International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Survey on Revolutionizing Digital Copyright Protection with POS Algorithms and Smart Contracts

Pranauv Kessavan[1], Ajay V[2], Hari Haraan M S[3], Amala Margret[4]

[1,2,3]Student, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry.
[4]Assistant Professor, Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry.

Abstract
Digital copyright protection systems aim to secure creators' rights and ensure they're fairly compensated, but traditional methods struggle with data verification and tamper-resistance. The proposed solution enhances these protections by integrating proof-of-stake (PoS) algorithms and smart contracts into the blockchain framework. PoS, a consensus mechanism in blockchain, requires participants to stake tokens, ensuring that they have a stake in maintaining the integrity of the system. This approach secures the network and safeguards against tampering. Smart contracts—self-executing, tamper-proof agreements stored on the blockchain—automate copyright enforcement, making it impossible to alter ownership records once added to the blockchain. This automation reduces manipulation risks and improves efficiency. Additionally, the decentralized structure of blockchain distributes data across multiple nodes, preventing any single entity from altering or compromising the information. This guarantees the immutability and transparency of digital content and ownership records. Together, these technologies offer a robust, efficient solution for digital copyright protection. Blockchain's decentralized, tamper-resistant nature, combined with PoS's secure verification and smart contracts' automated enforcement, provides a trustworthy framework that better secures ownership and prevents unauthorized manipulation.

Keywords: Digital copyright protection, Proof of Stake, Smart contracts, immutability.

1. Introduction

Digital copyright systems are essential for protecting creators' intellectual property in the digital age, ensuring they control how their work is used, receive proper credit, and are fairly compensated. As digital content creation and distribution grow, traditional copyright systems struggle to maintain data integrity, prevent tampering, and enforce copyright laws effectively due to their reliance on centralized authorities and vulnerable verification algorithms. One common verification method, ring signatures, allows content authentication while preserving user anonymity. However, this algorithm has weaknesses that permit data manipulation, compromising content security and making it difficult to confirm ownership with certainty.

By using a distributed and decentralized ledger system that allows data to be exchanged among a network of nodes and prohibits any one party from changing records, blockchain technology solves these issues.

This decentralized nature ensures that all ownership records remain immutable and verifiable. When content is registered on the blockchain, its ownership and history are permanently recorded, making it nearly impossible for unauthorized changes to go undetected. The use of Proof of Stake (PoS) algorithms enhances the security of this blockchain-based system. In PoS, participants must stake tokens to validate transactions, creating a vested interest in maintaining network integrity. Because participants are motivated to act honorably in order to safeguard their investment, PoS is a secure option for confirming copyright transactions, which lowers the possibility of manipulation. By automating copyright enforcement, smart contracts reinforce the system even more. When certain requirements are fulfilled, these self-executing contracts—which are kept on the blockchain—automatically carry out certain terms, such payments or licenses. Smart contracts minimize disagreements, human error, and processing delays by doing away with middlemen. This combination of blockchain, PoS, and smart contracts provides a secure, efficient, and reliable solution for modern digital copyright protection, empowering creators in an interconnected digital environment.

2. Literature Survey

Enhancing Copyright Protection Through Blockchain and Ring Signature Algorithm from Lattice [1] Jian Jiang; Yulong Gao [1]

This paper presents a solution to address privacy risks in blockchain-based digital copyright systems. While blockchain's transparency aids data authentication, it can expose sensitive copyright information. To counter this, the authors propose a secure copyright protection scheme that integrates blockchain with a lattice-based ring signature algorithm. This lattice-based approach allows anonymous signing without revealing signer identities, protecting privacy. Using the lattice basis delegation algorithm, the public-private key pair is generated without increasing computational complexity. Rejection sampling further reduces the signing process's complexity, ensuring privacy with minimal overhead. This new scheme combines the privacy of ring signatures with blockchain's security, resulting in an efficient system with lower communication costs and smaller key sizes than similar methods. It offers a secure, private, and computationally efficient framework for copyright protection, balancing privacy with blockchain's verification benefits.

A Blockchain Copyright Protection Scheme Based on CP-ABE Scheme with Policy Update [2] Yufei Gong and Zhengtao Jiang [2]

The suggested blockchain-based copyright protection plan mitigates the risks associated with quantum computing assaults while addressing important data security issues including controlled administration of copyright material and safe access. Only authorized users may access copyright data thanks to this scheme's fine-grained access control, which is made possible by the use of attribute-based encryption (ABE). The ABE algorithm strengthens the system's defenses against quantum assaults by utilizing lattice cryptography and the decision ring learning with errors (R-LWE) issue. The approach is adaptable and effective for handling changing copyright regulations as it also enables searchable ciphertext and policy revisions. Additionally, security analysis confirms that the scheme is resilient to various types of attacks, including adaptive keyword and plaintext attacks. Comparative analysis and experiments show that it achieves lower computational and storage costs, offering a more secure and efficient solution for managing copyright data in a blockchain environment.

Blockchain-based reliable image copyright protection [3] Xiangli Xiao, Xiaotong He [3]

This paper proposes BB-RICP, a blockchain-based image copyright protection system using Hyperledger Fabric to address challenges in secure and efficient copyright management. Traditional centralized

systems risk data loss and tampering, while typical blockchain platforms like Ethereum face efficiency and cost limitations. Hyperledger Fabric in BB-RICP improves on these by offering a more efficient, cost-effective, and reliable platform for managing copyright lifecycles, from creation to distribution. BB-RICP includes GM algorithms, which align with Chinese standards, and uses a consortium blockchain with the practical Byzantine Fault Tolerance (PBFT) algorithm, boosting security and efficiency. Spread spectrum watermarking enhances user-friendliness by embedding ownership information directly into images. Kubernetes is used to test the system's reliability in a simulated blockchain environment, making BB-RICP a comprehensive and resilient solution for image copyright protection.

A digital resource copyright protection scheme based on blockchain cross-chain technology [4] Renqiang Xie, Min Tang [4]

With the growth of digital publishing, copyright infringement of digital resources has become a pressing issue. While blockchain offers a solution, existing single-chain or consortium blockchain systems face issues with efficiency, scalability, and alignment with business needs. This study suggests a copyright protection system that makes use of blockchain cross-chain technologies in order to overcome these constraints. Interaction across several blockchains is made possible by cross-chain technology, which boosts copyright protection and greatly increases processing speed and scalability. The proposed system supports the full copyright lifecycle, including registration, transactions, modifications, and enforcement, creating a collaborative ecosystem where stakeholders can effectively manage copyright rights. By applying cross-chain technology, the system enhances scalability, maintainability, and practicality, offering a robust, future-proof approach to digital copyright protection that adapts well to industry demands.

Research on digital copyright protection based on the Hyperledger fabric blockchain network technology [5] Renqiang Xie, Min tang [5]

The rise of network technology has increased digital copyright infringement, threatening content creators' rights and discouraging innovation. Traditional copyright protection struggles with weak enforcement, slow processing, and complex verification, leaving creators vulnerable to unauthorized use and revenue loss. This paper introduces a blockchain-based copyright protection system that addresses these issues by leveraging blockchain's decentralized, tamper-resistant qualities. Using smart contracts within the hyperledger fabric framework, the system automates the full digital rights lifecycle, enhancing both efficiency and security. Results show that this approach significantly improves copyright protection by streamlining rights verification and offering creators a more secure and effective way to protect their intellectual property in the digital realm.

A blockchain-based code copyright management system [6] Nan Jing, Qi Liu, Vijayan Sugumaran [6]

This paper introduces a blockchain-based system for managing code copyright that addresses code plagiarism more effectively than traditional detection methods. The system utilizes an Abstract Syntax Tree (AST)-based verification model to assess code originality by comparing it against existing code. Once originality is confirmed, the Peer-to-Peer blockchain network stores the copyright information, ensuring that it remains immutable and traceable. The system also employs code fingerprints—256-bit hash values generated via the SHA256 algorithm based on code eigenvalues—as an efficient method for storing copyright data. These fingerprints enhance storage efficiency and response time while providing robust security due to SHA256's uniqueness and irreversibility. Experimental results show that the

proposed system effectively verifies code originality, offering a secure, transparent, and efficient solution for managing code copyrights.

3. Proposed System

As digital content expands, traditional copyright protection methods face growing challenges in verification, enforcement, and efficiency. Managing copyrights in a centralized system is increasingly inadequate due to security risks, tampering, processing delays, and human error. Digital content creators need a reliable, efficient way to safeguard their intellectual property. To solve these problems, the suggested solution incorporates blockchain technology, more especially smart contracts and the Proof of Stake (PoS) algorithm. Copyright data is kept safe and unchangeable because to blockchain's decentralized, tamper-resistant architecture. PoS enhances security by validating transactions with minimal computational power, making it more energy-efficient and cost-effective. Smart contracts automate enforcement, executing copyright rules consistently without intermediaries, reducing human error, and ensuring reliable application. This system enables faster verification of ownership, automated enforcement of copyright agreements, and transparency that reduces disputes. Smart contracts manage tasks like licensing and royalty distribution, streamlining processes and supporting scalability. Overall, the proposed solution strengthens copyright protection, meeting the needs of digital content creators in the modern era with an efficient, scalable approach.

A. PROOF OF STAKE (POS) ALGORITHM MODULE:

By choosing validators according to how many tokens they possess and are prepared to "stake" as collateral, the Proof of Stake (PoS) module plays a critical role in preserving the blockchain network's security. PoS chooses validators more energy-efficiently than the conventional Proof of Work (PoW) approach, which depends on energy-intensive mining to validate transactions. Because they risk losing their staked tokens if they try to manipulate the network, the validators are motivated to behave honorably. This approach ensures that only legitimate validators participate in maintaining the network’s integrity, thereby securing copyright data from unauthorized access or manipulation. Additionally, by reducing energy consumption, PoS offers a more sustainable solution for blockchain-based digital copyright management, without compromising security.

B. SMART CONTRACTS MODULE:

The blockchain's smart contracts module is essential to automating copyright agreement enforcement. These self-executing algorithms, known as smart contracts, automatically perform predetermined tasks in response to particular events, like the purchase of a license or the use of material. For example, when a user purchases the rights to a digital work, the smart contract can automatically transfer ownership or release payment without the need for manual intervention. This automation eliminates the need for intermediaries, making the process more efficient and cost-effective. Additionally, smart contracts ensure that the agreements are executed in a transparent and tamper-proof manner, as all actions are recorded immutably on the blockchain. This greatly simplifies the process of managing copyright, while improving trust and reliability.

C. BLOCKCHAIN LEDGER MODULE:

The blockchain ledger module serves as the foundational component of the system, where all copyright information is recorded immutably on a decentralized ledger. This module securely stores essential data such as transaction details, ownership records, and changes to copyright information. The use of blockchain ensures that this data is tamper-resistant, meaning it cannot be altered once it is recorded, which preserves the integrity of the copyright information. The blockchain's decentralized structure further lowers the possibility of data loss or corruption by preventing any one party from controlling the data.

This decentralized approach fosters secure and transparent management of digital rights, providing all participants with confidence in the accuracy and permanence of the recorded data.

D. COPYRIGHT REGISTRATION AND TRANSFER MODULE:

This module serves a crucial function in the realm of copyright management by facilitating the registration of new copyrights on the blockchain and enabling the seamless transfer of copyrights between owners. By leveraging smart contracts and the blockchain ledger, it ensures that each transaction is secure, transparent, and easily traceable. This innovative approach simplifies what has traditionally been a complex and often cumbersome process, making it more efficient for creators and copyright holders. As a result, users can enjoy peace of mind knowing that their intellectual property rights are managed with the highest level of security and accuracy, ultimately fostering a more reliable system for ownership changes and registration.

E. AUDIT AND COMPLIANCE MODULE:

This module plays a vital role in tracking and auditing copyright transactions while enforcing relevant rules and regulations within the system. By maintaining a comprehensive record of all transactions, it enhances accountability and transparency, enabling users to verify compliance with copyright laws effortlessly. This ensures that digital content is properly attributed to its rightful owners, minimizing the risk of infringement and promoting ethical use of creative works. As a result, creators and copyright holders can navigate the complexities of copyright management with confidence, knowing that the system safeguards their rights and fosters a culture of respect for intellectual property.

F. ENCRYPTION AND PRIVACY PROTECTION MODULE:

By using cutting-edge encryption techniques, this module is crucial for guaranteeing the protection of critical copyright information. Since blockchain is a public domain, this module is essential to protecting copyright owners' privacy by encrypting important information while preserving the integrity of publicly verifiable records. This dual approach allows users to enjoy the benefits of blockchain's transparency without compromising their personal information or digital assets. Consequently, copyright holders can protect themselves against unauthorized access, enhancing their overall privacy and security in the digital landscape. This ensures that their rights are respected and their valuable creations are shielded from potential threats.

4. Architecture Diagram

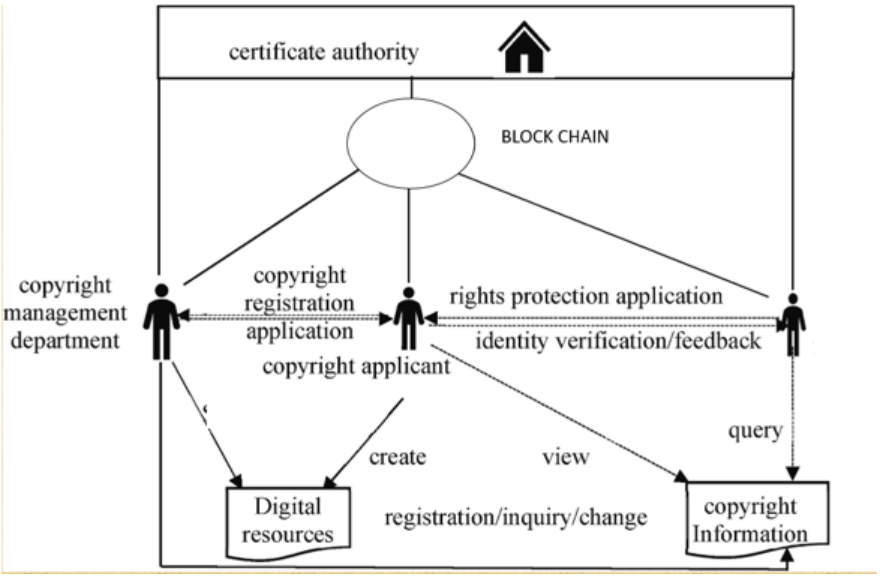

Figure: Digital Copyright Protection using PoS

The diagram depicts a blockchain-based system for copyright management, involving several key entities. The copyright applicant submits a copyright registration application to the copyright management department. This department works alongside a certificate authority to authenticate and validate the application. After being verified, the copyright data is saved on the blockchain, guaranteeing its immutability and traceability. The applicant can create digital resources and view or modify the registered copyright information. Additionally, the system allows users to submit rights protection applications and receive feedback through identity verification mechanisms. Queries related to the registered copyright information can also be performed, making the system transparent and secure for managing digital copyrights.

5. Result and Discussion

The outcomes show how well the suggested blockchain-based copyright protection system works to overcome the drawbacks of conventional techniques. By leveraging blockchain's decentralized and tamper-resistant architecture, the system ensures the secure storage and immutability of copyright data, reducing the risk of unauthorized alterations. By reducing the processing needs, the Proof of Stake (PoS) method improves transaction validation and lowers operating costs and energy consumption, adaptations of conventional techniques. Additionally, smart contracts streamline enforcement by automating copyright rules and agreements, which minimizes reliance on intermediaries, reduces the potential for human error, and provides more consistent copyright protection. Through real-world testing, the system has shown significant improvements in processing speed for verifying ownership and executing copyright agreements, leading to faster and more transparent management of digital rights. Overall, the findings indicate that this system not only strengthens copyright enforcement but also supports a scalable and sustainable solution that aligns well with the increasing demands of digital content management. This advancement in copyright protection provides a more robust, reliable framework that benefits creators by securing their intellectual property in an increasingly digital landscape.

6. Comparison of Ring Signature and Proof of Stake Algorithm

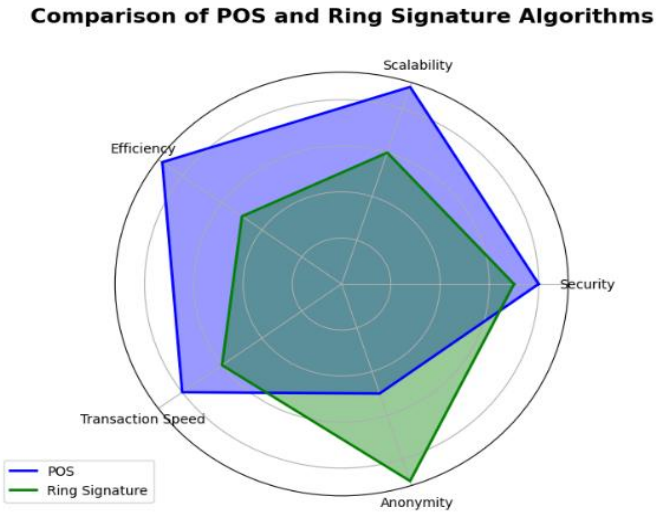

Figure: Comparison of PoS and Ring Signature Algorithms

The Ring Signature and Proof of Stake (PoS) algorithms are both cryptographic techniques used for ensuring security and authenticity, but they serve different purposes and operate under distinct principles.

Ring Signatures are primarily designed for privacy and anonymity. They let a user sign a communication on behalf of a group without identifying the group member who did so. This protects the participants' privacy by guaranteeing that the signer's identity stays anonymous, making it challenging to link the activity to a particular person. However, this privacy comes at the cost of potentially weakening the system's security, as it is easier for malicious actors to manipulate the data without being detected. In a blockchain context, ring signatures can be useful in scenarios where privacy is critical, such as in digital content protection or anonymous transactions, but they may not offer robust security guarantees against data manipulation.

On the other hand, blockchain networks employ the Proof of Stake (PoS) consensus mechanism to verify transactions and safeguard the network. Unlike Proof of Work (PoW), which depends on processing power, Proof of Stake (PoS) requires participants to stake a specific number of cryptocurrencies or tokens in order to take part in the validation process. The amount staked determines the likelihood of getting chosen to verify a block. PoS ensures network security and transaction integrity by incentivizing honest behavior—participants risk losing their staked tokens if they validate fraudulent transactions. It also offers advantages over PoW in terms of energy efficiency and scalability, as it does not require the vast computational resources that PoW does. However, PoS systems may face issues like centralization, as those with more tokens have a higher probability of validating transactions, potentially leading to a concentration of control. While ring signatures focus on privacy and anonymity, PoS emphasizes network security and transaction validation. The combination of these two techniques could complement each other, as PoS could secure the system's integrity, while ring signatures could ensure the anonymity of users interacting with the system. However, both have their respective strengths and weaknesses depending on the specific requirements of the application.

7. Efficiency Graph for Proof of Stake Algorithm

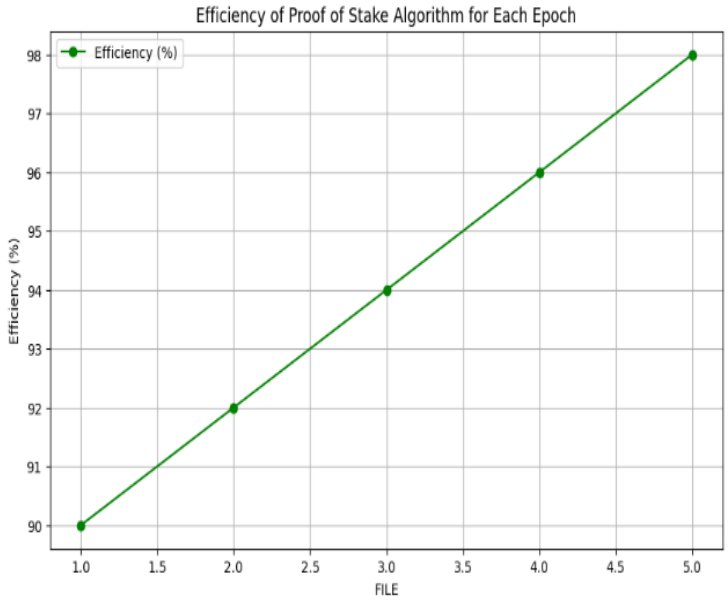

Figure: Efficiency of Proof of stake Algorithm for Each Epoch

The Proof of Stake (PoS) method's efficiency graph shows how well the system performs across various time periods. Every epoch denotes a certain time frame in which a group of validators is chosen to approve

transactions and produce fresh blocks. The PoS method's efficiency, represented as a percentage on the y-axis, gauges how well the algorithm makes use of the resources at its disposal to reach agreement and preserve network security. The graph illustrates how the PoS algorithm's efficiency usually rises with each new epoch. Improvements in the validator selection method, network protocol optimization, and higher validator involvement and stake are some of the reasons for this improvement. Increased efficiency shows that the PoS algorithm is becoming better at choosing validators, confirming transactions, and protecting the network while using the fewest resources possible. The algorithm's capacity to reach consensus faster and with less resources is indicated by a rising efficiency curve, which speeds up transaction processing times and enhances network performance in general. On the other hand, a decreasing or static efficiency curve might point to PoS algorithmic inefficiencies like poor validator selection or elevated network congestion.

8. Time Graph for Proof of Stake Algorithm

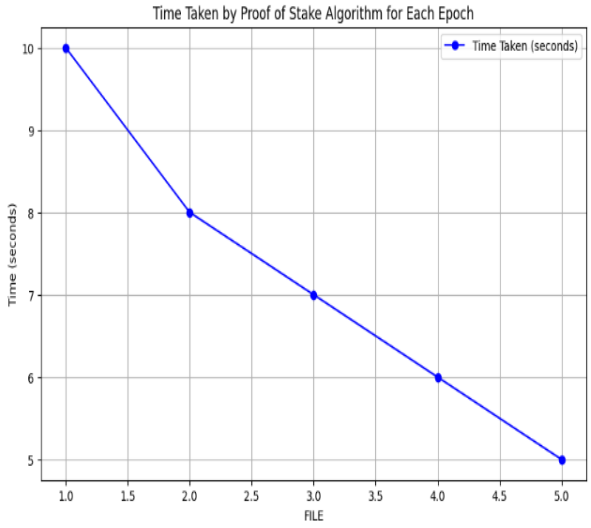

Figure:Time Taken by Proof of Stake Algorithm for Each Epoch

The Proof of Stake (PoS) algorithm's time graph shows how long it takes the system to process each blockchain network epoch. Every epoch denotes a certain time frame during which validators are chosen to approve transactions and produce fresh blocks. The graph's y-axis, which shows the amount of time needed for each epoch, shows how well the PoS algorithm performs and processes transactions to reach consensus. The graph illustrates how variables like network congestion, shifts in validator involvement, and modifications to the PoS algorithm itself may cause the time required for each epoch to alter over time. Generally speaking, a declining trend in the time graph denotes advancements in the PoS algorithm's scalability and efficiency, which lead to quicker transaction processing times and lower network latency. On the other hand, a rising trend or oscillations in the time graph can point to problems or inefficiencies with the PoS algorithm, including higher processing costs for transaction validation or network congestion. These variations could lead network managers to make changes or modifications to enhance the PoS algorithm's reliability and performance.

9. Encryption vs Decryption Time

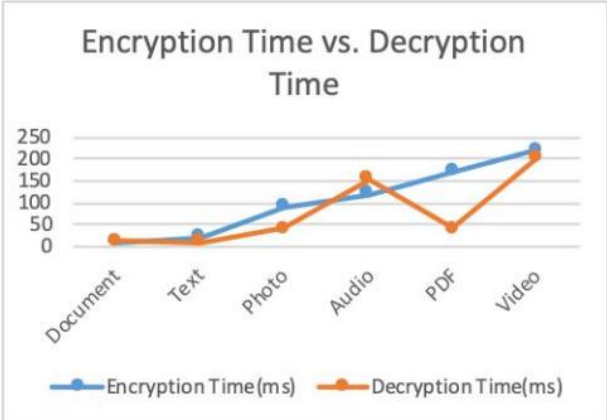

Figure: Encryption Time vs. Decryption Time

Differences in the computing needs of different electronic data formats, including text, photo, and video files, are suggested by the observed differences in encryption and decryption times. Since the same key is used for both encryption and decryption, symmetric key encryption techniques, such as Blowfish, typically show comparable encryption and decryption timings. Nonetheless, the disparity in the case of PDF files, where the decryption time exceeds the encryption time, may be explained by the unique features of PDF file formats.

10. Conclusion

In conclusion, the proposed solution significantly enhances digital copyright protection systems by addressing critical challenges related to data verification and resistance to tampering. Traditional methods, particularly those relying on ring signature algorithms, have shown vulnerabilities that allow for easy manipulation of data, compromising the system's security and reliability in safeguarding digital content. By integrating Proof of Stake (PoS) algorithms with smart contracts, this solution offers a more robust approach to digital rights management. The automation of copyright enforcement ensures that rules are consistently applied, while also maintaining the immutability of data, thereby preventing unauthorized changes. Additionally, preserving the integrity of digital material is greatly aided by blockchain technology's decentralized structure. This ensures that copyright holders can confidently verify ownership and protect their intellectual property without fear of infringement. By providing a secure and efficient framework for managing digital rights, the proposed solution fosters a more trustworthy environment for creators and copyright holders. Ultimately, it represents a significant advancement in modern digital copyright protection, promoting respect for intellectual property in an increasingly digital world.

References

1. T. Nurhaeni, L. Nirmalasari, A. Faturahman, and S. Avionita, ‘‘Transformation framework design on digital copyright entities using blockchain technology,’’ Blockchain Frontier Technol., vol. 1, no. 1, pp. 35–43, Jul. 2021, doi: 10.34306/bfront.v1i01.5.
2. W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, ‘‘Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection,’’ IEEE Trans. Emerg. Topics Comput., vol. 9, no. 3, pp. 1410–1420, Jul. 2021, doi: 10.1109/TETC.2020.2993032.

3. X. Zhang and Y. Yin, ‘‘Research on digital copyright management system based on blockchain technology,’’ in Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC), Mar. 2019, pp. 2093–2097.
4. K.-C. Li and R.-H. Shi, ‘‘A flexible and efficient privacy-preserving range query scheme for blockchain-enhanced IoT,’’ IEEE Internet Things J., vol. 10, no. 1, pp. 720–733, Jan. 2023, doi: 10.1109/JIOT.2022.3203182.
5. T. Jiang, A. Sui, W. Lin, and P. Han, ‘‘Research on the application of blockchain in copyright protection,’’ in Proc. Int. Conf. Culture-Oriented Sci. Technol. (ICCST), Oct. 2020, pp. 616–621.
6. H. Mala, M. Dakhil-alian, and M. Brenjkoub, ‘‘A new identity-based proxy signature scheme from bilinear pairings,’’ in Proc. 2nd Int. Conf. Inf. Commun. Technol., 2004, pp. 3304–3308.
7. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, ‘‘Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction,’’ Theor. Comput. Sci., vol. 469, pp. 1–14, Jan. 2013, doi: 10.1016/j.tcs.2012.10.031.
8. S. S. M. Chow, S. M. Yiu, and L. C. K. Hui, ‘‘Efficient identity based ring signature,’’ in Proc. 3rd Int. Conf., New York, NY, USA, Jun. 2005, pp. 7–10.
9. P. W. Shor, ‘‘Algorithms for quantum computation: Discrete logarithms and factoring,’’ in Proc. 35th Annu. Symp. Found. Comput. Sci., 1994, pp. 20–22.
10. R. L. Rivest, A. Shamir, and L. Adleman, ‘‘A method for obtaining digital signatures and public-key cryptosystems,’’ Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.
11. L. Harn, M. Mehta, and W.-J. Hsin, ‘‘Integrating Diffie–Hellman key exchange into the digital signature algorithm (DSA),’’ IEEE Commun. Lett., vol. 8, no. 3, pp. 198–200, Mar. 2004, doi: 10.1109/LCOMM.2004.825705.
12. V. S. Miller, ‘‘Use of elliptic curves in cryptography,’’ in Conference on the Theory and Application of Cryptographic Techniques. Cham, Switzerland: Springer, 1985.
13. S. V. S. Vasundhara and D. K. V. D. Dr. K. V. Durgaprasad, ‘‘Elliptic curve cryptosystems,’’ Indian J. Appl. Res., vol. 4, no. 3, pp. 308–311, Oct. 2011.
14. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, ‘‘A survey on privacy protection in blockchain system,’’ J. Netw. Comput. Appl., vol. 126, pp. 45–58, Jan. 2019, doi: 10.1016/j.jnca.2018.10.020.
15. R. Zhang, R. Xue, and L. Liu, ‘‘Security and privacy on blockchain,’’ ACM Comput. Surveys, vol. 52, no. 3, pp. 1–34, Jul. 2019, doi: 10.1145/3316481.