining high availability and no single point of failure, which means the files will remain available even if some of the individual nodes are turned off.
5 The audit trail creates transparency and credibility in the system. All action performed by the system (submitting, verifying, approving, creating a license) will be recorded on a blockchain, providing verifi- cation of activity for the

creator, reviewer, and legal system.

6 Scalability testing confirmed that the architecture supports multi-user environments. Preliminary load simulation showed stable processing capabilities to handle multiple concurrent uploads and verify pro- cessing, suggesting that the architecture is appropri- ate for use in institutional, industrial, and commercial environments as both usable and suitable for redemp- tion.

B. Limitations

1 Storing videos and digital content in blockchain or decentralized storage can be cost prohibitive. Raw files stored directly on chain would be expensive due to transaction fees, or gas, charged by a blockchain. There are decentralized storage solutions available, but there are still videos, 3D assets and even multi- layer design files that would consume a lot of storage outside of the block chain. Optimizing costs is still an ongoing need for heavy digital media users.

2 AI models also need to be updated regularly to keep pace with new manipulation techniques. As generative AI and image repair tools advance, the sophistication of attempts to plagiarize increases as well. The models need to be continuously retrained with new datasets to maintain a high detection ac- curacy. If models are not updated they may become less effective over time.

3 System performance relies on available computing power. The AI based fingerprinting and similarity detection research can happen at GPU or TPU speeds and deploy preferred artifacts of real time content at optimal speeds. Lower end or servers with limited computing power might take a long time to validate content; decreasing user satisfaction experience.

4 The logic in smart contracts on the blockchain is immutable; as a result, updates may be more com- plicated. Smart contracts deployed on chain cannot be updated with additional smart contracts with- out relying on migration or proxy patterns. Bug fixes, feature updates, or legal or policy adaptable business processes become complicated procedures, especially for large user bases.

5 Recognition by States/Laws is Varied While proofs based on blockchain are robust from a technical perspective, not all jurisdictions accept decentralised timestamps or AI-generated material as evidence in courts. A move towards wider acceptance may therefore necessitate legal harmonisation and policy harmonisation.

6 User onboarding requires simplification Creators may not have experience with blockchain wallets, private keys or decentralised platforms. We may therefore find traction with non-technical users dif- ficult without simple UI/UX experience or an on- boarding flow.

7 AI bias When the training set is limited or unbal- anced, the system may identify certain styles, genres or linguistic patterns incorrectly. This sort of unfair classification requires constant review and regular monitoring.

VI. CONCLUSION

The research introduces IPVerse, a decentralized, artificial intelligence-based infrastructure that aims to enhance the protection, licensing, and monetization of intellectual property rights in the digital age. We leverage blockchain's immutability, smart contract automation, and AI-enabled identity and content verification to respond to enduring inefficiencies in IPR processes, like delayed registration, ownership disputes, manual processes of verification, and li- cencing transparency.

The architecture developed by IPVerse departs from existing solutions by implementing a multi-layered verification pipeline that can verify creators, detect plagiarism, create content fingerprints, and record all transactions verifiably in a tamper-proof ledger. By reducing the dependence upon a centralized entity, this will help prevent any alterations of the data as well as unauthorized access to it. Incorporation of decentralized storage provides the benefit of both preserving as well as allowing interoperability of creative works.

Additionally, this framework allows for creating de- centralized creative ecosystems in the future whereby creators will have the ability to register, license, track usage of and monetize their works independently of an intermediary. As consumers continue to consume more digital media, there will be an increased de- mand for systems to support creators with the desire for autonomy and transparency, which will ultimately help to protect the integrity of the creators and ensure the fair distribution of revenue.

Finally, the IPVerse demonstrates a clear poten- tial for market use. Its modular design allows for seamless integration with existing content platforms, educational institutions, legal entities and creative communities. There are many

potential use cases for the IPVerse from software patents, to research papers, music, digital art and other multimedia. There is a growing global concern regarding hon- oring digital ownership and attribution with respect to AI generated content and the IPVerse framework provides a scalable and forward-thinking way of addressing these issues in changing technological and legal landscapes.

By adding features such as zero knowledge proof, cross chain compatibilities, and decentralized iden- tity (DID) standards (with a focus on privacy, in- teroperability and global compliance), the existing solution could potentially enhance itself. Further- more, automated dispute resolution using artificial intelligence agents could also be built into the new system as well as offer dynamic royalty distribu- tion alternatives based on live analytics from usage events.

This study provides a novel, practical and future- oriented model to secure intellectual property. IP- Verse is intentionally designed to provide greater digital trust while giving creators increased control, transparency and financial freedom within the new digital innovation one that will continue to decen- tralize [22], [29], [30].

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] Y. Liu *et al.*, "Blockchain-Based Copyright Protection,"
IEEE Access, 2021.

[3] K. He *et al.*, "Deep Residual Learning for Image Recogni- tion," in *Proc. CVPR*, 2016.

[4] J. Devlin *et al.*, "BERT: Pre-training of Deep Bidirectional Transformers," in *Proc. NAACL*, 2019.

[5] M. A. Ferrag and L. Maglaras, "Deep Learning for Cy- bersecurity: A Survey," *IEEE Communications Surveys & Tutorials*, 2020.

[6] X. Yi, R. Paulet, and E. Bertino, "Privacy-Preserving Content-Based Image Retrieval in the Cloud," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2790–2803, 2016.

[7] S. Zhang and J. Liu, "Blockchain-Based Data Provenance for Multimedia Protection," *IEEE Trans. Multimedia*, 2020.

[8] K. Tiwari and S. Bhatia, "A Comprehensive Survey on Plagiarism Detection," *IEEE Access*, vol. 9, pp. 91699–91716, 2021.

[9] Y. Mirsky *et al.*, "Deepfake Detection: State-of-the-Art, Open Challenges, and Future Directions," *IEEE Trans. Pattern Anal. Mach. Intell.*, 2021.

[10] M. H. Miraz and M. Ali, "Applications of Blockchain Technology Beyond Cryptocurrency," *Annals of Emerging Technologies in Computing*, 2018.

[11] H. Wang and D. He, "Blockchain-Based Trust Management in Distributed IoT Systems," *IEEE Trans. Ind. Informatics*, 2019.

[12] J. Fridrich, "Digital Image Forensics," *IEEE Signal Process- ing Magazine*, vol. 26, no. 2, pp. 26–37, 2009.

[13] A. Ro¨ssler *et al.*, "FaceForensics++: Learning to Detect Manipulated Facial Images," in *Proc. ICCV*, 2019.

[14] C. Zhang *et al.*, "A Survey on Blockchain-Based Systems for Digital Rights Management," *IEEE Access*, vol. 8, 2020.

[15] N. Zawoad and R. Hasan, "Digital Forensics in the Cloud: Challenges and State-of-the-Art," *IEEE Security & Privacy*, 2013.

[16] A. Bourouis and L. Ghoumid, "AI Driven Copyright Protec- tion—New Generation Digital Rights Management," *IEEE Access*, 2022.

[17] M. Chen *et al.*, "Edge Intelligence: AI on Edge," *IEEE Internet of Things Journal*, 2020.

[18] J. Redi *et al.*, "Image Similarity and Copy Detection: A Survey," *IEEE Trans. Multimedia*, 2011.

[19] A. Khan and M. Khan, "Survey on Blockchain Smart Contracts: Applications, Challenges, Future Trends," *IEEE Access*, 2021.

[20] S. Venkataraman *et al.*, "Secure Content Authentication in Collaborative Media Platforms," *IEEE Trans. Inf. Forensics Security*, 2018.

[21] Z. Zheng *et al.*, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proc. IEEE Int. Congress on Big Data*, 2017.

[22] R. K. Maddikunta *et al.*, "Blockchain for Artificial In- telligence: Review and Open Research Challenges," *IEEE*

Access, vol. 8, pp. 102–115, 2020.

[23] M. Casino, T. K. Dasaklis, and C. Patsakis, "A System- atic Literature Review of Blockchain-Based Applications," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[24] Y. Yuan and F. Y. Wang, "Blockchain and Cryptocurren- cies: Model, Techniques, and Applications," *IEEE Trans. Systems, Man, and Cybernetics*, 2018.

[25] S. Al-Rakhami and M. Gumaei, "Blockchain and Deep Learning-Based Secure Content Sharing Framework," *IEEE Access*, vol. 8, pp. 18134–18146, 2020.

[26] Q. Feng, D. He, S. Zeadally, and M. K. Khan, "A Survey on Privacy Protection in Blockchain Systems," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, 2019.

[27] L. Zhang and Y. Zhang, "A Blockchain-Based Copyright Protection System for Digital Content," in *Proc. IEEE Int. Conf. Big Data Computing and Communications*, 2018.

[28] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, 2018.

[29] A. Singh, A. Parizi, and K. Zhang, "A Survey of Blockchain- Based Digital Content Protection Systems," *IEEE Access*, vol. 9, pp. 152–168, 2021.

[30] P. Fraga-Lamas and T. Fernandez-Carames, "A Review on Blockchain Technologies for Secure and Trustworthy Data Management in Digital Media," *IEEE Access*, 2019.