IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 30, No. 11, November, 2025, pp. 3077-3082
Journal homepage: http://iieta.org/journals/isi

Blockchain-Enabled Digital Timestamping and Consensus-Based Incentivization for Collaborative Intellectual Property Management

Saima Zareen Ansari[1*], Shrikant D. Zade[2]

[1] Department of Computer Science and Engineering, G.H. Raisoni University, Pandhurna 480337, India
[2] Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur 441501, India

Corresponding Author Email: saimazareen.ansari.phdcs@ghru.edu.in

https://doi.org/10.18280/isi.301125

Received: 1 October 2025
Revised: 14 November 2025
Accepted: 26 November 2025
Available online: 30 November 2025

Keywords:
digital timestamping, blockchain, intellectual property rights, consensus-based polling, collaborative research, incentivization

ABSTRACT

Collaborative research environments, particularly in medical and interdisciplinary domains, often struggle with fair attribution, and secure management of shared intellectual assets. Existing digital timestamping and blockchain-based copyright solutions primarily focus on proof of existence and immutability, while offering limited support for equitable contribution assessment among multiple collaborators. To address this gap, this paper proposes a blockchain-enabled framework that integrates digital timestamping with a consensus-based polling mechanism for proportional intellectual property rights (IPR) allocation. Each research contribution is securely timestamped, cryptographically protected, and recorded on a tamper-resistant ledger, while collaborators collectively evaluate individual inputs through structured polling to determine ownership shares transparently. Smart contracts automate record-keeping, consent management, and version control, reducing dependency on centralized authorities and minimizing post-collaboration disputes. The framework is particularly suited to medical research scenarios, where long project lifecycles, sensitive data, and multi-stage contributions demand both technical integrity and trust among participants. By combining secure documentation with democratic incentive allocation, the proposed system advances current IPR protection models toward more collaborative, transparent, and dispute-resilient research ecosystems.

1. INTRODUCTION

Establishing verifiable proof of authorship and ownership remains a critical concern in collaborative research environments. In this context, demonstrating the existence of a document at a specific point in time plays a crucial role in determining the sequence of idea generation and ownership claims. Digital timestamping offers a reliable mechanism for asserting such temporal evidence, particularly in scenarios involving copyright and intellectual property disputes. When combined with blockchain technology, timestamping systems gain enhanced security, transparency, and resilience against manipulation, making them more reliable than conventional centralized approaches [1].

Blockchain-based timestamping eliminates the dependence on a centralized Time Stamping Authority by leveraging decentralized consensus to validate and record timestamps. This approach significantly reduces risks associated with single points of failure, unauthorized data modification, and trust violations [2, 3]. Due to the immutable nature of blockchain, once a timestamp is recorded, it cannot be altered or erased, thereby providing enduring proof of document existence and ownership [4]. Prior studies have also demonstrated that integrating blockchain with supporting techniques such as digital watermarking, perceptual hash functions, and QR codes can further strengthen copyright protection mechanisms [5].

The traceability and transparency inherent in blockchain systems substantially enhance the effectiveness of intellectual property protection frameworks. Blockchain-enabled copyright registration and management systems simplify administrative processes while ensuring tamper-proof record keeping and fraud resistance. Smart contracts and distributed ledger technologies enable automated validation of ownership claims and proof of existence, improving both efficiency and integrity in global digital environments. From a theoretical standpoint, property rights literature suggests that equitable distribution of intellectual property among contributors can reduce opportunistic behaviour and promote sustained collaboration, particularly in knowledge-intensive domains [6].

Despite these advancements, most existing blockchain-based IPR solutions primarily focus on proof of existence, ownership registration, or access control, offering limited support for fair and transparent allocation of rights among multiple collaborators. In complex research settings, such as medical and pharmaceutical research, contributions are often incremental, interdisciplinary, and distributed over long project lifecycles. Treating all contributors equally under traditional IPR frameworks, regardless of effort or impact, can lead to dissatisfaction, disputes, and reduced incentives for innovation.

To address this limitation, this work introduces a collaborative IPR management framework that combines secure digital timestamping with a consensus-based polling mechanism for contribution assessment. By allowing participants to collectively evaluate and agree upon the relative value of individual contributions, the proposed approach seeks to establish proportional and transparent IPR ownership [7]. This incentive-driven model strengthens trust among collaborators while better aligning technical protection mechanisms with real-world research dynamics. Particularly in sensitive domains such as medical research where accountability, confidentiality, and fairness are paramount.

2. LITERATURE SURVEY

Recent research has increasingly explored the use of blockchain technology for securing intellectual property, managing copyrights, and ensuring the integrity of digital documents through timestamping and cryptographic validation. These studies broadly demonstrate that decentralization, immutability, and consensus mechanisms can significantly improve trust and transparency in ownership verification and document preservation systems. However, the scope and depth of these contributions vary depending on their focus, ranging from cryptographic enhancements to application-specific copyright frameworks.

Several works emphasize strengthening timestamping and signature verification using blockchain-supported cryptographic schemes. Sowmiya et al. [8] proposed a linear elliptical curve digital signature integrated with blockchain to enhance security in cloud environments, highlighting efficiency and reduced computational overhead. Similarly, Hyla and Pejaś [9] examined long-term verification of digital signatures by embedding timestamped proofs into blockchain ledgers, demonstrating improved integrity over traditional electronic signature systems. Ma et al. [10] further validated the reliability of blockchain-based timestamping by leveraging the Bitcoin platform to establish trusted event timelines, arguing that decentralized consensus provides stronger temporal guarantees than centralized timestamping authorities. These studies collectively confirm blockchain's suitability for secure timestamping but remain largely focused on verification rather than collaborative ownership management.

Beyond cryptographic validation, blockchain has also been applied directly to intellectual property protection and copyright lifecycle management. A blockchain-based intellectual property protection system records ownership claims and timestamps to minimize disputes, thereby enabling traceability across the IP lifecycle. This concept is extended to hardware design by proposing a circuit copyright blockchain that integrates homomorphic encryption, allowing protected IP usage without exposing sensitive design details [11]. These approaches illustrate blockchain's adaptability across IP domains, yet they primarily concentrate on ownership registration and enforcement rather than contribution valuation in collaborative settings.

In multi-author and collaborative environments, the challenge of shared ownership becomes more pronounced. Multi-signature mechanisms on blockchain platforms such as Ethereum enable joint ownership and consent verification without relying on trusted third parties [12]. While these schemes facilitate collective authorization, they do not address how ownership shares should be determined or adjusted based on individual contribution levels. Similarly, Kim and Hwang [13] discussed peer-to-peer architectures, encryption, and watermarking techniques for IPR protection, providing foundational insights into secure content distribution but offering limited guidance on equitable rights allocation.

The integration of watermarking with blockchain has also received attention as a dual-layer protection mechanism. Geethanjali et al. [14] demonstrated how digital watermarking combined with blockchain-based metadata storage can enhance traceability and ownership verification of digital content. Fallucchi et al. [15] broadened the application domain by examining blockchain-based certification, timestamping, and data ownership in digital government services, reinforcing the role of blockchain in automating and securing institutional record management. These systems strengthen content authenticity but assume predefined ownership structures rather than dynamically negotiated rights.

Recent advancements have further addressed privacy, scalability, and interoperability challenges in blockchain-based timestamping systems. Abadi et al. [16] introduced timed signatures and zero-knowledge proofs to enable privacy-preserving timestamp verification, which is particularly relevant for sensitive research data. Tas et al. [17] proposed interchain timestamping to support cross-platform verification in distributed environments, addressing scalability and interoperability limitations. While these developments improve system robustness, they do not explicitly consider incentive mechanisms or collaborative decision-making processes.

From a theoretical perspective, Chen et al. [6] demonstrated that equitable intellectual property rights sharing can reduce opportunism and foster long-term collaboration, especially in knowledge-intensive projects. However, existing blockchain-based IPR systems rarely operationalize this principle through structured, participant-driven mechanisms. Most solutions assume static ownership definitions or centralized arbitration, which may not align with the evolving and incremental nature of collaborative research.

In summary, existing literature confirms the effectiveness of blockchain technology for secure timestamping, ownership verification, and copyright protection. Nevertheless, a clear gap remains in supporting transparent, contribution-aware, and consensus-driven allocation of intellectual property rights, particularly in long-term, multi-stage research environments such as medical research. The present work addresses this gap by integrating digital timestamping with a polling-based consensus mechanism, enabling collaborators to collectively assess contributions and establish proportional IPR ownership in a secure and tamper-resistant framework.

3. PROPOSED SOLUTION

Medical and pharmaceutical research generates highly sensitive and valuable intellectual assets, including experimental datasets, clinical trial results, analytical reports, and treatment protocols. These documents are the outcome of extensive expertise, time investment, and creative effort by researchers, clinicians, and institutions. Ensuring appropriate protection and attribution of such intellectual property is essential not only for legal compliance but also for sustaining innovation, trust, and ethical research practices. Without adequate safeguards, researchers risk misappropriation of their

work, distortion of findings, and disputes over ownership, issues that can significantly hinder scientific progress and collaboration.

Conventional intellectual property rights (IPR) frameworks often struggle to address the realities of collaborative research. In many cases, contributors are treated uniformly, regardless of the scale, timing, or impact of their individual contributions. This "equal-share" assumption may appear administratively simple, but it frequently leads to dissatisfaction, conflicts, and reduced motivation, particularly in long-term projects involving multidisciplinary teams. The challenge becomes more pronounced in medical research, where projects evolve over multiple phases and contributions are incremental, diverse, and temporally distributed.

To overcome these limitations, the proposed framework introduces a collaborative, contribution-aware IPR management system that integrates digital timestamping, blockchain-based document security, and a consensus-driven polling mechanism for ownership allocation. The core objective is to ensure that every contribution is securely recorded at the time of creation while enabling collaborators to transparently evaluate and agree upon the relative value of each participant's input. At the foundation of the system lies digital timestamping. This establishes verifiable proof of existence for each research artifact. Every document, whether textual, tabular, or image-based, is cryptographically hashed and timestamped before being recorded on the blockchain. This process guarantees data integrity, prevents unauthorized modifications, and preserves a chronological record of contributions throughout the research lifecycle. Any attempt to alter a timestamped record would require consensus from multiple distributed nodes, making tampering practically infeasible.

Building on this secure record layer, the framework incorporates a polling-based consensus mechanism to address the problem of equitable IPR allocation. Instead of relying on centralized arbitration or predefined ownership rules, collaborators participate in structured polling rounds to assess the significance of individual contributions. These polls allow members to express agreement, raise concerns, or propose adjustments regarding ownership shares, fostering transparency and collective accountability. By grounding ownership decisions in documented contributions and group consensus, the system aligns technical safeguards with real-world collaborative dynamics.

The architecture follows a hybrid design, combining centralized components for user authentication and access control with decentralized blockchain infrastructure for immutable storage and verification. Centralized services handle identity validation, role management, and authorization, ensuring compliance with regulatory and institutional requirements. Meanwhile, the blockchain layer stores encrypted document hashes, timestamps, and ownership metadata in a read-only, version-controlled manner. This separation balances efficiency with trust, enabling secure collaboration without sacrificing scalability. A key strength of the proposed solution is its support for dynamic ownership evolution. As research progresses and new data or insights are generated, ownership shares can be revisited through additional polling cycles, allowing the IPR structure to evolve alongside the project itself. This is particularly valuable in multi-stage medical research, where protocols are refined over time and contributions vary across phases. The proposed methodology adopts established cryptographic and blockchain mechanisms to ensure integrity, non-repudiation, and scalability. Secure hashing and digital signatures are employed to generate immutable document fingerprints, consistent with prior blockchain-based timestamping and proof-of-existence frameworks [18]. Batch timestamping using Merkle tree structures is incorporated to improve efficiency and scalability, as recommended in existing blockchain timestamping systems [19], while the overall design aligns with decentralized intellectual property protection models reported in the literature [20].

In summary, the proposed framework addresses critical gaps in existing IPR management systems by combining secure digital timestamping with blockchain-backed transparency and democratic, contribution-aware incentive allocation. By protecting sensitive research outputs while fostering fair recognition and trust among collaborators, the system provides a practical and scalable solution for modern, collaborative research environments.

4. METHODOLOGY

Medical research workflows involve ethically sensitive data, long project durations, and contributions from multiple stakeholders operating across different phases. These characteristics demand a methodology that ensures secure document handling, verifiable authorship, transparent contribution tracking, and equitable intellectual property rights (IPR) allocation. The proposed system addresses these requirements through a multi-phase workflow that integrates centralized authentication, cryptographic timestamping, blockchain-based storage, and consensus-driven ownership allocation. The overall execution flow is illustrated in Figure 1.

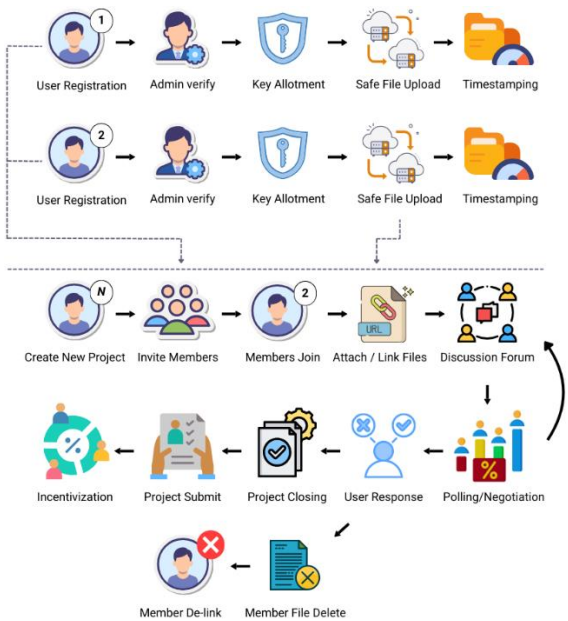

Figure 1. Proposed system execution workflow

4.1 Phase 1: Registration and identity authentication

The workflow begins with the registration of individual participants through an IPR management portal. Each user is required to possess a valid digital signature, which serves as a cryptographic identity for authentication and non-repudiation.

Public Key Infrastructure (PKI) is employed to verify user credentials, ensuring that only authorized individuals can access, submit, or modify research artifacts. This phase establishes traceability by binding every subsequent action, document submission, voting, or approval, to a verified identity.

The implementation involves three principal entities:

(a) The user requesting digital timestamping services,

(b) A centralized authority responsible for user validation and access control, and

(c) A digital timestamping server that issues timestamp tokens and manages protected document records.

Once registration and verification are completed, each user is issued a private cryptographic key, which must be securely maintained and is used for signing and protecting submitted documents.

4.2 Phase 2: Secure document submission and timestamping

After authentication, users may upload research documents to the timestamping server. Each document is hashed and digitally signed using the user's private key to establish ownership. The timestamping server verifies the signature and generates a timestamp token that binds the document hash to a verifiable time reference. The signed timestamp serves as immutable proof of document existence and authorship.

For scalability, the system supports batch timestamping using Merkle tree structures, allowing multiple document hashes to be anchored efficiently within the blockchain. This process ensures integrity while minimizing computational and storage overhead. The overall document protection and validation workflow is illustrated in Figure 2, which represents the supporting infrastructure layer of the proposed system.

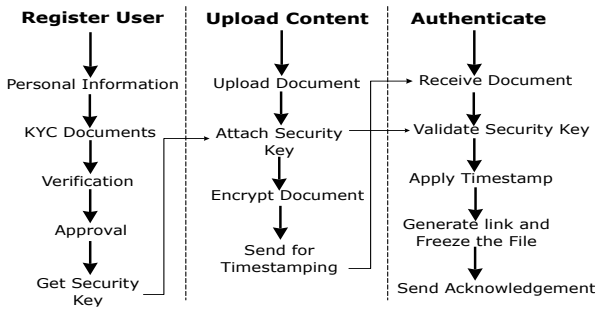

Figure 2. Timestamping based file management and validation process

Standard procedure for the digital timestamping is presented in algorithm 1 as given below.

Algorithm 1. Digital timestamping the document

```
/* Input: Original document. | Output: Fixed-size hash value (e.g., using SHA-256) */
Hash = SHA-256(document)

/* Send hash code and request for timestamp to digital timestamp server*/
Request = (Hash, Request Information)

/* Input: Hash and server's current time. | Output: Timestamp token (hash + timestamp) */
TimestampToken = (Hash, CurrentTime)

/* Input: Timestamp token. | Output: Digitally signed timestamp token. */
SignedToken = Sign(TimestampToken, ServerPrivateKey)

/* Server sends the digitally signed timestamp back to the client. */
Response = SignedToken

/* Verify the timestamp */
if (Hash(document) == HashInTimestamp) and Verify (SignedToken, ServerPublicKey):
    a. print ("Document is verified with timestamp.")
```

4.3 Phase 3: Formation of collaborative groups and document association

Once documents are securely registered, users can initiate or join collaborative research groups associated with a specific IPR application. Each group defines its scope, objectives, and participating members. Contributors may link previously timestamped documents or upload new artifacts directly to the group workspace.

The system supports both registered members and invited collaborators, enabling flexible participation while preserving document ownership and integrity. All documents remain permanently associated with their original owners and timestamps, allowing fine-grained tracking of contributions throughout the project lifecycle. This phase ensures transparency and structured collaboration from the outset. Figure 3 depicts the IPR application registration workflow, showing how users and documents are associated with collaborative groups within the proposed framework.

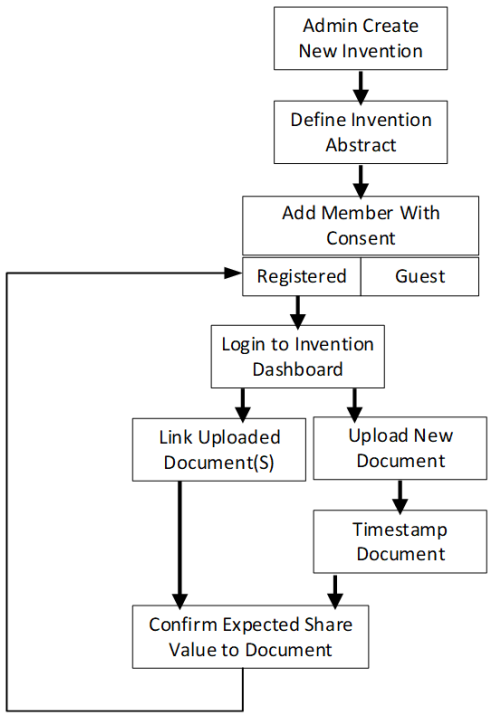

Figure 3. IPR application registration and member association

4.4 Phase 4: Contribution evaluation and polling-based IPR allocation

Following document submission, the system activates a polling-based consensus mechanism to evaluate individual contributions. Group members can review timestamped artifacts and participate in structured polling rounds to assess contribution value, raise concerns, or propose revisions to ownership shares.

This consensus-driven process replaces centralized or arbitrary ownership assignment with transparent, collective decision-making. Polling rounds may be repeated iteratively until consensus is achieved. If agreement cannot be reached, contributors retain the option to withdraw their participation and associated documents. The polling and share allocation workflow is illustrated in Figure 4.

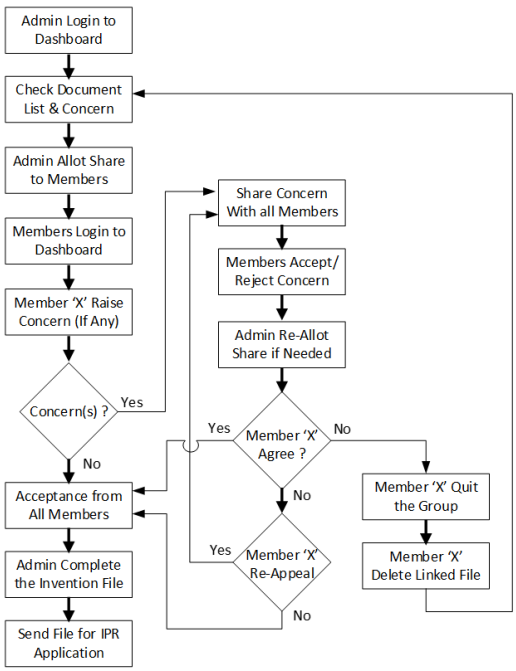

Figure 4. IPR share value discussion and polling mechanism

4.5 Phase 5: Agreement finalization and IPR submission

Once consensus is reached, the agreed ownership distribution is formalized through a digitally signed agreement accepted by all group members. The system maintains a multi-level association model, shown in Figure 5, linking users, documents, project phases, and ownership records through timestamped nodes and sub-nodes.

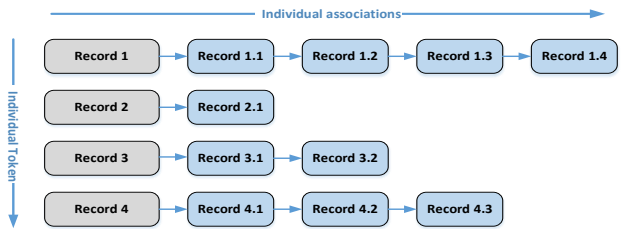

Figure 5. Multiple records with multi-dimension associations for on-going research protection architecture

In the final stage, the complete project package, including timestamped documents, polling records, ownership agreements, and metadata, is submitted to the IPR authority for examination and registration. Blockchain-backed storage ensures that all records remain immutable, auditable, and verifiable throughout the approval process.

4.6 Methodological summary

Through these five phases, the proposed methodology ensures that every research contribution is securely recorded, fairly evaluated, and transparently attributed. By combining digital timestamping with blockchain-backed immutability and consensus-based ownership allocation, the system enables trustworthy collaboration while minimizing disputes and preserving the integrity of sensitive research outputs.

5. CONCLUSIONS

This work presents a secure and transparent framework for managing intellectual property rights (IPR) in collaborative research environments, with particular relevance to medical research. By integrating digital timestamping, blockchain-based storage, and a polling-driven consensus mechanism, the proposed system addresses persistent challenges related to authorship verification, contribution tracking, and equitable ownership allocation. Each research artifact is cryptographically protected and timestamped at the moment of creation, ensuring data integrity and providing verifiable proof of existence throughout the research lifecycle.

A key contribution of the proposed framework lies in its consensus-based approach to IPR incentivization. Unlike conventional systems that assume static or equal ownership among contributors, this model enables collaborators to collectively evaluate and agree upon proportional ownership shares based on documented contributions. This approach enhances transparency, reduces the likelihood of post-collaboration disputes, and strengthens trust among participants. The hybrid system architecture, combining centralized identity management with decentralized blockchain storage, balances regulatory compliance, efficiency, and security. Despite its advantages, the proposed system has certain limitations. The effectiveness of polling-based consensus depends on active participation and honest evaluation by group members, which may be influenced by interpersonal dynamics or power imbalances in large research teams. Additionally, while the framework supports scalability through batch timestamping, performance may be affected in environments with very high transaction volumes or strict real-time constraints. Legal and regulatory variations across jurisdictions may also influence the practical deployment of blockchain-based IPR solutions.

Future work will focus on addressing these limitations by incorporating automated contribution metrics to complement human polling, exploring incentive-compatible voting mechanisms, and evaluating system performance under large-scale deployment scenarios. Further research will also examine integration with existing institutional IPR databases and compliance frameworks, as well as the application of post-quantum cryptographic techniques to ensure long-term security.

Overall, the proposed framework advances current approaches to collaborative IPR management by aligning technical security mechanisms with fair and transparent incentive structures. It offers a practical foundation for

fostering trustworthy collaboration while safeguarding intellectual assets in complex, multi-stage research environments.

REFERENCES

[1] Wang, J. (2023). Exploring digital timestamping using smart contract on the Solana blockchain. In Second International Conference on Green Communication, Network, and Internet of Things (CNIoT 2022), Xiangtan, China, pp. 184-190. https://doi.org/10.1117/12.2667788

[2] Meng, Z., Morizumi, T., Miyata, S., Kinoshita, H. (2018). Design scheme of copyright management system based on digital watermarking and blockchain. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, pp. 359-364. https://doi.org/10.1109/COMPSAC.2018.10258

[3] Shawn, L.W.M., Murali Mohan, P., Loh Kok Keong, P., Balachandran, V. (2021). Blockchain-based proof of existence (POE) framework using Ethereum Smart Contracts. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, USA, pp. 301-303. https://doi.org/10.1145/3422337.3450319

[4] Luo, L. (2022). Application of blockchain technology in intellectual property protection. Mathematical Problems in Engineering, 2022(1): 4641559. https://doi.org/10.1155/2022/4641559

[5] Varaprasada Rao, K., Panda, S.K. (2022). A design model of copyright protection system based on distributed ledger technology. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, pp. 127-141. https://doi.org/10.1007/978-981-19-1976-3_17

[6] Chen, Y., Bharadwaj, A., Goh, K.Y. (2017). An empirical analysis of intellectual property rights sharing in software development outsourcing. Mis Quarterly, 41(1): 131-162. https://doi.org/10.25300/MISQ/2017/41.1.07

[7] Ansari, S.Z., Zade, S.D. (2025). A blockchain-based decentralized framework for securing medical research data via digital timestamping. Ingénierie des Systèmes d'Information, 30(7): 1861-1867. https://doi.org/10.18280/isi.300718

[8] Sowmiya, B., Poovammal, E., Ramana, K., Singh, S., Yoon, B. (2021). Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server. IEEE Access, 9: 138245-138253. https://doi.org/10.1109/ACCESS.2021.3115238

[9] Hyla, T., Pejaś, J. (2020). Long-term verification of signatures based on a blockchain. Computers & Electrical Engineering, 81: 106523. https://doi.org/10.1016/j.compeleceng.2019.106523

[10] Ma, G., Ge, C., Zhou, L. (2020). Achieving reliable timestamp in the bitcoin platform. Peer-to-peer Networking and Applications, 13(6): 2251-2259. https://doi.org/10.1007/s12083-020-00905-6

[11] Liang, W., Zhang, D., Lei, X., Tang, M., Li, K.C., Zomaya, A.Y. (2020). Circuit copyright blockchain: Blockchain-based homomorphic encryption for IP circuit protection. IEEE Transactions on Emerging Topics in Computing, 9(3): 1410-1420. https://doi.org/10.1109/TETC.2020.2993032

[12] Reader, C. (2006). AVS intellectual property rights (IPR) policy. Journal of Computer Science and Technology, 21(3): 306-309. https://doi.org/10.1007/s11390-006-0306-3

[13] Kim, H., Hwang, D.J. (2001). A study on the system call for the protection of intellectual property rights on Linux base. In Proceedings 2001 Pacific Rim International Symposium on Dependable Computing, Seoul, Korea (South), pp. 295-298. https://doi.org/10.1109/PRDC.2001.992711

[14] Geethanjali, D., Priya, R., Bhavani, R. (2020). Blockchain-based protected digital copyright management with digital watermarking. Intelligent Systems and Computer Technology, 37: 9-17. https://doi.org/10.3233/APC200113

[15] Fallucchi, F., Gerardi, M., Petito, M., De Luca, E.W. (2021). Blockchain framework in digital government for the certification of authenticity, timestamping and data property. In Proceedings of the 54th Hawaii International Conference on System Sciences, pp. 2307-2316. https://doi.org/10.24251/HICSS.2021.282

[16] Abadi, A., Ciampi, M., Kiayias, A., Zikas, V. (2020). Timed signatures and zero-knowledge proofs—timestamping in the blockchain era—. In Applied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, pp. 335-354. https://doi.org/10.1007/978-3-030-57808-4_17

[17] Tas, E.N., Han, R., Tse, D., Yu, M. (202). Interchain timestamping for mesh security. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark, pp. 1585-1599. https://doi.org/10.1145/3576915.3616612

[18] Lu, W., Wu, L. (2024). A blockchain-based deployment framework for protecting building design intellectual property rights in collaborative digital environments. Computers in Industry, 159: 104098. https://doi.org/10.1016/j.compind.2024.104098

[19] Piccirillo, I.N., Amaral, D.C., De Oliveira, M.G. (2022). A research Agenda for collaborative roadmapping supported by blockchain technology. Sustainability, 14(20): 13093. https://doi.org/10.3390/su142013093

[20] Yuan, S., Yang, W., Tian, X., Tang, W. (2024). A blockchain-based privacy preserving intellectual property authentication method. Symmetry, 16(5): 622. https://doi.org/10.3390/sym16050622