Blockchain: Research and Applications 6 (2025) 100308

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Research Article

Tiered blockchain framework: A secure, trustworthy, and cost-efficient solution for the digital rights protection

Muhammad Hanif [a], Ehsan Ullah Munir [a], Muhammad Maaz Rehan [a,b], Saima Gulzar Ahmad [a], Imtiaz Khan [c,*], Rossitza Setchi [d]

[a] Department of Computer Science, COMSATS University Islamabad, Wah Campus, Wah Cantt 47030, Pakistan
[b] Department of Computer Science, School of Engineering and Computing, University of Lancashire, PR1 2HE Preston, UK
[c] Cardiff Metropolitan University, CF5 2YB Cardiff, UK
[d] School of Engineering, Cardiff University, CF24 3AA Cardiff, UK

ARTICLE INFO

Keywords:
Blockchain
Intellectual property (IP)
Intellectual property rights (IPRs)
Distributed ledger technology (DLT)
Security
Distributed computing
Digital rights
Access control

ABSTRACT

Protecting intellectual property (IP) in the digital age presents significant challenges due to rapid technological advancements and industrial growth. Traditional methods of registering and securing IP are becoming increasingly ineffective. To address these challenges, a more robust system is needed to control access, prevent unauthorized use, and safeguard digital rights. Despite efforts to transition from central registries to encrypted systems, vulnerabilities still exist that can compromise IP security. Therefore, a comprehensive solution must ensure legal use, prevent misuse, and enhance overall IP protection. This study introduces a robust framework designed to prioritize IP security and protection while addressing financial considerations. Our tiered Blockchain-based approach features logically segregated layers governed by smart contracts, which control access based on predefined agreements set by the IP owner. A common application interface (CAI) via smart contracts simplifies common operation with regard to an IP. The decentralized nature of Blockchain technology ensures unassailable trust, availability, and security. Additionally, we employ a flexible off-chain identity verification and storage mechanism for quick access and improved processing capabilities. Financial aspects tied to digital rights are managed through Blockchain's oracle services, ensuring seamless integration and management. Our integrated solution provides a reliable platform for IP protection, validated through thorough performance evaluations across diverse real-world scenarios. This framework demonstrates significant improvements in efficiency, security, and cost-effectiveness compared to traditional IP protection methods. By leveraging Blockchain's immutable ledger and decentralized network, we enhance the traceability and accountability of IP transactions, reinforcing legal compliance and reducing disputes. Ultimately, this approach ensures that IP is safeguarded, valued, and shared in a manner that benefits creators, consumers, and society as a whole. The rigorous analysis showed significant enhancements in process optimization, technology adoption, efficiency, and cost reduction compared to traditional IP rights protection practices.

1. Introduction and background

1.1. Introduction

Intellectual property (IP), encompassing patents, copyrights, trademarks, and trade secrets, plays a pivotal role in incentivizing innovation and creativity across diverse industries. The global IP licensing market is booming, with a current value of $13.23 billion in 2023, and is projected to skyrocket to $40.12 billion by 2030, growing at a remarkable rate of 17.05% annually from 2024 to 2030, unveiling vast opportunities for innovators and creators to monetize their IP [1]. According to the research study, IP infringement costs the average company almost $102 million in revenue per year, and that number is increasing with time [2]. Conversely, malicious actors persistently exploit vulnerabilities in

* Corresponding author.
E-mail addresses: hanif-cui@ciitwah.edu.pk (M. Hanif), ehsan@ciitwah.edu.pk (E.U. Munir), mmrehan@uclan.ac.uk (M.M. Rehan), saimagulzarahmad@ciitwah.edu.pk (S.G. Ahmad), ikhan@cardiffmet.ac.uk (I. Khan), setchi@cardiff.ac.uk (R. Setchi).

https://doi.org/10.1016/j.bcra.2025.100308
Received 8 December 2024; Received in revised form 8 January 2025; Accepted 10 February 2025

Available online 14 May 2025

intellectual property rights (IPRs) security protocols, resulting in the misuse of IP and subsequent financial losses for authors and owners in terms of royalty fees. According to Statista, there has been a discernible upward trajectory in IP disputes, specifically within the domain of cybersquatting based on data provided by the World Intellectual Property Organization (WIPO) between the years 2000 to 2022 [3]. In the year 2000, the recorded count stood at 1857 instances of cybersquatting disputes, encompassing 3760 domain names. Throughout this period, there has been observable variability in the numbers of both cases and domain names implicated in these disputes. Notably, a substantial surge in both case numbers and domain names involved became evident from 2019 onwards, culminating in 2022 with the highest figures on record, comprising 5423 cases entailing 7908 domain names [4].

These data underscore the escalating prominence of safeguarding IPRs in general and in the context of domain names in particular over the past two decades, with precise emphasis on the recent surge in such cases. Since its inception in 2012, the online copyright infringement tracker survey has emerged as a vital resource for documenting the prevalence of digital copyright infringement in the United Kingdom. WIPO has observed a notable uptick in submissions to its intelligence hub, surpassing the previous year's figures by a substantial margin, showcasing a 13% increase in referrals associated with online criminal activities [5]. The protection and safeguarding of these intellectual assets have become paramount in the digital age, where unauthorized reproduction and distribution have proliferated [6]. Traditional methods of IPRs protection, often reliant on centralized authorities, face significant challenges in adapting to the evolving landscape of technology-driven IP threats. This backdrop underscores the pressing need to explore innovative solutions that not only uphold the integrity of IP but also foster an environment conducive to innovation and fair compensation for creators [7]. To meet the escalating need for a highly trustworthy and secure protocol for safeguarding digital assets, the development of a robust IP protection system is paramount.

1.1.1. Problem statement

This research aims to address the pressing need for a sustainable and innovative solution to protect IPRs and effectively ensure IP integrity, security, and availability of IP across the ecosystem. The proposed solution prioritizes scalability, interoperability, and decentralization to ensure the long-term viability of IPRs protection in a rapidly changing digital landscape.

1.1.2. Motivation and contributions

IPRs protection emerges as a pivotal technological component within the framework of reuse-based design methodologies. In the context of an increasingly advanced high-tech landscape, the world is undergoing a profound transformation propelled by the dominance of data-driven processes [8]. Simultaneously, it's crucial to highlight the rising frequency of disputes related to the safeguarding of IPs. This surge in disputes has created significant challenges within the traditional IP ecosystem, emphasizing the growing need for innovative and sustainable solutions to protect digital rights [9].

This research study aims to introduce a mechanism for improving the safety, security, integrity, availability, and fair use of IPRs. The research study conducts the comprehensive research to present the current scenario of safeguarding the rights of IP owners within the digital realm and proposed viable solution which ensures the ownership and transparent utilization, transfer of IP, augment the cost effectiveness, and build trust without the need for an intermediary governing body.

1.2. Background

The current industry and government systems rely on centralized registries to ensure uniqueness, security, and fair compensation for inventors and owners. Digital rights management (DRM) technology has emerged as a pivotal tool for safeguarding IPRs in the digital realm. By exerting control over access, reproduction, and dissemination of digital content, including musical compositions, cinematic works, electronic publications, and software, DRM systems effectively protect the economic interests of content creators and distributors. Current DRM implementations typically employ a combination of encryption techniques and licensing mechanisms to ensure that digital content is only accessible to authorized users under predetermined conditions [10]. DRM technologies currently in use, including Silverlight, Flash Air, and the DRM systems employed by Windows and Apple, primarily concentrate on copyright management and content encryption. However, these systems exhibit significant limitations in addressing content leakage and accountability. In the event of unauthorized content dissemination, these DRM solutions lack the capability to trace and identify the parties responsible for violations. Furthermore, existing DRM technologies are inadequate in providing verifiable evidence of copyright infringement concerning digital content. While these systems have limited reach and operate within state legal boundaries, not protecting IPRs jurisdiction.

Protection of IP can be achieved through proper authentication, proof of ownership, and ensuring the legitimacy of the content. For this purpose, various publicly verifiable, fingerprinting mechanisms, digital signature (hashing), and watermarking schemes have been discussed and used in the literature. These practices are viable only for the physical security of the IP, while on the digital platform these techniques become useless [11]. The embedding of fingerprints into IP does not ensure the online copying and unauthorized use of IP. Similarly, watermarking the digital document does not ensure the protection of the IP on the network. One of the valid practices that ensure the security of the IP is the use of the hashing technique to encrypt the digital format of the IP on the network [12]. Protection of IP is a global phenomenon and is not bound to a specific location; therefore, its applicability and availability across the globe are one of the major requirements of the IP owners and users. Keeping in view the current issues and available option for a viable solution, Blockchain offers comparatively optimal characteristics to be considered a viable technology solution.

Blockchain, a distributed ledger technology (DLT), has transformed the technology landscape by introducing a secure and decentralized way of storing and sharing data, making it a game-changer in the fight against cyber threats [13]. Blockchain, as a peer-to-peer (P2P) network, supplemented by additional layers of security, transparency, and provenance, is well-suited for safeguarding IP. Blockchain enables efficient pricing, allowing for micro-monetization and establishing trust. This mechanism streamlines the distribution and utilization of IP via a smart contract-based interface. These smart contracts are designed to ensure compliance with the terms of use and service level agreements [14]. Its inherent characteristics, including decentralization, immutability, transparency, and smart contract capabilities, offer promising avenues for enhancing the security and management of IPRs [15]. By leveraging Blockchain technology, a paradigm shift is envisioned, where creators, innovators, and rights holders can assert greater control over their intellectual assets, minimize the risk of infringement, and streamline the complex processes of IP management. Furthermore, the integration of Blockchain technology can facilitate global accessibility and interoperability of IPRs, transcending geographical boundaries and legal jurisdictions.

To achieve global accessibility and applicability, a decentralized IPR system is proposed, with Blockchain technology offering optimal security, transparency, autonomy, and immutability. Blockchain has the potential to address concerns related to IPRs protection, licensing, and the verification of origins and ownership. Blockchain technology inherently embodies the principles of immutability, trust, security, and provenance, making it an indispensable solution for the protection of IPRs [16]. However, integrating the DRP system with current Blockchain applications faces challenges in scalability, legal compliance, and manageability. In detail limitations of Blockchain technology are described in the following section.

1.3. Limitations of the Blockchain technology

Blockchain technology presents a compelling vision for securing and managing digital rights, particularly in the realm of IP. However, this technology has significant limitations. One such limitation is its immutability. While this feature ensures security, it also makes it challenging to correct errors. Regulatory uncertainty, data privacy concerns, and security vulnerabilities pose additional hurdles. Additionally, Blockchain doesn't inherently verify the accuracy of the initial data entered; trust among participants is crucial. The relative immaturity of Blockchain technology is also a limitation, as various design choices impact factors like speed, security, and storage [17].

Blockchain, being a distributed storage, exhibits performance bottlenecks such as transaction delays and the high cost of on-chain data storage, that can significantly hinder the scalability and efficiency of the system. Transaction delays arise due to the consensus mechanisms employed by blockchain networks, where each transaction requires validation and approval by multiple nodes, creating latency that may affect real-time IP tracking and licensing processes [18]. Furthermore, on-chain data storage, although providing immutable records for IP can incur high costs due to the limited block sizes and the growing volume of data associated with IP assets. This can be particularly challenging in tiered blockchain models, where data is categorized and stored across multiple layers, potentially adding complexity in maintaining the balance between security, accessibility, and cost-efficiency. These bottlenecks necessitate the exploration of hybrid solutions that integrate off-chain storage, Layer 2 protocols, and optimized consensus algorithms to enhance the performance of blockchain-based IP protection systems [19].

Furthermore, challenges such as scalability, high energy consumption, and building trust for off-chain communication need to be addressed. The widespread adoption of Blockchain for IP protection is also hindered by interoperability issues and the complexity of achieving industry-wide consensus. High transaction fees and the substantial costs of setting up and maintaining Blockchain systems can be prohibitive, especially for small and medium-sized enterprises [20]. Moving forward, technological advancements in privacy-enhancing technologies and energy-efficient consensus mechanisms are crucial, alongside the development of clear legal frameworks for Blockchain-based IP management. By addressing these limitations, Blockchain technology can be effectively harnessed for robust IP and DRP.

The rest of this paper is organized into clear sections. In Section 2, a comprehensive review of existing research and comparison with current practices and key identified gaps are presented. Section 3 introduces the proposed method and framework, explaining how it addresses these gaps. Section 4 presents results and provides a brief analysis of what the results speak. Finally, in Section 5, concludes research findings and suggests potential directions for future research.

2. Literature review

IP protection has a rich history spanning centuries, arising to safeguard human creations, inventions, and innovations. Over time, various legal systems have evolved to grant creators exclusive rights, fostering innovation. However, modern challenges persist. Traditional systems struggle with issues like ownership proof, slow enforcement, and digital piracy threats, exacerbated by increasing digitization [8]. Many DRM systems aim to address IP violations, yet none are perfect. Various technologies, including watermarking, hashing, and centralized registries, have been proposed for IP protection. Blockchain technology has emerged as a disruptive force in this realm, offering decentralization, immutability, transparency, and cryptographic security [5,21,22]. Blockchain presents a new paradigm for IP management, addressing trust, transparency, and security issues. This article provides a comprehensive review to identify research gaps and understand the current state of IP protection using Blockchain technology. The upcoming sections delve into a comprehensive examination of legacy systems, highlighting their inherent weaknesses and substantiating the imperative need for a contemporary solution using Blockchain technology. Through an extensive literature review, the research aims to point out the deficiencies in existing legacy systems while also identifying prior research efforts in the realm of DRP.

2.1. Blockchain technology and IP protection

Blockchain technology has gained prominence as a state-of-the-art, transparent, and secure mechanism, finding widespread adoption in both scientific and industrial communities. It operates as a decentralized, immutable, and time-sequenced ledger, facilitating transactions by anonymous parties [23]. Miners competitively gather these transactions to form new chains, earning incentives for their successful creation of legitimate blocks. The Blockchain's data remains unalterable, as it undergoes verification and is stored at multiple participating nodes in addition to local copies. Any alterations to the local ledger version must undergo a consensus-based endorsement to be accepted by the Blockchain, ensuring tamper resistance. Users can access and trace any data within the Blockchain network, as transactions are validated before being recorded during the mining process, guaranteeing traceability and non-repudiation of transactions [24–26]. There are two kinds of Blockchains: proprietary Blockchains, where there are limits on who can take part and what can be done, and public Blockchains, in which anyone can read or write in the ledger. The Gartner research report showed that by 2030, Blockchain is projected to reach a market valuation of US Dollar 3.1 trillion. However, business spending grew dramatically by 2023 [27].

Blockchain networks provide an open and transformative platform for IP registries, offering cost-effective, faster, more precise, and reliable operations. This technology enhances the accuracy and transparency of rights management, especially in licensing systems and trademark processes, driving significant efficiency gains [22]. A research study [28] investigated IP protection using data encryption schemes based on quantum logistic maps, with ongoing efforts directed toward optimization. Moreover, studies suggest that adopting Secure Hash Algorithm 3 (SHA-3) over Secure Hash Algorithm 2 (SHA-2) can improve security and efficiency, particularly in hardware implementations. Secure Hash Algorithms (SHA) generate unique cryptographic hashes of fixed size for digital data, such as files or messages, ensuring data integrity. While limited studies address IP protection, existing research focuses on encryption and hashing mechanisms, but lacks exploration of cutting-edge technologies like Blockchain.

Numerous studies have explored the motivations driving researchers to commercialize their inventions. Conversely, BlockVerify [29] presents a noteworthy startup leveraging Blockchain technology to establish the provenance of luxury goods and physical products, effectively combating counterfeit issues by verifying the legal status of pharmaceuticals, diamonds, and electronics. In the public sector, Blockchain has far-reaching implications for state-maintained records. In regions plagued by poor data management and corruption, Blockchain offers a dependable alternative to existing registries. The immutability of Blockchain transaction histories prevents any tampering by corrupt individuals, while its decentralized nature virtually eliminates duplicate content. Notably, Blockchain's independence from a single governing authority safeguards against mismanagement-induced points of failure, ensuring the accuracy and integrity of records [30].

2.2. Legacy systems and research work

IP protection mechanisms commonly utilize watermarking, hashing, and digital signature-based techniques to achieve their objectives. Hashing, such as the Message Digest Algorithm 5 (MD5) is a cryptographic function that converts any message into a unique 128-bit "fingerprint."

Table 1 summarizes the major contributions by authors toward IP protection. Fingerprint and watermarking-based systems, although widely used, represent older practices compared to advancements in information technology. Researchers [31] have strategically employed public and private watermarking techniques to define and control IP access levels.

IP protection enables researchers to outsource the hunt for application and commercialization opportunities, allowing for specializations. Relationships with industry and other problems touching IP within the disciplines of research in which researchers are involved can play a major role in protecting IP. Table 1 summarizes and provides insights into the strengths and weaknesses of different approaches to IP protection, including watermarking and Blockchain-based solutions, while highlighting areas for improvement and potential security concerns. Watermarking, along with encryption techniques, adds to the protection level of an IP; the same techniques have been adopted in the research study for preventing IP infringements [32]. The encryption of the digital IP hash function-based encoding techniques has been incorporated to achieve an adequate level of protection [33]. The same techniques remain in use for a long time, but due to advancements in the processing power of computers, the encryption cracking techniques target the system and eventually, the same techniques become prone to attacks. To address the limitations block ciphers, an optimized solution based on a field programmable gate arrays based solution has been proposed [33], which is centered on computationally extensive signatures and consists of long bytes that are being utilized by industries due to its computationally intensive nature; the likelihood of implementation is difficult for ordinary users.

The IP trading scheme proposed by Ref. [20] leverages the Secure Hash Algorithm 1 (SHA-1) to facilitate random trading queries for verifying parties, preventing illegal multiple embedding and information stenography. The scheme adds anonymity to authorship, enhancing security and shielding IP from known attacks, with Ref. [34] demonstrating the successful integration of anonymity and traceability into blockchain for better security and efficiency.

While watermarking has traditionally safeguarded both physical and digital IP, its reliability has diminished with advancements in image processing. More contemporary approaches favor large key spaces and reduced computational time for enhanced security, with hashing being used to create unique IP identifiers [35]. Blockchain transforms IP protection by securing hashed digital certificates and automating royalties through smart contracts, simplifying IP processes for regulatory agencies, and ensuring originality [9]. It also addresses the challenge of cataloging works and verifying copyright ownership [36], as well as enhancing traceability of IP transactions. Research study [33] also emphasizes the difficulties faced by IP owners in identifying users and licensees. Blockchain's ability to maintain a comprehensive record of ownership and activities significantly improves IP rights management, overcoming limitations of legacy systems, particularly for online-published research articles.

Additionally, maintaining IPRs and traceability through a complete chain of ownership is a crucial challenge for DRP. Blockchain effectively addresses this by maintaining a comprehensive record of all activities and providing the provenance of every transaction recorded within it. A thorough literature review underscores the shortcomings of the legacy system currently in use for IP protection, especially concerning research articles published online.

2.3. *Limitations of the existing digital rights protection systems*

IPRs play a pivotal role in regulating the fair utilization of IP and upholding licensing terms; however, inherent vulnerabilities in this system expose it to unjust exploitation and breaches of usage agreements, endangering the investments made by IP creators [37]. One significant deficiency is the insufficient enforcement of IPR regulations, leading to inadequate protection of IP. Additionally, the lack of a standardized cost framework for safeguarding different forms of IP, coupled with economic disparities, results in inconsistent IP protection expenses. The imposition of supplementary processing and protection fees further burdens IP owners, potentially hindering efficient asset management. Moreover, many existing systems rely on outdated infrastructure, posing security risks exploitable by malicious actors. The human-dependent nature of these systems fosters a lack of transparency, creating an environment conducive to piracy and counterfeiting, undermining IP's integrity. Addressing these weaknesses in current IP protection systems is essential for ensuring security, fairness, and overall effectiveness in IP management and safeguarding.

A systematic review of IP protection methods reveals a notable lack of integration with modern technology, hindering the attainment of optimal security, protection, and transparency in IP utilization. Most of the research work in the IPRs domain suggests that Blockchain technology holds substantial promise for enhancing IP protection through avenues such as digital watermarking, traceability, authority management, and the implementation of Blockchain based IP registries. These advantages extend to areas like copyright registration, transaction monitoring, and evidence maintenance. Consequently, the literature underscores a research gap in IP protection, particularly the underutilization of advanced technologies like Blockchain to establish a transparent and resource-efficient mechanisms. Additionally, this study critically examines existing Blockchain-based IP protection systems, setting the stage for the proposed Tiered Blockchain IP Protection framework, aimed at addressing IP protection challenges.

Subsequent sections provide an in-depth description of the proposed method, working framework and insight discussions on performance indicators, evaluation results and real-world use cases of the proposed framework.

Table 1
Critical analysis of legacy systems and research: gaps, challenges, and resolutions.

Ref.	Year	Techniques / methods	Research gaps	Addressed research gaps
J. Fie et al. [38]	2022	Image watermarking technique for the protection of generative adversarial networks (GANs) model.	The proposed method has limited accuracy and is not suitable for higher parameters.	The research gap persists, and no suitable solution is proposed.
R.F. Ciriello et al. [12]	2023	Proposed design principles for Blockchain-based DRM for transparent licensing, rights metadata, and efficient royalty payout.	A standard Blockchain-based access control mechanism is used, which is prone to compromise.	A secure DRM with strong access control is a research gap that persists in the literature.
L. Xiao et al. [20]	2020	Proposed a distributed random embedding mechanism and position mapping function using the SHA-1 hash function for the protection of IP.	Utilized higher computational resources for hashing, which can be minimized by intelligent smart contracts.	Secure intelligent contract protocol [37] for IP protection mechanism is proposed.
S. Bhaduria et al. [21]	2021	The research study introduces a scheme for combining digital watermarking and Blockchain technology.	The watermarking is subject to sophisticated attackers by utilizing the latest technology.	The research gap has been addressed with a machine learning based solution [38].

Table 1 (*continued*)

Ref.	Year	Techniques / methods	Research gaps	Addressed research gaps
H. Kim et al. [39]	2019	The article examines Blockchain for IP registries, highlighting advantages over traditional methods due to drawbacks related to dispute resolution.	Dispute resolution in IPRs is proposed; however, the solution does not cover the rights of a group of people, i.e., IP owned by companies, etc.	The research gap persists; no suitable solution has been proposed to address the multifaceted IP protection system.
J. Lach et al. [40]	2001	Watermarking & MD5 for hashing, verification is done using the subset of the watermark	Linkage of watermark positions after public verification. This can pose a serious hazard to the IP owner.	Watermarking and MD5 hashing replaced with traceable IP protection algorithms [41].
G. Qu [41]	2002	Public-private watermark verification is done by revealing the encoding scheme	Watermark is subject to tampering attack, which is a serious copyright threat.	Copyright issues addressed using deep learning based intelligent watermarking [38].
S.P. Mohanty et al. [42]	2004	Added a watermark generated using linear feedback shift registers (LFSR)	Low values of peak signal-to-noise ratio (PSNR) indicate that there can be a threat to the watermarked image that has been tampered with.	Deep learning based intelligent watermarking scheme is proposed to address the copyright issues [38].
C.-C. Chang et al. [43]	2006	Using a fragile watermarking scheme over center 3x3 block embedding bits for generating a cryptographic hash function.	Cryptographic research work [44] contradicts the claims, tampering, and unique binding to the owner found missing.	Attribute based encryption (ABE) [35] proposed to address the cryptographic tampering issues.
D. Saha et al. [45]	2012	Zero-knowledge based field programmable gate arrays (FPGAs) digital signature. It addresses the issue of information leakage of the watermark.	Relies on the trust of IP buyers. Fake buyers can reveal the watermark information, which is a serious security threat.	Zero trust-based solution [2] has been proposed to address the fake identity protection.
A. Garba et al. [46]	2021	Using scalable Blockchain-based overlay network, a DRM system providing security of digital content by Digital watermarking is proposed.	The research study utilized the public blockchain, which exhibits higher latency, transaction maturity time and limited applicability scope.	A secure DRM with strong access control is a research gap that persists in the literature.
H. Zhang et al. [34]	2023	Blockchain based, anonymous and traceable intellectual property management (ATIPM) is proposed to enhance protection and efficiency using smart contracts.	The research study only discusses the private Blockchain scheme and does not provide public access to the Blockchain network.	The issues of incorporating the three modes (e.g., public, private, consortium) of Blockchain persist.

3. Proposed solution and framework

Long-term prosperity and economic success hinge on a nation's ability to innovate and be creative. IP protection is one of the most essential governmental regulations in the industries and global marketplaces of the twenty-first century [47]. The fundamental right of IPR protection is to foster innovation by allowing IP owners to recoup their research and development costs [22]. These intellectual rights are being protected using different mechanisms. However, a universal system addressing the basic functionality of IP protection is deemed necessary. The proposed solution primarily harnesses the power of Blockchain technology to safeguard the digital rights of IP across networked environments. The Tiered Blockchain framework represents an evolution of traditional Blockchain structures, as it introduces the concept of logically separated tiered chains, each inherently distinct and maintained. The primary objective behind adopting this tiered structure is to establish a robust access control mechanism for the protection of digital rights. This innovative framework aims to enhance the security and management of IP rights, ultimately fostering a more secure and incentivized environment for innovation and economic growth.

3.1. Proposed system architecture

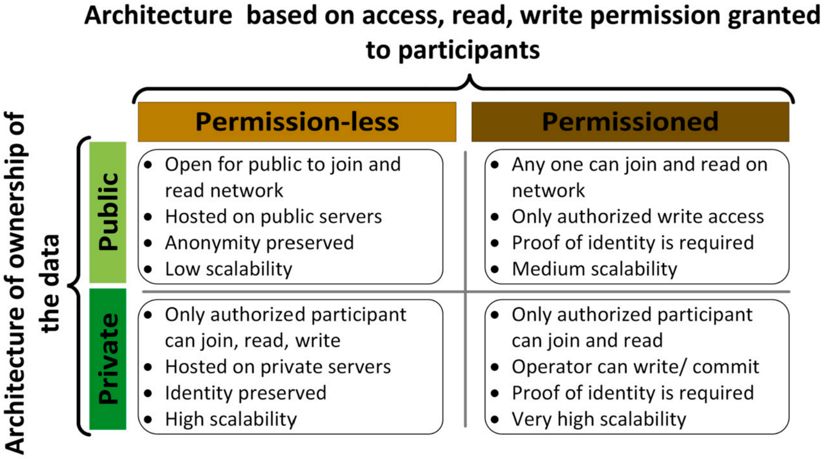
In the digital realm, access control mechanisms play a pivotal role in ensuring the confidentiality, integrity, and availability of digital content. To systematically manage digital rights, a segregation of relevant entities is imperative. This research study introduces a three-tiered approach, categorizing them as public, private, and consortium, which are fundamental types of Blockchains employed across various domains. However, this study takes a novel approach by amalgamating these types into a unified chain, implementing them logically, thus achieving a harmonized outcome.

Fig. 1 illustrates a classification of blockchain architectures based on access, read, and write permissions granted to participants. It categorizes blockchains into public and private types, with further subdivisions into permissionless and permissioned models.

1. Public permissionless: open to anyone for joining and reading, hosted on public servers, preserving anonymity but with low scalability.
2. Public permissioned: anyone can join and read, but only authorized participants can write. Identity proof is required, offering medium scalability.
3. Private permissionless: restricted to authorized participants for joining, reading, and writing, hosted on private servers, ensuring identity preservation with high scalability.
4. Private permissioned: only authorized participants can join and read, while an operator handles write/commit actions. Proof of identity is mandatory, offering very high scalability.

Open source Blockchain technology is typically deployed in public and permissionless environments, which aligns with its broader scope and application. However, when it comes to safeguarding IP, a private Blockchain with permissioned access levels proves to be a suitable choice. In the realm of modern Blockchain 3.0 technologies, robust solutions for implementing IP protection systems are readily available. Prominent examples include Hyperledger Fabric and Ethereum, both of which operate within the private permissioned Blockchain ecosystem. These platforms offer advanced network and organization-level access management protocols, ensuring a secure and controlled environment for the protection of IP. Traditional DRM systems have limitations in addressing content management violations. Blockchain technology offers a solution by providing a secure and transparent framework. It enhances content protection by tracking usage, identifying violations, and holding violators accountable [48]. This addresses the limitations of legacy DRM systems and promotes a fairer and more secure environment.

In IP protection using a tiered Blockchain, trust, privacy, and security are essential components. Trust represents the stakeholders' reliability in the system's integrity and fairness, fostered by transparent and



Architecture based on access, read, write permission granted to participants

Architecture of ownership of the data

	Permission-less	Permissioned
Public	Open for public to join and read network Hosted on public servers Anonymity preserved Low scalability	Any one can join and read on network Only authorized write access Proof of identity is required Medium scalability
Private	Only authorized participant can join, read, write Hosted on private servers Identity preserved High scalability	Only authorized participant can join and read Operator can write/ commit Proof of identity is required Very high scalability

Fig. 1. Comprehensive information of a Blockchain-based system, showcasing varying levels of data access control in public and private blockchains, and highlighting their distinct access privileges and security features.

immutable records. Privacy ensures the confidentiality of sensitive IP transaction details and user identities, protecting them from unauthorized access [49]. Security encompasses the technical measures, such as cryptographic techniques and consensus algorithms, that defend the system against attacks and unauthorized actions [50]. Proposed tiered blockchain IP protection system, implemented while balancing security, trust, and privacy, a secure and reliable environment. The proposed system also offers a comprehensive range of services to consume the IP in different ways, depending on the platform and utilization. In the following sections, a detailed discussion is presented on the proposed framework.

3.2. Tiered Blockchain architecture

IP can be safeguarded through various methods, including lightweight binary watermarking, signatures, and hashing utilizing a public-private key architecture. The primary goal in IP protection is to achieve immutability and trust, and Blockchain technology offers these properties with minimal trade-offs. The Blockchain network is structured into three logical layers, each determined by the level of access. Since the proposed system is based on the Ethereum public Blockchain, these layers correspond to networks and align with the logical organization structure inherent in Ethereum's three-layered architecture.

The tiered architecture of blockchain, structured into logically separated layers—Public, Private, and Consortium—offers a powerful approach for the efficient and scalable protection of IP. This design leverages the strengths of each layer to address distinct access and data management needs. The Public Layer provides open access to general metadata, ensuring transparency and enabling public verification without compromising sensitive information. The Private Layer is reserved for storing critical and confidential IP data, accessible only to authorized users, is based on access granted through a smart contract. Whereas the Consortium Layer facilitates collaborative data sharing among a specific group of users or organizations, enabling secure multi-party transactions and co-management of IP assets. By segregating data and access rights across these layers, the tiered architecture optimizes resource utilization, reduces transaction costs, and enhances scalability. This layered approach not only bolsters the security and integrity of IP protection systems, but also lays a solid foundation for the broader adoption of blockchain-based applications in complex, data-intensive environments.

A tiered approach, as depicted in Fig. 2, offers a robust framework for managing IPRs, combining the benefits of public and private access levels in blockchain paradigms. This multi-tiered approach provides a scalable and secure environment, balancing openness and confidentiality, making it ideal for IP management and sensitive applications. At the core lies the Logical Tiered Manager, which handles data segregation into three layers: Public (public metadata), Private (restricted data for authorized users), and Consortium (data accessible to specific groups). The framework integrates Identity and Access Management for user privileges and an Oracle Service Registry to connect with external off-chain storage and payment exchanges via oracle services. The common application interface (CAI) bridges the blockchain with a Web3.js-powered application and an interactive user dashboard. The design ensures secure and scalable access control, supporting both on-chain and off-chain transactions while maintaining proof-of-ownership and robust IP integrity.

3.3. IP protection working framework

The system is structured with virtual layers that effectively manage access control for different levels of access rights. These access rights are categorized into three main types: public, private, and consortium based. In the public rights category, access is open to all users within the network. Private rights restrict access to the owners of the assets exclusively, while consortium-based access rights are specific to certain individuals or groups whose access is carefully managed. Fig. 3 depicts the workflow of this layered approach in the system's operational model. In this model, the underlying Blockchain primarily serves as a storage platform for digital assets. However, access to these assets is controlled using a tiered token-based mechanism, where access tokens are issued through a smart contract interface. This structured approach ensures secure and organized management of access rights within the DRP ecosystem.

Fig. 3 illustrates a tiered blockchain-based framework that integrates private, consortium, and public tiers to facilitate robust IP rights management. At the top, the author or owner registers their unique identity and IP with a CA, which issues a certificate. The private tier is responsible for handling sensitive IP-related data, including physical documents, designs, or digital media. It enforces IP rights and implements access control mechanisms. Access permissions are managed through a defined list of users, roles, and groups, with specified time periods for access.

The consortium tier determines whether collaborative support from a group of administrators or organizations is needed to manage shared IP. This tier facilitates decentralized management of shared resources. The public tier stores publicly accessible metadata and related information about the IP using blockchain technology, ensuring transparency and security. Ethereum and its sidechain are integrated via a CAI to enable seamless interactions, improve scalability, and prevent double-spending. Additionally, the framework connects APIs, gateways, IP of-

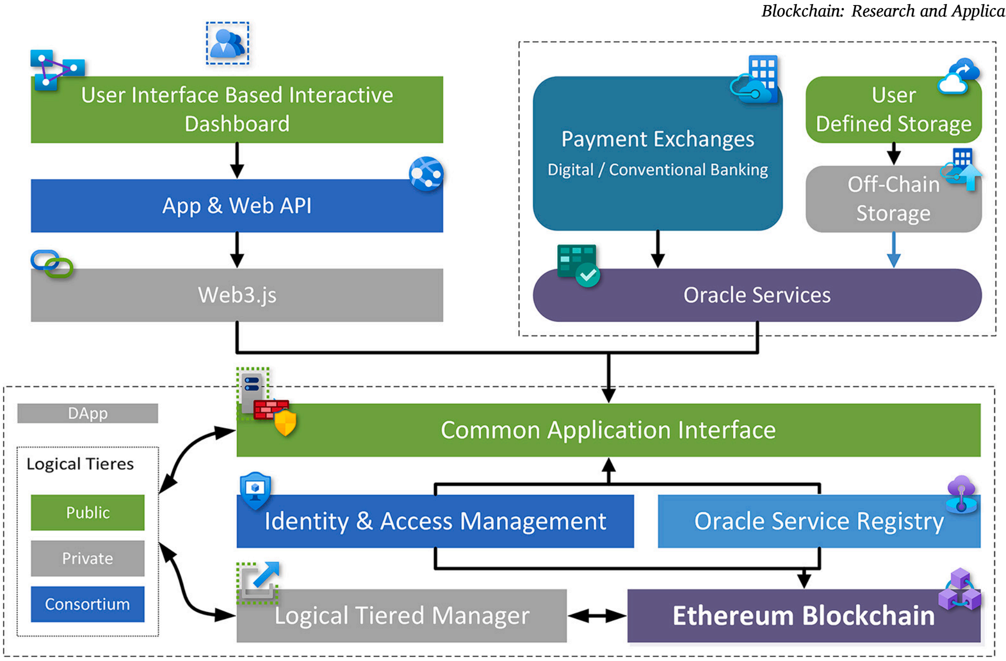


Fig. 2. Block Diagram of the proposed system, integrated with Oracle services through a common application interface (CAI).

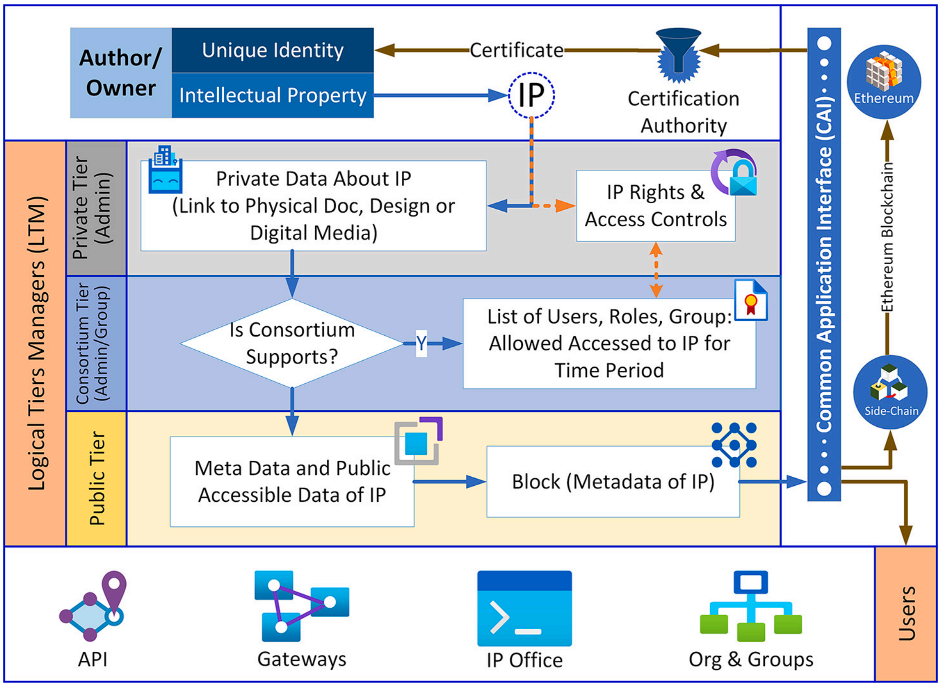

Author/ Owner
Unique Identity
Intellectual Property
Certificate
IP
Certification Authority
Logical Tiers Managers (LTM)
Private Tier (Admin)
Private Data About IP (Link to Physical Doc, Design or Digital Media)
IP Rights & Access Controls
Consortium Tier (Admin/Group)
Is Consortium Supports?
Y
List of Users, Roles, Group: Allowed Accessed to IP for Time Period
Public Tier
Meta Data and Public Accessible Data of IP
Block (Metadata of IP)
Common Application Interface (CAI)
Ethereum
Ethereum Blockchain
Side-Chain
API
Gateways
IP Office
Org & Groups
Users

Fig. 3. Data flow diagram of the proposed system presenting the tiered Blockchain structure for intellectual property (IP) protection.

fices, and organizations to create a comprehensive and scalable IP management system.

The adoption of a tiered Blockchain framework has introduced a highly optimized access control mechanism that aligns seamlessly with the separation of concerns principle. This strategic approach aims to enhance the efficiency of the system by segregating user access levels, a crucial factor in ensuring that the performance of the proposed scheme can scale effectively to accommodate a large user base. The tiered structure also brings an array of benefits; one of the main functionalities among those benefits is the streamlining of access rights management. By organizing access control into distinct tiers, this mechanism effectively minimizes conflicts and mitigates the risk of privilege escalation scenarios. This not only ensures smoother and more reliable access to digital rights but also fortifies the overall security and integrity of the system.

3.3.1. Logical tiered architecture (LTA) manager

The tiered architecture enhances security and privacy on top of the distributed network by organizing data into logical layers. The LTA manager is responsible for transforming data into the appropriate format for Blockchain storage. Additionally, it manages access to off-chain storage based on the access levels associated with a particular IP. To better describe the framework's operation, the system's workflow is explained in the following paragraphs.

To access digital IP on the network, users must first become authenticated members of the network. This involves a series of steps designed to ensure secure access to IP details. Step 1 entails prospective buyers fulfilling a smart contract containing essential conditions for IP acquisition, including payment and affiliation. Affiliation implies a user's association with a company or group that already has access to the specific IP. Step 2 within the IP system, enables users to initiate purchase requests for specific IP via a smart contract, meeting predefined criteria. Step 3 involves the selling process, initiated when users request to purchase IP. For IPs with special criteria requiring owner approval, access rights approval hinges on the owner's consent. The entire DRP process operates through a smart contract-based interface, where smart contracts enforce algorithms to maintain transparency. Subsequent sections delve into the specifics of these smart contracts and their implementation.

Once IP is published on the Blockchain network, access to it is controlled by the owner of the IP. The owner retains the authority to distribute copyright and other sharing rights related to the IP. To manage sharing and royalty earnings, smart contracts are employed. These smart contracts contain the logical code that governs how the Blockchain handles distribution and access rights. By utilizing smart contracts, this research ensures the protection of royalties and minimizes access by unauthorized entities, enhancing the security and integrity of IP within the Blockchain ecosystem. Management of a blockchain-based system relies on the different governing roles. These roles are responsible for maintenance, updates, and ensuring the smooth running of the system. Following is the detail description of key components of the proposed system.

3.4. *Key components of proposed system*

The proposed system is a complex ecosystem comprising various interconnected and interdependent components. These components collaborate seamlessly to facilitate secure, transparent, and efficient transactions on a blockchain network.

3.4.1. *Identity and access management*

IP represents the primary asset targeted for protection, and each IP is assigned a globally unique identifier. The system's foundation relies on the initial declaration and verification of the actual IP owner. Ownership history, including previous owners (i.e., provenance), is preserved. Metadata, such as the creation date, nature, unique identifier, and scope, are vital metrics that determine the IP's uniqueness and are accessible for record searches. The following principal actors participate in maintaining the system:

Owner. The owner is responsible for registration, asserting ownership, signing smart contracts, and receiving royalties for the IP. Owners play a central role in the Proof of Ownership (PoO) consensus mechanism, which validates IP ownership at a specific point in time.

Service requester. The service requester initiates service requests or invokes smart contracts, following predefined steps to complete contracts, the requester of IPRs must sign a contract via a smart contract and pay applicable royalties.

Certification authority (CA). The CA regulates IP protection and enforces its fair usage policy. CA issues certificates to validate the legitimacy of the Blockchain-based ecosystem and provides validation certificates to owners, confirming their identity through the PoO consensus mechanism.

Administrator. Administrators ensure the system operates smoothly. Due to the distributed system's nature, platform maintenance is distributed, and administrators are responsible for system upkeep. Administrators have no stake in the system other than the development and the publication of necessary updates, which are committed after achieving consensus.

Trusted nodes. Trusted nodes are essential for maintaining a secure ecosystem. These specialized nodes have dedicated roles in consensus, user authentication, and transaction verification, making them trustworthy actors in the system.

Notary. All smart contracts are sent to the Blockchain network, and notaries actively participate in verifying smart contract proofs. Notaries assess service effectiveness and authenticate ownership for both service requestees and owners when receiving a smart contract. If the service contract is valid and all IP licenses are legitimate, it is accepted as valid and added to the Blockchain ledger. If the majority of notaries validate the smart contract successfully, the proof process is considered complete.

3.4.2. *Smart contracts*

Smart contracts are lines of code stored on the Blockchain that automatically execute when predefined terms and conditions are met. These contracts facilitate IP agreements such as licenses and permission fees, allowing IP owners to define terms in real time. Smart contracts execute the agreed upon terms between the owner and buyer during the sale, ensuring transparency and transaction history. Smart contracts also enable the transfer of IP to other users by any owner, ensuring seamless asset transfer on the Blockchain while keeping the security, integrity, and authenticity intact. A detailed description of key smart contracts is presented in Section 3.8.

3.4.3. *Immutable storage*

Blockchain technology's security stems from its resistance to tampering. Hackers attempting to alter data within a Blockchain need to modify all successive blocks in the chain, making their changes detectable and ineffective. Furthermore, each piece of data in the Blockchain is recorded with a unique digital hash, complete with a timestamp. Any attempt to manipulate this data becomes evident, as the new digital fingerprint does not match the original one. Blockchain's operation introduces an exceptional level of trust to everyday enterprise data, offering data integrity and transforming auditing into an efficient, cost-effective process that demonstrates data's tamper-free nature to stakeholders. To demonstrate the immutability of the storage in a mathematical model: Let B be the set of blocks in the Blockchain, $H(b)$ represents the hash function applied to block b, resulting in a unique hash value, $P(b)$ denotes the previous block in the chain. To calculate the hash of the block:

$$H(b) = \text{hash}(\text{blockData}(b) + \text{hash}(P(b))), \forall b \in B \tag{1}$$

Where, $blockData(b)$ represents the data contained in block b, and $hash(P(b))$ is the hash of the previous block. Eq. (1) ensures that the hash of each block is computed based on its data and the hash of the previous block. Any attempt of tamper with the Blockchain can be identified by comparing the calculated hash of a block with its stored hash in the Blockchain. If both hashes do not match, it indicates tampering.

3.4.4. *Encryption*

Digital signatures using cryptographic key pairs facilitate participant authentication, asset ownership verification, transaction initiation, smart contract signing, and data registration within the Blockchain network. Verified transactions are time-stamped and incorporated into blocks of data, secured through cryptographic hashing. Each new block's hashing process includes metadata from the previous block, creating an unbreakable chain. Any attempt to alter or delete validated data is thwarted because subsequent blocks reference the original data, making modifications detectable and rejectable due to invalid hashes. In essence, tampering with the data breaches the Blockchain protocol and is immediately detectable. This robust feature contrasts sharply with traditional databases, where data modifications or deletions occur easily and inconspicuously.

3.4.5. Off-chain storage

Off-chain storage offers a scalable and efficient solution for managing large or sensitive data in blockchain systems. This approach enhances system efficiency while giving users the flexibility to manage their data through oracle services. The proposed method incorporates off-chain storage via a smart contract-based oracle service, enabling the secure storage of IP-associated physical data or digital media. The data is encrypted and stored on user-specific storage solutions or decentralized platforms like the InterPlanetary File System.

Only metadata and access controls are stored on the blockchain, ensuring transparency, immutability, and traceability without overloading the chain with excessive data. Encryption ensures that access to off-chain data is restricted to authorized parties with the appropriate decryption keys, enhancing security and privacy. Oracle services act as a bridge between the blockchain and off-chain storage, facilitating seamless interaction, real-time synchronization, and integrity validation. By offloading data to off-chain systems, this approach reduces blockchain congestion, improves transaction efficiency, and enhances the framework's ability to manage diverse and complex IP assets. This seamless integration of blockchain's robustness with off-chain storage's flexibility provides a comprehensive, scalable, and efficient solution for modern IP rights management.

3.5. PoO consensus mechanism

Evidence of ownership through establishing the consensus for an IP right is a critical task. The key benefits of PoO are the lack of unnecessary computational processes, and as a result, a lower entry barrier for block creation and authentication is achieved. Authentication on the Blockchain network is always achieved through consensus. Consensus is the mechanism that ensures the implementation of the rules agreed upon by the community on the P2P network. Generally used consensus mechanisms in DLT are Proof of Work [30], Proof of Existence [51], and Proof of Burn [52], are few consensus mechanisms among others, to authenticate the originality of the action performed by the user on the network [25].

In the context of IP protection, ownership proof is a key metric for authenticating IP ownership. To address this issue, PoO is proposed to identify IP ownership. This mechanism accurately identifies the rightful owner of the IP claimed as an owner on the DRP network. The protocol ensures the distribution of owned IP with the consent of the owner. A brief pseudo-code for the PoO algorithm is presented as Algorithm 1.

To maintain ownership, a fuzzy hashing mechanism (ω) is introduced to verify the ownership of the file. To conceptualize the ownership verification mechanism, different registries are maintained:

$\omega_{f\epsilon} = \{\omega_{f\epsilon_1}, \omega_{f\epsilon_2}, \omega_{f\epsilon_3}, \dots, \omega_{f\epsilon_n}\}$ a registry of fuzzy hashes corresponding to unique IPs, $\epsilon = \{\epsilon_1, \epsilon_2, \epsilon_3, \dots, \epsilon_n\}$ a registry of IP information, $U = \{u_1, u_2, u_3, \dots, u_n\}$ the set of registered users on the DRP network, $O_\epsilon = \{o_{\epsilon_1}, o_{\epsilon_2}, o_{\epsilon_3}, \dots, o_{\epsilon_n}\}$ the owner's registry having one or more IPs, $A_{\epsilon u} = \{a_{\epsilon u_1}, a_{\epsilon u_2}, a_{\epsilon u_3}, \dots, a_{\epsilon u_n}\}$ the list of users who have rights to the corresponding IP. Given these definitions, PoO is the Boolean function that takes the IP (ϵ) and user (U) as input and returns the ownership authenticity as described below.

$$\Delta(\epsilon) = \prod_{k=1}^{n} \omega_{f\epsilon_i} \text{ where } \omega_{f\epsilon_i} \in \omega_{f\epsilon} \tag{2}$$

$$\text{PoO } (\epsilon_i, U_i) = \Delta(\epsilon) \wedge [U_i, \epsilon_i | U_i] \tag{3}$$

Eq. (2) describes the mathematical model of the fuzzy hash calculation function Δ, which takes the IP as the input function and returns its matching percentage. Here, ϵ contains the identification details (i.e., block IDs) of the IP stored in the Blockchain, which are always unique. U is the registered user on the DRP network, and A_{ϵ_u} represents users with granted access to the network for certain IPs.

PoO calculates the ownership of IP ϵ_i for a user u_i with the ID ω_{fhi}. ω_{fhi} belongs to the registry of fuzzy hashes of authenticated IPs (as per Eq. (3)) on the network against a certain owner O_i who has legally granted access to registered users. The PoO defines a clear mechanism for the authentication of the owner and access rights for users who have legitimately acquired access for content retrieval.

Hence, PoO is defined by a summary function PoO(U_i, ϵ), which can be randomized and takes the input file ϵ and a security parameter U. It also involves an interactive two-party protocol $\Pi(\epsilon \leftrightarrow U)$.

PoO is a dedicated consensus mechanism tailored to meet the requirements of IP ownership verification, operating as a sidechain to the Ethereum Blockchain. This mechanism enhances the security and efficiency of IP management by leveraging consensus independence while maintaining periodic anchoring to Ethereum for added verification and security. PoO enables the sidechain to implement custom consensus algorithms, providing flexibility and adaptability for specific applications.

The integration is facilitated through bridge contracts deployed on Ethereum, which lock assets on the main chain and mint equivalent tokens on the sidechain, ensuring seamless asset transfer and preventing double-spending. By offloading transactions to the sidechain, this approach addresses Ethereum mainnet scalability issues, reducing network congestion. Additionally, it promotes interoperability by enabling diverse consensus mechanisms suited to distinct use cases while relying on Ethereum's robust infrastructure. This innovative integration ensures secure, transparent, and efficient protection of digital assets, significantly enhancing Blockchain technology's potential in managing IPRs.

Validity. The validity scheme $PoO = (U_i, \epsilon_i)$ is valid under the following conditions:

1. U and ϵ are both already registered with DRP, and U belongs to the list of owners of ϵ (IP).
2. For every input IP $\omega_{fhi} \in \omega_f \epsilon$, it holds true in the $\Pi(\epsilon \leftrightarrow U)$ relation.

Efficiency. The key efficiency constraint of PoO is the IP with minor changes in content (for digital IP only) in this case all possible matches of hashes are considered.

While Blockchain technology can be used in different ways, a Blockchain solution generally builds on four features: security, immutability, provenance, and decentralized validation. On Blockchain, triggering a transaction initiates the process for new data blocks describing the transaction added to a chain after attaining the consensus among the relevant participants and the validity of the transaction. In the proposed method PoO is being used on top of the PoS algorithm, being the default consensus algorithm of the Ethereum Blockchain.

Algorithm 1: Pseudo-code for PoO consensus mechanism.

```
Input  : ipHash(H), Sender(S)
Output: bool
Start
while true do
    Search for H in ipRegister (R)
    if found then
        return $ip.owner == S$
```

Redundancy. The Blockchain is continuously replicated on all or at least a group of nodes in a network. As a result, no single point of failure exists [31]. Data redundancy is one of the critical parts of the proposed system. To ensure the system always remains synced, no selected miner node should be inactive during consensus. If a particular node is offline, the transaction will wait until enough nodes are online to reach a consensus.

$$P = \{p_1, p_2, p_3, \dots, p_n\}, P_a = \{p_i, p_j, p_k, \dots, p_x\} \tag{4}$$

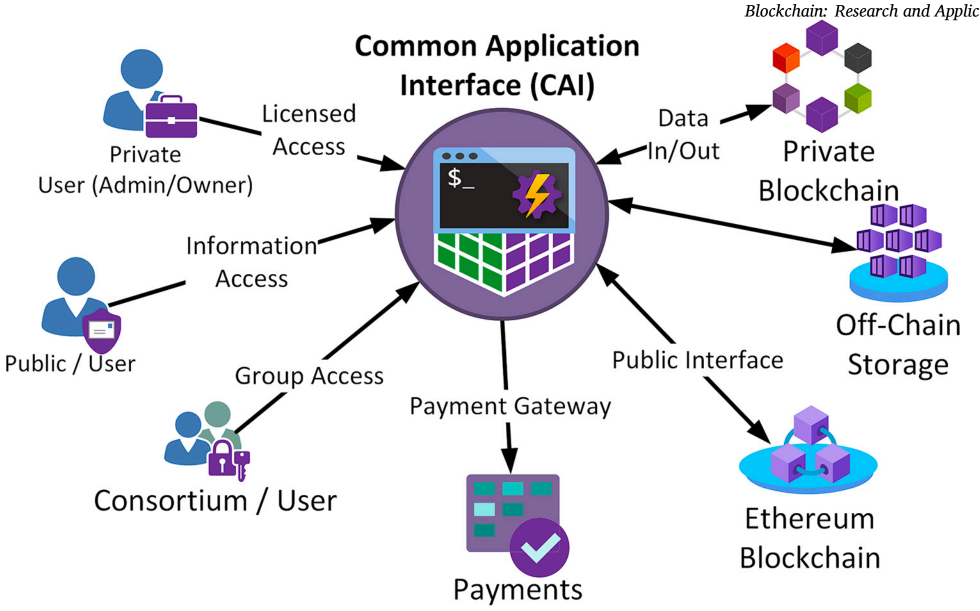


Fig. 4. Work flow of the on-chain and cross-chain communication architecture for secure IPRs management, showcasing a tiered approach for accessing IPRs and IP assets through a common application interface (CAI).

$$C = \sum_{p_a} \quad \therefore \quad p_a \subseteq P, C \geq \frac{3}{2} P \wedge C_s \geq P_s \qquad (5)$$

In Eq. (4) P is the set of all registered node peers on the network, P_a are the live node peers at the time of consensus, and a subset of the P. C is the consensus on the PoO mechanism that depends upon the majority peer's endorsement for checking the transaction as legitimate or $false$. If consensus is reached with fewer peers than required, it is considered null and void. Then, as per Eq. (5), consensus C_s $[Consensusofselectedtrustedpeers(P_s)]$ is computed, if the majority of peers endorse the ownership it is treated as true, otherwise, the request is denied.

3.6. Ownership privileges

Maintaining ownership of an IP is the protection aim of the proposed system. To protect the ownership of the IP, a PoO consensus mechanism has been proposed. This mechanism restricts the access as well as the change in the IP with the permission of the owner using the smart contracts being associated with the time of publishing the IP on Blockchain. The security of the platform is ensured through a strong PoO consensus mechanism. Without the need for a central certifying authority, transactions are rendered, this mechanism is particularly suitable for the authentication of ownership rights. This includes digital property, IP, and physical property, including physical products and land.

Detailed workflow for on-chain and cross-chain communication architecture through CAI is presented in Fig. 4, which shows that access permissions are mandatory for each user to access the IP, for these purposes, the user has to pass through the smart contract of that IP and fulfill all the conditions of the contract prior to access the IP. The smart contract comprises all the logic required to get legitimate access to the IP, including paid and membership-based access. Ownership information is to be kept on the Blockchain, and access is granted to authorized devices and peers passing through the smart contracts only. This architecture leverages smart contracts and a payment gateway to facilitate secure and efficient transactions, enabling seamless communication between IP owners, users, and payment systems.

These smart contracts embody a comprehensive set of terms and conditions governing usage and access. Smart contracts dictate how data is retrieved from the Blockchain, facilitating this process through a CAI. This CAI serves as the gateway through which authorized parties interact with the Blockchain to access the specified IP and its associated rights. Smart contracts ensure that every aspect of IP usage adheres to predefined rules and temporal constraints, thus providing a systematic and transparent framework for managing and controlling IP access. Through the API, users can securely and efficiently interact with the Blockchain to access the protected IP, with the smart contracts serving as the binding agreements that enforce compliance with IP ownership and usage terms.

Smart contracts are at the core of the system, encapsulating the business logic governing authorized IP usage and managing the entire authorization process, from initial request to the terms of use. To ensure the efficiency and responsiveness of the Blockchain, digital versions of the IP are stored in off-chain storage. This approach keeps the Blockchain lightweight and agile, enabling swift access to data. Integration with off-chain storage is facilitated through oracle services. Oracle services act as intermediaries that identify and validate real-world events, providing this information to smart contracts on the Blockchain. The payoff mechanism is a pivotal component of the IP protection system, ensuring that authorized parties receive their entitled compensation for the use of the IP. This robust architecture combines on-chain smart contracts, off-chain storage, and secure oracle services to provide comprehensive protection and management of IPRs.

3.7. Royalty payment mechanism

The content and data ownership are governed by mutually agreed-upon terms of use between the owner and the user. These agreements may include financial terms based on content usage and its nature. To address the financial aspects, a dual payment mechanism, both on-chain and off-chain [53] has been introduced through network-level smart contracts. On-chain payments involve cryptocurrencies, while off-chain payments can be made in various agreed upon fiat currencies facilitated by oracle services. As a result, payment methods are embedded within the smart contract itself. Once the smart contract is signed and conditions are met, access to a particular asset is granted. This approach offers the flexibility to process cross-border payments through various gateways that are already integrated with Blockchain-based networks, such as Wirex, Revolut, and Abra, among others. These gateways enable seamless transactions between different currencies and Blockchain networks, enhancing the efficiency and accessibility of financial transactions in the DRP ecosystem.

Table 2
Parameter and their respective abbreviations as used in the proposed scheme.

Parameter	Description
msgSender	Sender user class instance
ipHash	Hash of the subject IP
Status	Status of the user / IP (active/inactive)
ipAdmin	Admin of the IP
wallet	Payment wallet of the user/owner
allowtime	A lease time of an IP for access control based on an agreement
authRegister	The list of records containing authorized users with IP and bound time

3.8. Smart contracts based APIs

From a legal perspective, smart contracts are a vital component of many Blockchain systems. These contracts are programmed and self-executing that enable the inclusion of contractual terms and conditions. These are self-executing due to the terms of the agreement between parties, which are directly encoded into lines of code. The primary function of smart contracts is to automate the execution of agreements. When specific conditions outlined by the parties are met (e.g., timing of execution, a particular exchange rate, registration of an IP right, etc.), a smart contract fulfills an obligation, such as licensing an IP right or transferring property, money, or any other asset. These software programs effectively embody the parties' commitments. The generic interface facilitating communication between the DRP system and the user is achieved through smart contracts. Smart contracts serve as the foundation for enforcing legal rights, controlling access based on licensing, enhancing rewards, transferring assets, and enforcing transaction workflows. The primary smart contract integrated into the system is explained in the subsequent sections. Table 2 describes the particular terms used in the construction of the pseudo code of the smart contracts implemented for DRP.

3.8.1. IP registration smart contract

The initial step in engaging with the Tiered Blockchain-based DRP framework is to register digital rights on the network. The Algorithm 2 outlines the process for IP registration. The variable "msgSender" encapsulates the user currently logged into the system. This process requires both an IP and a pre-registered user. During the IP registration, the IP is recorded on the system, with the registering user established as the owner. This owner is then granted control over the IP for subsequent transfers or leases.

Algorithm 2: Pseudo-code of IP registration smart contract.

```
Input  : msgSender, ip
Output: ipHash
State:
address address_sender
MAP(address user, bool status) _user
MAP(address admin, address userHash) _ipAdmin
MAP(address owner, address ipHash, address userHash) _ipOwner
MAP(byte ipHash, byte userHash, timestamp allowTime)
  _authRegister
MAP(address ip, bool status) _ip
MAP(byte ipHash, address ip) _registeredRequest
MAP(byte wallet, address user) _userWallet
Function RegisterIp: onlyIpOwner, onlyipAdmin
Begin:
    _ip[msg.sender] ← True
    _iphash ← hash(ip)
    _registeredRequest[ipHash] ← msg.sender
    return ipHash
End
```

3.8.2. Royalty payment policy enforcer Smart contract

IPs are assets that can be leased and transferred, much like physical assets. To ensure a seamless payment and fee process, a smart contract-based payment method is utilized. This smart contract is responsible for executing the payment policy for IP when the DRP seeks royalty compensation for its usage. Algorithm 3 outlines the process for IP payment within a specific time frame. The $PaymentOfIpUsage$ function takes the $ipHash$ and sender data as inputs to access the conditions and verify the user's balance for the pending payment. Upon successful verification, the algorithm initiates the transfer of the payment from the sender's wallet to the owner's wallet. Additionally, it adds the access token to the $authRegister$, granting authorized access to the IP. This smart contract-based payment mechanism ensures a transparent and secure process for compensating IP owners for the usage of their intellectual properties.

Algorithm 3: Pseudo-code of royalty payment policy enforcer smart contract.

```
Input  : msgSender, ipHash
Output: paymentHash
Function PaymentOfIpUsage: onlyRegisteredUser
Begin:
    if userWallet.Balance > ipHash.AccessFee && ipHash.isActive then
        startSession()
        allowTime ← ipHash.owner.Wallet - sender.wallet -
          ip.Royaltyfee
        return (authRegister(ipHash, sender.hash, allowTime), ipHash)
    else
        return (false, ipHash)
End
```

3.8.3. IP access controller smart contract

In the context of the Blockchain-based DRP system, the access controller plays a crucial role as it acts as a mediator between the user and the IP owner. Unlike traditional Blockchain architectures, the tiered Blockchain mechanism employed in this system introduces a unique approach. A dedicated mechanism is established, which serves as a central processing hub, primarily relying on smart contracts for its operation. The key aspect of this system is the management of access to IP assets through smart contracts. Access to IP is not a onetime event but is rather governed by specific contract conditions, including a predefined time frame. When an authorized user seeks to access an IP, the system checks their authorization status. To provide a more detailed understanding of this process, Algorithm 4 has been developed. This algorithm outlines the step-by-step procedure for granting access to IP for users within the blockchain-based DRP system.

Algorithm 4: Pseudo-code of access control mechanism for accessing IP on blockchain.

```
Input  : msgSender, ipHash
Output: ipAccessSession
Function DigitalRightsProtectionAccessController:
  onlyRegisteredUser
Begin:
    if authRegister Contains (Sender.hash, ipHash, allowTime >
      timestamp) || sender.hash = ip.ownerHash then
        startSession()
        return ipAccessToken
    else
        disconnectSession()
End
```

3.8.4. Smart contract for digital rights ownership

To ensure the secure and transparent transfer of IP assets between different owners, the Blockchain-based DRP system employs a smart contract-based transfer mechanism. This mechanism is designed to facilitate the smooth transition of IP ownership from one party to another. Algorithm 5 outlines the specific steps and processes involved in this smart contract, which governs the transfer of IP ownership on the Blockchain.

Algorithm 5: Pseudo-code of IP transfer on blockchain.

```
Input  : newOwnerHash, ipHash
Output: ipOwnership, ownerHash
Function IpTransfer: onlyIpOwner
Begin:
    if PoO(sender.hash) then
        if newOwnerHash is Active then
            Ip.owner ← newOwnerHash
        else
            disconnectSession()
    else
        disconnectSession()
End
```

The utilization of smart contract-based interfaces within the system offers automation and transparency, significantly enhancing user trust in the process.

3.9. Use case analysis and proof-of-concepts

In the world of online journal publication, safeguarding IPRs is paramount. Proposed solution is the implementation of a tiered Blockchain system, which offers robust protection and transparency for both journal publishers and authors. In this scenario, when an author submits their research paper to an online journal, the tiered Blockchain system records the ownership and access rights of that IP. This ensures that the author's work remains protected and can be accessed only by authorized users, such as journal subscribers or academic institutions. Smart contracts, embedded in the Blockchain, govern the terms of access, usage, and even royalty payments. This means that authors can receive fair compensation for their work, and publishers can maintain control over their journal's content.

The use cases for verifying the developed system have been constructed in two highly suitable scenarios, and a thorough test case has been conducted to validate the proposed method. The operational behavior was closely observed during this dry run of the test cases. Detailed step-by-step use cases are described in the following paragraphs.

3.9.1. Use Case 1: digital artwork copyright protection

An artist creates a digital artwork and wishes to protect their copyright while also allowing limited digital reproductions for sale. Alice is a talented digital artist who creates unique and valuable digital artworks. She wants to protect her copyrights and ensure that her creations are not used without her permission. Alice decided to use the Tiered Blockchain IP Protection framework for digital artwork copyright protection. She wants to ensure that her artwork is not illegally copied or distributed without her permission. Implementation as per the proposed solution is being appended below:

Registration and timestamping. Alice registers her digital artwork on the Blockchain. The artwork is hashed, and this hash is timestamped and stored on the Blockchain, creating a unique, immutable digital certificate that proves her ownership and the creation date. This certificate is stored in the public ledger, making it immutable and tamper-proof.

Access control. Alice sets access control permissions using smart contracts. She allows viewing or using her artwork only to those who agree to her terms and conditions through the smart contract, including the number of authorized reproductions allowed and the royalty fee for each sale. When someone requests access, the smart contract verifies the agreement, ensuring compliance with the copyright.

Licensing and royalties. When a user wants to license Alice's artwork for a specific use, a new agreement in the form of a smart contract is created. This contract outlines the licensing terms, including duration and compensation. The user pays the licensing fee using cryptocurrency or a payment mode of choice using Oracle services, which is automatically recorded in the Blockchain. Smart contracts manage royalty payments to Alice each time her artwork is used or licensed.

Reproduction without license. Any attempt to reproduce or distribute the artwork without proper authorization triggers an alert within the Blockchain system and such an attempt is not considered legitimate. The Blockchain's transparency ensures that all transactions related to the artwork are traceable and verifiable.

3.9.2. Use Case 2: online research paper publication

Bob is a researcher who wants to publish his research papers online. He is concerned about maintaining the integrity and ownership of his work while making it accessible to the academic community. Bob decided to use the Tiered Blockchain IP Protection framework for online research paper publication. He also wants to have control over who can access and use his research work. Implementation of the use case in the proposed system is appended below:

Submission and timestamping. Bob submits his research paper to the Blockchain-based publication platform. The paper is hashed and timestamped, creating a verifiable record of the original content and publication date.

Access control and peer review. Bob sets access control permissions for his paper. He allows access to peers and reviewers for evaluation. Peer review comments and revisions are securely recorded on the Blockchain, providing transparency and accountability.

Copyright protection. Upon publication, Bob's research paper is protected by copyright on the Blockchain. Any unauthorized use or distribution is easily detectable, as the paper's hash is publicly available. Bob can specify licensing terms for researchers who wish to reuse his work, ensuring proper attribution and compliance with copyright.

Traceability. The Blockchain maintains a transparent history of revisions, comments, and access, ensuring the provenance of the research paper. This traceability enhances the credibility and trustworthiness of the published work. These use cases demonstrate how Blockchain technology can be leveraged to protect digital rights, ensure fair compensation, and provide creators with greater control over the distribution of their IP in the digital realm. The Blockchain's transparency, security, and automated smart contracts enhance the effectiveness of IP protection in the digital age.

It is important to acknowledge that Blockchain technology, despite its numerous advantages, also has inherent limitations that can impact the system's functionality. In the subsequent sections, the proposed method is analyzed against real-world use cases, and a detailed discussion of the limitations of the proposed method is provided.

3.10. Security evaluation of the network

Blockchain technology has the potential to establish trustworthy networks, particularly in the context of DRP. These trust networks comprise interconnected computers and legal regulations that define and govern data-related opportunities. In the realm of personal data, these networks enforce user permissions for individual data items and serve as legal contracts outlining actions in case of breaches. The proposed mechanism introduces an access control system within and between network tiers, ensuring secure and foolproof communication. To establish and operate a trusted network, policies for applications, service providers, data, and users are implemented. Access control lists, based on access rights, are enforced through a smart contract-based interface, guaranteeing compliance with access control policies. Unlike traditional systems prone to security vulnerabilities, Blockchain's inherent data storage mechanism and smart contract-based APIs offer enhanced security. This approach empowers IP owners with authority over digital rights and associated data, providing an effective means of security based on contract terms and conditions.

3.11. Limitations of the proposed method

The proposed method, built on the Ethereum blockchain, inherits several of its inherent limitations, such as issues with interoperability, scalability, and security. These limitations are compounded by the framework's reliance on off-chain services for ownership verification and storage, which can present integration challenges with dependent APIs. The method also depends on user-claimed ownership, which must be authenticated and verified by local authorities through Oracle services. However, the availability and authenticity of these Oracle services are beyond the framework's control, potentially undermining the reliability of the ownership verification process. Scalability remains a significant obstacle to the widespread adoption of this method due to the inherent complexity of blockchain technology, which is still evolving and not fully understood by many government enforcement bodies. This complexity can hinder the effective implementation and regulation of blockchain for IP protection. Furthermore, regulating blockchain technology for IP protection is a daunting task, requiring proactive and adaptable regulatory frameworks.

3.12. Technology integration and advantages

The integration of blockchain technology into IP protection systems offers transformative benefits, including decentralization, security, transparency, and immutability. By leveraging blockchain's decentralized architecture, intermediaries are eliminated, reducing costs and enhancing efficiency while increasing trust among participants. Furthermore, robust cryptographic mechanisms ensure data security and protection against unauthorized access, making it highly resilient to cyber threats. This creates a secure and trustworthy environment for IP protection, where creators and owners can confidently manage and monetize their digital assets.

The incorporation of smart contracts and a tiered approach further enhances the benefits of blockchain-based IP protection. Smart contracts automate processes through self-executing agreements, reducing manual errors and delays. A tiered approach combines the advantages of public, private, and consortium blockchain models, balancing transparency, privacy, and scalability. Additionally, the use of off-chain storage in combination with blockchain ensures efficient management of large datasets while maintaining on-chain metadata for auditability. Overall, blockchain integration fosters greater accountability, security, and operational efficiency across industries, making it a vital tool for modern digital ecosystems.

4. Results and discussions

Blockchain technology and its applications have experienced remarkable growth, evolving from relative obscurity to a prominent innovation buzzword. This transformative DLT addresses key challenges in IPRs protection. The immutability of Blockchain ensures indisputable ownership records, preventing ownership disputes. When combined with smart contracts, it adds an extra layer of security for licensing and royalty collection. Eliminating third party reliance enhances data security and trustworthiness.

4.1. Experimental setup

The proposed IP protection mechanism was successfully implemented through Ethereum smart contracts, employing the Solidity programming language. The experimentation environment was meticulously crafted within the Remix Ethereum IDE, a web-based platform offering robust testing and debugging capabilities for smart contracts integrated into a virtual Ethereum Blockchain environment. To facilitate this setup, Oracle VM VirtualBox hosted an Ubuntu 16.04 virtual machine, granting access via the web3 service. The host computer, equipped with an Intel Core i5 processor and 16 GB of RAM, ensured the efficient execution of the trials. Throughout these experiments, the focus centered on a singular smart contract. For a thorough and detailed evaluation, the experiment employed a network of 20 to 25 Ethereum nodes, each representing an individual user interacting with a shared smart contract. This setup allowed for a comprehensive assessment of the system's performance, scalability, and ability to handle multiple users simultaneously. A broad spectrum of key performance metrics was meticulously tracked throughout the testing process. These metrics included critical parameters such as transaction cost (in gas), execution cost (in gas), miner's fee, transaction time, and the total elapsed time for each transaction triggered by an IP-related action within the Blockchain network. By gathering this extensive data, the goal was to not only evaluate the technical performance of the proposed IP protection mechanism, but also to understand its real-world practicality and efficiency when deployed within the Ethereum Blockchain ecosystem. This holistic analysis provided a deep insight into how the system performs under different conditions and offered valuable information on its scalability, transaction efficiency, and overall effectiveness for secure IP management.

The experiments are conducted in lab simulated environment, several challenges were face in setting up environment, testing and collecting the telemetry. One of the major difficulties was the absence of a fully functional simulation environment. This limitation made it challenging to replicate real-world conditions and scale the test setup efficiently. As a result, testing conducted using the Ethereum test network, which lacks the real-world scenarios, especially for large-scale transactions. Additionally, testing the smart contract for financial transactions posed significant hurdles. Ensuring that the contract was secure and reliable for real-world financial transactions required extensive debugging and optimization to prevent potential vulnerabilities, such as reentrancy attacks or transaction failures.

Another challenge was the integration of Oracle services within a simulated environment, which was necessary to fetch external data for IP protection actions. The integration required careful calibration of the smart contract with external oracles, ensuring the data fetched from external sources was accurate and trustworthy. Furthermore, the implementation of tiered Blockchain architectures added complexity due to the need for efficient consensus mechanisms and handling side-chain interoperability.

4.2. Key performance metrics

The performance evaluation of the proposed innovative framework has undergone rigorous testing, with a focus on smart contract-based interfaces and their programmed functionalities. The various key performance metrics are recorded, and a thorough assessment is conducted to gauge the system's efficiency, these metrics include transaction costs in terms of gas, execution costs in terms of gas, Elapsed time (in microseconds), transactions per second (TPS), latency, and miner fees associated with each smart contract within the proposed system.

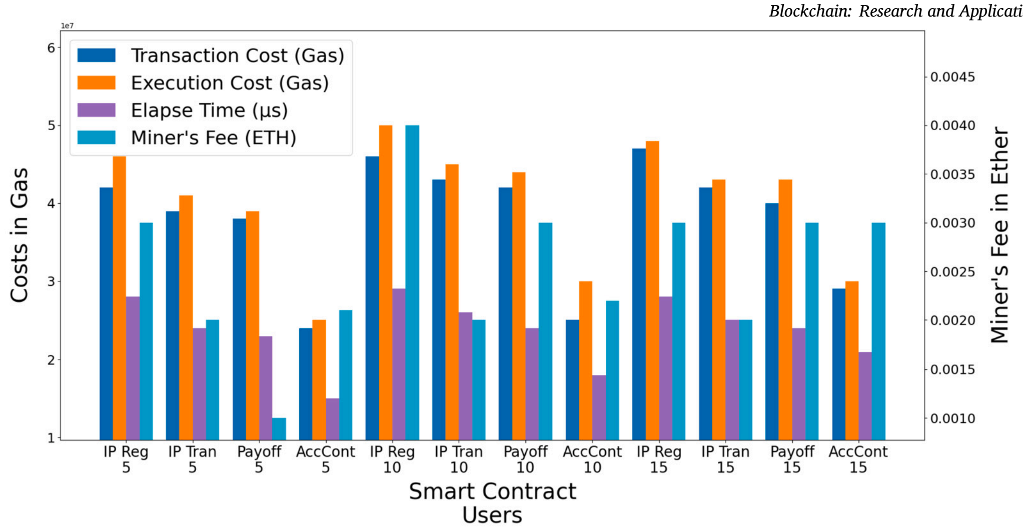


Fig. 5. Impact of user activity on system performance and cost.

4.3. Evaluation and performance results

Evaluation of the proposed DRP mechanism focuses on Blockchain platform metrics, including execution time, miner fees, and gas consumption, as well as security aspects, covering potential attacks and vulnerabilities. Fig. 5 presents the Blockchain metrics in a bar chart, revealing that nodes with higher user activity require more execution time, while simultaneously reducing mining fees and gas consumption. This phenomenon occurs due to the execution of transactions locally in private mode, which optimizes resource usage and minimizes external dependencies. As a result, the system efficiently handles transactions internally, leading to lower costs despite the increased execution time for nodes with high activity.

Blockchain offers a solution to store information about IP in its distributed ledger. By creating a time stamp record of when the work was uploaded and the details of the creator, Blockchain owns PoO of the creator. This technology helps the artists to benefit from their intellectual work and reduces the rate of piracy in the market. Intermediaries have always been a pain to the authors and owners of the IP by always taking a remarkable share of their work. Simply by serving as outsourcing platforms, intermediaries believe that they do the bulk of the work, so they deserve more. Smart contracts offered on Blockchain platforms eliminate the need for intermediaries. Smart contracts offer, as an artist, an avenue to dictate the terms of your work directly with your customers. This optimization of the process enables the user and the owner of an IP to remain secure and safe and benefit fully from their intellectual effort. Finally, Blockchain offers robust security and trust for data through its distributed ledgers that negate the presence of a single point of vulnerability and failure.

4.4. Security and performance analysis

Being a security critical system, analysis of the system concerning security controls is a key requirement. To attain the optimum level of security, a smart contract based access control mechanism is implemented. Smart contracts enforces the access mechanism to be set by the owner of the IP at the time of registration. To test the effectiveness of the access control mechanism, test procedures have been undertaken.

Understanding how Blockchain-based applications perform under various conditions is crucial. As shown in Fig. 6, our tests reveal that increasing the number of nodes in the Blockchain network leads to higher latency. This insight highlights the critical impact of network size on system performance. This phenomenon is often a result of the increased complexity in the network's communication and consensus processes as more nodes are involved. Additionally, as the concurrent load on the system increases, meaning a higher number of transactions are being processed simultaneously, the transaction confirmation time also tends to increase. This is due to the need for the system to handle and prioritize multiple transactions, potentially leading to delays in confirming each transaction. These increased factors highlight the importance of optimizing Blockchain networks to maintain acceptable performance levels, especially as network scale in size and transaction volume.

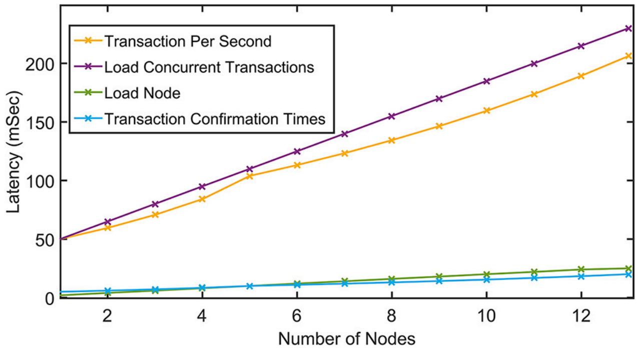


Fig. 6. Effect of number of nodes, transaction confirmation time, and concurrent load to TPS.

The IP system consists of three logical tiers. Regular and trustworthy nodes participate in maintaining the IPRs and managing user access levels within these tiers. A Blockchain-based framework operates via a client on all nodes. Since a separate node operates on the trusted exchange, in addition to the device client, it does not affect Blockchain efficiency. Therefore, it is necessary to independently evaluate the performance of the Blockchain and the trustworthy portal to analyze the performance of the entire solution.

4.4.1. Quantitative analysis of performance metrics

The performance evaluation of the proposed framework was conducted using Ganache, a local and virtual Ethereum Blockchain environment designed specifically for testing purposes. This evaluation primarily focused on two critical performance metrics: transaction throughput and latency. Latency refers to the number of transactions the Blockchain can validate per second, whereas throughput measures the time required to process a single transaction. These metrics were analyzed in relation to the frequency of transactions submitted to the Blockchain to assess how the system responds under varying workloads.

To ensure the accuracy and reliability of the findings, each experiment was repeated 100 times. The results, illustrated in Fig. 7, provide a detailed insight into the performance trends. Fig. 7 (A) highlights

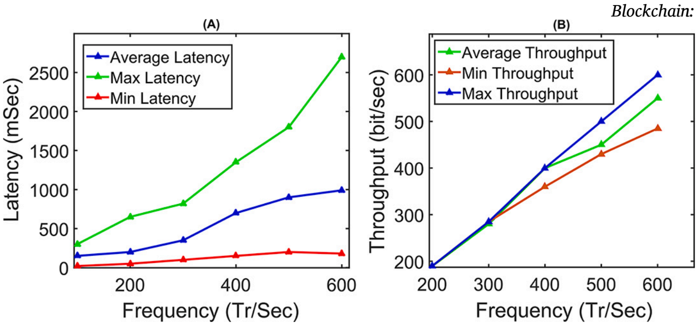


Fig. 7. (A) Latency observed with changes in transactions per second, (B) Throughput (verified transactions per second) with changes in transaction frequency.

the relationship between transaction frequency and the time required for transaction verification. As the transaction frequency increases, the time to verify each transaction also grows. Notably, when the transaction frequency reaches 300 TPS, the maximum latency experiences a sharp increase, indicating a significant performance bottleneck due to throughput lags.

In parallel, Fig. 7 (B) demonstrates the impact of transaction frequency on the number of transactions verified per second. The system operates optimally, maintaining ideal throughput levels, up to a transaction frequency of 300 TPS. Beyond this threshold, the average throughput begins to fall behind the transaction frequency, signaling that the system's capacity to handle additional load diminishes as the frequency continues to rise.

These results underscore the importance of managing transaction frequencies within the optimal range to ensure consistent performance. Additionally, they highlight the need for scalable solutions, such as Layer 2 protocols or sharding, to address performance limitations and accommodate higher transaction loads without compromising the efficiency of the Blockchain system.

Open source permissioned Blockchain storage has the vast ability to be configured at a large scale, but as the size of the network goes up, the latency of the network tends to increase. For this issue, an off-chain storage mechanism is the optimal way. To keep the trust level of the whole system up, off-chain storage is maintained using a P2P approach. In theory, third parties could use the Blockchain to see the complete chain of ownership of a work, including any licenses, sub-licenses, and assignments. As Blockchain can maintain data integrity, it has broad appeal for multiple kinds of IP protection. Using Blockchain technology to establish ownership rights, reduce counterfeiting, license through smart contracts, and IP might give enhanced efficiency and authenticity. In-depth performance analysis is evident that the proposed method outperformed the conventional Ethereum network. Fig. 8 reveals a crucial comparison of how our proposed method stacks up against Ethereum's public network in terms of cost and latency per transaction, as transaction speed increases. The results show that while both methods experience higher costs and latency as TPS rise, our proposed method consistently outperforms Ethereum, with lower costs and latency across the entire range of TPS tests.

The PoO consensus algorithm is evaluated using a use case of digital fingerprints, which securely prove ownership of creative works. PoO's revolutionary mechanism ensures only legitimate owners can validate transactions and create blocks, building trust and safeguarding IPR. This cutting-edge technology provides owners with assurance. In contrast, PoS selects validators based on their stake in the P2P community, making validation more efficient and less vulnerable to centralization. However, for IP protection scenarios, PoS relies on ownership verification to validate digital asset ownership on the DLT. In the proposed method, PoO is being used on top of the PoS algorithm, being the default consensus algorithm of the Ethereum Blockchain. Therefore, the performance of PoO does not affect due to PoS algorithms being used in the Ethereum Blockchain. Table 3 compares the PoO and PoS algorithms, highlighting their differences.

PoO and PoS are two consensus mechanisms with distinct utilization and performance characteristics. PoO excels in security and transaction throughput, processing 200-300 TPS. It boasts low energy consumption, moderate scalability, and high interoperability, making it suitable for specialized IP transactions. PoO prioritizes security and performance, PoS focuses on scalability and efficiency, making it suitable for different use cases in the blockchain landscape. Fig. 8 presents the analysis of the latency and cost incurred on various TPS of the proposed method and the conventional Ethereum platform metrics.

4.5. *Comparative analysis*

The proposed tiered approach aims to enhance security, trustworthiness, and cost efficiency in DRM. The Tiered Blockchain Framework leverages a multi-layer blockchain architecture to address various aspects of DRP. The proposed method enhances security through a layered architecture. The public blockchain ensures data immutability and transparency, while the consortium and private blockchains manage data with controlled access, reducing vulnerability to attacks. This analysis compares this framework with the state-of-the-art methods currently discussed in the literature. Table 4 comprises of comparative analysis of the proposed method with the state-of-the-art IP protection method [46] proposed in the literature.

Table 4 compares the performance metrics of the proposed tiered Blockchain-based IP protection method with an existing method. The proposed method demonstrates a substantial improvement across various metrics. It achieves a higher transaction throughput of 300 TPS, compared to 150 TPS, and reduces transaction latency from 35 seconds to just 0.2 seconds. Additionally, the cost per transaction is notably lower, at 0.013 Gwei versus 0.26 Gwei, at 300 TPS. In terms of data integrity and immutability, the proposed method enhances security through multi-layer SHA-256 encryption and tokenization. Scalability is significantly improved with a multi-layer architecture, in contrast to the current method's reliance on sharding. The proposed approach excels in interoperability, offering extensive cross-chain capabilities through private oracle services, while the existing method has limited cross-chain functionality. User adoption rates are also higher for the proposed method, indicating greater user acceptance. Furthermore, it demonstrates superior compliance with a broader range of IP and digital rights laws. Lastly, throughput efficiency is markedly higher, with 98% successful transactions compared to just 85% in the existing method.

Tiered Blockchain frameworks demonstrate significant potential for advanced IP protection, surpassing the limitations of traditional single-layer solutions. The proposed flexible architecture, enhanced security, and high interoperability enable efficient and reliable management of IP in a decentralized environment. This multi-layered approach enhances security, trustworthiness, and cost efficiency compared to state-of-the-art single-layer methods. While traditional public and consortium Blockchains each have their advantages, the tiered framework effectively balances these benefits, providing a scalable, flexible, and interoperable system that addresses the complex needs of DRM more effectively.

Table 3
Performance comparison of the proposed and the inherit consensus method of Ethereum public Blockchain.

Metric	Proof of ownership	Proof of stake
Throughput (TPS)	High, 200–300 TPS	Low, 100–150 TPS
Latency	High, due to ownership re-verification is carried out (0.2–0.5 seconds)	Moderate, as validators are pre-selected (0.02–0.05 seconds)
Cost per transaction	Moderate, dependent on network conditions and gas prices	Moderate, dependent on network conditions and gas prices
Energy consumption	Low, no extensive computational power needed	Very low, significantly more efficient than PoW
Security	Very high, ensure only legitimate owners can validate	High, economic incentives deter malicious behavior
Scalability	Moderate, suitable for specialized IP transactions	High, designed to handle a wide range of transactions.
Interoperability	High, can integrate with existing IP systems	Moderate to high, depending on the Blockchain's ecosystem.
Compliance with legal standards	Very high, tailored for IP and digital rights compliance	Variable, general compliance depends on the application.

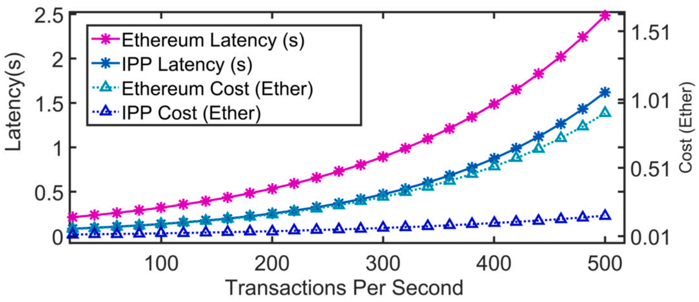


Fig. 8. Performance analysis of the proposed method with conventional Blockchain based application on cost and latency parameters.

Table 4
Comparative analysis of the proposed method with state-of-the-art method in the literature.

Performance metric	Ref. [46]	Proposed method
Throughput (TPS)	150 TPS	300 TPS
Latency	35 seconds	0.2 seconds
Cost per transaction (Gas)	0.26 Gwei	0.013 Gwei
Data integrity and immutability	High, SHA-256 encryption	Very high, multi-layer SHA-256 and tokenization.
Scalability	High, supports sharding	Very high, multi-layer architecture
Interoperability	Medium, limited cross-chain capabilities	High, extensive cross-chain capabilities using private oracle services.
User adoption rate	Medium adoption among targeted users	High adoption among targeted users.
Compliance with legal standards	Medium, adheres to basic IP laws	High, adheres to extensive IP and digital rights laws.
Efficiency	85% successful transactions	98% successful transactions.

In conclusion, this research highlights the urgent need for innovative solutions to IPRs in the digital age. With the value of creative and intellectual works becoming increasingly vulnerable, existing systems are struggling to keep up with the rapid pace of technological evolution. The tiered Blockchain based DRP framework offers a robust and forward-thinking approach to these challenges by integrating advanced technology, comprehensive legal frameworks, and cryptographic security to provide a secure and transparent IP management system. This framework mitigates the risks of counterfeiting and unauthorized use while simplifying the licensing process, ensuring a more efficient and reliable system for managing IPRs. While navigating the ever-evolving landscape of digital innovation, the tiered Blockchain IP protection framework stands as a guiding light toward a future where IP is safeguarded, valued, and shared in ways that benefit creators, consumers, and society at large. Addressing critical issues such as data integrity, interoperability, and scalability, it enhances the traceability and accountability of IP transactions through the Blockchain's immutable ledger and decentralized nature. This not only reinforces legal compliance and reduces disputes but also fosters an environment where innovation can thrive. By embracing this framework, the full potential of IP, driving creativity, innovation, and progress for generations, can be unlocked. This framework ensures the benefits of digital advancements are widely and fairly distributed.

5. Conclusions

Managing and safeguarding IP is a multifaceted endeavor, shaped not only by national interests but also by market demands, commercial considerations, and the evolving landscape of DRM. This research introduces an innovative paradigm for IP protection, leveraging Blockchain technology. The tiered Blockchain-based framework ensures that the right content is delivered to the right users in a platform-independent manner. It offers cost-effective maintenance, heightened transparency, reduced administrative burden, and resistance to fraud. Within this framework, open-source permission-based Blockchain technology is employed, with smart contracts serving as the CAI for content retrieval and storage. IP access and utilization are governed by smart contracts that encapsulate the agreed-upon terms and conditions as stipulated by the owner. These smart contracts serve as the mechanism to ensure strict compliance with the specified terms and conditions, thereby providing a secure and automated way to manage and safeguard IPRs. To accommodate large digital content, an off-chain storage mechanism using Oracle services is proposed, ensuring efficiency. The Blockchain storage scheme incorporates robust authentication, privacy protection, and a multi-signature-based PoO mechanism, guaranteeing content distribution with the owner's approval only. Traceability of access requests, both legal and illegal, is recorded on the Blockchain for enhanced trustworthiness. A comprehensive performance evaluation, based on diverse use cases, validates the Blockchain-based digital content service's reliability, security, efficiency, and tamper resistance. The analysis reveals substantial improvements in process optimization, technology adoption, enhanced efficiency, and cost reduction. This framework, aligned with the vision of delivering tailored content securely and efficiently, holds great promise for advancing IP and trade as Blockchain technology evolves.

CRediT authorship contribution statement

Muhammad Hanif: Writing – original draft, Visualization, Validation, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Ehsan Ullah Munir:** Writing – review & editing, Validation, Supervision. **Muhammad Maaz Rehan:** Supervision, Methodology, Investigation. **Saima Gulzar Ahmad:** Writing – original draft, Methodology, Formal analysis. **Imtiaz Khan:** Writing – review & editing, Validation, Supervision. **Rossitza Setchi:** Writing – review & editing, Visualization, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] E. Bakaouka, Horizontal Licensing in Vertically Related Markets, Springer Science and Business Media Deutschland GmbH, 2024, pp. 57–94, https://doi.org/10.1007/S13209-023-00294-Y/TABLES/3.

[2] W. Sha, T. Luo, J. Leng, et al., Heterogeneous multi-blockchain model-based intellectual property protection in social manufacturing paradigm, in: 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, Hangzhou, China, 2022, pp. 891–896, https://doi.org/10.1109/CSCWD54268.2022.9776286.

[3] S.M.H. Bamakan, S.B. Far, Distributed and trustworthy digital twin platform based on blockchain and web3 technologies, Cyber Secur. Appl. 3 (2025) 100064, https://doi.org/10.1016/J.CSA.2024.100064.

[4] D.L. Cogburn, T.A. Ochieng, H.M. Wong, Towards an understanding of global 'private ordering' in ICANN: text mining 23 years of uniform domain-name dispute-resolution policy (UDRP) decisions, J. Cyber Policy 8 (2023) 186–217, https://doi.org/10.1080/23738871.2023.2286271.

[5] S. Feng, C.P. Sik, Multifaceted challenges of jurisdictional divergence in cross-border intellectual property violations, Int. J. Crim. Justice Sci. 19 (2024) 20–40, https://doi.org/10.5281/zenodo.19102/IJCJS.

[6] A. Leporati, L. Rovida, Looking for stability in proof-of-stake based consensus mechanisms, Blockchain Res. Appl. 5 (2024) 100222, https://doi.org/10.1016/J.BCRA.2024.100222.

[7] N. Kabra, P. Bhattacharya, S. Tanwar, et al., Mudrachain: blockchain-based framework for automated cheque clearance in financial institutions, Future Gener. Comput. Syst. (2020), https://doi.org/10.1016/j.future.2019.08.035.

[8] J. Hu, P. Zhu, Y. Qi, et al., A patent registration and trading system based on blockchain, Expert Syst. Appl. 201 (2022), https://doi.org/10.1016/j.eswa.2022.117094.

[9] H. Song, N. Zhu, R. Xue, et al., Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection, Inf. Process. Manag. 58 (3) (2021), https://doi.org/10.1016/j.ipm.2021.102507.

[10] P.H. Trung, D.M. Hieu, T.D. Khoa, et al., Evaluating blockchain platforms for efficient intellectual property rights management: a cross-chain analysis, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 15424, 2025, pp. 33–48, https://doi.org/10.1007/978-3-031-77069-2_3, https://link.springer.com/chapter/10.1007/978-3-031-77069-2_3.

[11] E. Rosati, The localization of IP infringements in the online environment: from web 2.0 to web 3.0 and the metaverse, J. Intellect. Prop. Law Pract. 18 (2023) 720–742, https://doi.org/10.1093/JIPLP/JPAD077.

[12] R.F. Ciriello, A.C.G. Torbensen, M.R.P. Hansen, et al., Blockchain-based digital rights management systems: design principles for the music industry, Electron. Markets 33 (2023), https://doi.org/10.1007/S12525-023-00628-5.

[13] I. Makhdoom, M. Abolhasan, J. Lipman, et al., Privysec: a secure and privacy-compliant distributed framework for personal data sharing in IoT ecosystems, Blockchain Res. Appl. 5 (2024) 100220, https://doi.org/10.1016/J.BCRA.2024.100220.

[14] Z. Zheng, S. Xie, H. Dai, et al., Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375, https://doi.org/10.1504/IJWGS.2018.095647.

[15] S. Bonnet, F. Teuteberg, Impact of blockchain and distributed ledger technology for the management of the intellectual property life cycle: a multiple case study analysis, Comput. Ind. 144 (2023) 103789, https://doi.org/10.1016/J.COMPIND.2022.103789.

[16] H. Baniata, A. Kertesz, Partial pre-image attack on proof-of-work based blockchains, Blockchain Res. Appl. 5 (2024) 100194, https://doi.org/10.1016/J.BCRA.2024.100194.

[17] A. Reyna, C. Martín, J. Chen, et al., On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190, https://doi.org/10.1016/j.future.2018.05.046.

[18] W. I. P. O. (WIPO), World Intellectual Property Report 2024: making innovation policy work for development, World Intellectual Property Organization, Geneva, Switzerland, https://www.wipo.int/web-publications/world-intellectual-property-report-2024/, 2024.

[19] G. Paik, G. Chhatani, A. Sharma, et al., Blockchain and its applications in intellectual property rights management, in: Proceedings of the International Conference on Computational Intelligence and Sustainable Engineering (CISES), IEEE, Greater Noida, India, 2023, pp. 386–391, https://doi.org/10.1109/CISES58720.2023.10183512.

[20] L. Xiao, W. Huang, Y. Xie, et al., A blockchain-based traceable IP copyright protection algorithm, IEEE Access 8 (2020) 49532–49542, https://doi.org/10.1109/ACCESS.2020.2969990.

[21] S. Bhadauria, P. Kumar, T. Mohanty, Intellectual property protection using blockchain and digital watermarking, Int. Symp. Adv. Networks Telecommun. Syst. ANTS December (2021) 1–6, https://doi.org/10.1109/ANTS52808.2021.9936909.

[22] L. Liu, B. Sun, Intellectual property protection method based on block chain technology, in: M. Atiquzzaman, N.Y. Yen, Z. Xu (Eds.), Proceedings of the 4th International Conference on Big Data Analytics for Cyber-Physical System in Smart City - Volume 2, Springer Nature Singapore, Singapore, 2023, pp. 531–538, https://doi.org/10.1007/978-981-99-1157-8_64.

[23] C. Zhuang, Q. Dai, Y. Zhang, BCPPT: a blockchain-based privacy-preserving and traceability identity management scheme for intellectual property, Peer-to-Peer Netw. Appl. 15 (2022) 724–738, https://doi.org/10.1007/S12083-021-01277-1/TABLES/3, https://link.springer.com/article/10.1007/s12083-021-01277-1.

[24] P. Kudumakis, T. Wilmering, M. Sandler, et al., The challenge: from MPEG intellectual property rights ontologies to smart contracts and blockchains [standards in a nutshell], IEEE Signal Process. Mag. 37 (2) (2020) 89–95, https://doi.org/10.1109/MSP.2019.2955207.

[25] A. Guru, B.K. Mohanta, H. Mohapatra, et al., A survey on consensus protocols and attacks on blockchain technology, Appl. Sci. 2023 (13) (2023) 2604, https://doi.org/10.3390/APP13042604.

[26] R. S, S. Vishva E, L. Dua, et al., Chapter 7 - Blockchain for digital rights management, in: S.H. Islam, A.K. Pal, D. Samanta, S. Bhattacharyya (Eds.), Blockchain Technology for Emerging Applications, Hybrid Computational Intelligence for Pattern Analysis, Academic Press, 2022, pp. 177–205, https://doi.org/10.1016/B978-0-323-90193-2.00010-7.

[27] P. Gupta, S. Wadhwa, S. Chauhan, Crossroad of intellectual property rights of technology innovators and human rights: a systematic literature review, Dig. Policy Reg. Govern. 25 (2023) 236–249, https://doi.org/10.1108/DPRG-08-2022-0099/FULL/XML.

[28] C. Dong, Color image encryption using one-time keys and coupled chaotic systems, Signal Process. Image Commun. 29 (5) (2014) 628–640, https://doi.org/10.1016/j.image.2013.09.006.

[29] M. Pustišek, A. Kos, Approaches to front-end IoT application development for the Ethereum blockchain, Proc. Comput. Sci. 129 (2018) 410–419, https://doi.org/10.1016/j.procs.2018.03.017.

[30] Q. Zhuang, Y. Liu, L. Chen, et al., Proof of reputation: a reputation-based consensus protocol for blockchain based systems, in: ACM International Conference Proceeding Series, 2019, pp. 131–138, https://doi.org/10.1145/3343147.3343169.

[31] M. Muzammal, Q. Qu, B. Nasrulin, Renovating blockchain with distributed databases: an open source system, Future Gener. Comput. Syst. 90 (2019) 105–117, https://doi.org/10.1016/J.FUTURE.2018.07.042.

[32] R. Dalbouchi, A. Zitouni, A software/hardware secure watermarking scheme for Internet of Things applications, Multimed. Tools Appl. (2023) 1–20, https://doi.org/10.1007/S11042-023-16533-0/TABLES/9.

[33] J. Shen, Blockchain technology and its applications in digital content copyright protection, in: C. Yuan, X. Li, J. Kent (Eds.), Proceedings of the 4th International

Conference on Economic Management and Green Development, Springer Singapore, Singapore, 2021, pp. 18–25, https://doi.org/10.1007/978-981-16-5359-9_3.

[34] H. Zhang, L. Lin, G. Zhang, et al., ATIPM: a blockchain-based anonymous and traceable intellectual property management scheme, in: Proceedings of the 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE, Rio de Janeiro, Brazil, 2023, pp. 1080–1085, https://doi.org/10.1109/CSCWD57460.2023.10152748.

[35] G. Sharma, S. Gupta, S. Dhall, et al., Publicly verifiable watermarking scheme for intellectual property protection using quantum chaos and bit plane complexity slicing, Multimed. Tools Appl. 77 (24) (2018) 31737–31762, https://doi.org/10.1007/s11042-018-6226-8.

[36] X. Ren, F. Lin, Z. Chen, et al., BIA: a blockchain-based identity authorization mechanism, in: Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking (MSN), IEEE, Tokyo, Japan, 2020, pp. 98–105, https://doi.org/10.1109/MSN50589.2020.00031.

[37] I. Olubiyi, U. Emerole, A. Adetula, Contemporary challenges to intellectual property rights in developing countries: Looking beyond the laws (Nigeria as a case study), Int. Rev. Ind. Prop. Compet. Law 53 (1) (2022) 5–30, https://doi.org/10.1007/S40319-021-01138-7.

[38] J. Fei, Z. Xia, B. Tondi, et al., Supervised GAN watermarking for intellectual property protection, in: 2022 IEEE International Workshop on Information Forensics and Security (WIFS), vol. 1, IEEE, Shanghai, China, 2022, pp. 1–6, https://doi.org/10.1109/WIFS55849.2022.9975409.

[39] H. Kim, J. Park, M. Bennis, et al., Blockchained on-device federated learning, IEEE Commun. Lett. 24 (6) (2019) 1279–1283, https://doi.org/10.1109/lcomm.2019.2921755.

[40] J. Lach, W. Mangione-Smith, M. Potkonjak, Fingerprinting techniques for field-programmable gate array intellectual property protection, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 20 (10) (2001) 1253–1261, https://doi.org/10.1109/43.952741.

[41] G. Qu, Publicly detectable watermarking for intellectual property authentication in VLSI design, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 21 (11) (2002) 1363–1368, https://doi.org/10.1109/TCAD.2002.804205.

[42] S.P. Mohanty, R. Kumara C., S. Nayak, FPGA-based implementation of an invisible-robust image watermarking encoder, in: G. Das, V.P. Gulati (Eds.), Intelligent Information Technology, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 344–353, https://doi.org/10.1007/978-3-540-30561-3_36.

[43] C.-C. Chang, Y.-S. Hu, T.-C. Lu, A watermarking-based image ownership and tampering authentication scheme, Pattern Recognit. Lett. 27 (5) (2006) 439–446, https://doi.org/10.1016/j.patrec.2005.09.006.

[44] R.C.-W. Phan, Tampering with a watermarking-based image authentication scheme, Pattern Recognit. 41 (11) (2008) 3493–3496, https://doi.org/10.1016/j.patcog.2008.05.009.

[45] D. Saha, S. Sur-Kolay, Secure public verification of IP marks in FPGA design through a zero-knowledge protocol, IEEE Trans. Very Large Scale Integr. Syst. 20 (10) (2012) 1749–1757, https://doi.org/10.1109/TVLSI.2011.2162347.

[46] A. Garba, A.D. Dwivedi, M. Kamal, et al., A digital rights management system based on a scalable blockchain, Peer-to-Peer Netw. Appl. 14 (2021) 2665–2680, https://doi.org/10.1007/s12083-020-01023-z.

[47] R. Hamza, M. Dao, S. Ito, et al., Towards intellectual property rights protection in big data, in: ICDAR 2022 - Proceedings of the 3rd ACM Workshop on Intelligent Cross-Data Analysis and Retrieval, 2022, pp. 50–57, https://doi.org/10.1145/3512731.3534211.

[48] Z. Ma, M. Jiang, H. Gao, et al., Blockchain for digital rights management, Future Gener. Comput. Syst. 89 (2018) 746–764, https://doi.org/10.1016/J.FUTURE.2018.07.029.

[49] Y. Ma, Y. Sun, Y. Lei, et al., A survey of blockchain technology on security, privacy, and trust in crowdsourcing services, World Wide Web 23 (2020) 393–419, https://doi.org/10.1007/s11280-019-00735-4.

[50] M. Ghaleb, F. Azzedin, Towards scalable and efficient architecture for modeling trust in IoT environments, Sensors 2021 21 (2021) 2986, https://doi.org/10.3390/S21092986.

[51] M.T. Nakao, A numerical approach to the proof of existence of solutions for elliptic problems, Jpn. J. Appl. Math. 5 (2) (1988) 313–332, https://doi.org/10.1007/BF03167877.

[52] K. Karantias, A. Kiayias, D. Zindros, Proof-of-burn, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer, 2020, pp. 523–540, https://doi.org/10.1007/978-3-030-51280-4_28.

[53] D. Mancino, A. Leporati, M. Viviani, et al., A role and reward analysis in off-chain mechanisms for executing mev strategies in Ethereum proof-of-stake, Distrib. Ledger Technol. Res. Pract. 4 (3) (2024) 1–23, https://doi.org/10.1145/3672405.