Review

Not peer-reviewed version

Employing Blockchain, NFTs, and Digital Certificates for Unparalleled Authenticity and Data Protection of Source Code

Leonardo Juan Ramirez Lopez * and Genesis Gabriela Morillo Ledezma

Posted Date: 27 February 2025

doi: 10.20944/preprints202502.1048.v2

Keywords: Blockchain; Data protection; Digital certificates; Non-Fungible Tokens (NFTs); Source Code

Review

Employing Blockchain, NFTs, and Digital Certificates for Unparalleled Authenticity and Data Protection in Source Code

Leonardo Juan Ramirez Lopez * and Genesis Gabriela Morillo Ledezma

Osiris & Bioaxis Research Group, Engineering Faculty, Universidad El Bosque, Bogota 111321, Colombia

* Correspondence: ljramirezl@unbosque.edu.co; Tel.: +57-3114905014

Abstract: In higher education, especially in programming-intensive fields like computer science, safeguarding students' source code is crucial to prevent theft that could impact learning and future careers. Traditional storage solutions like Google Drive are vulnerable to hacking and alterations, highlighting the need for stronger protection. This work explores digital technologies that enhance source code security, with a focus on Blockchain and NFTs. Due to Blockchain's decentralized and immutable nature, NFTs can be used to control code ownership, improving security, traceability, and preventing unauthorized access. This approach effectively addresses existing gaps in protecting academic intellectual property. However, as Bennett et al. highlight, while these technologies have significant potential, challenges remain in large-scale implementation and user acceptance. Despite these hurdles, integrating Blockchain and NFTs presents a promising opportunity to enhance academic integrity. A successful adoption in educational settings may require a more inclusive and innovative strategy.

Keywords: blockchain; data protection; digital certificates; Non-Fungible Tokens (NFTs); source code

1. Introduction

In an era marked by rapid technological advancements and increasing concerns over intellectual property rights, protecting digital assets has become a critical challenge. For students in Computer Science and Software Engineering (CSSE), ensuring the integrity and ownership of their source code is essential, as it represents not only their academic effort but also potential intellectual property. Despite existing submission protocols and security measures, issues related to originality, authorship, and unauthorized use of student-developed code remain prevalent.

This paper explores how Blockchain and Non-Fungible Tokens (NFTs) can enhance the security and traceability of student projects. Specifically, it examines the submission and evaluation processes in universities, with a particular focus on the Massachusetts Institute of Technology (MIT). Additionally, it discusses the importance of source code protection through licensing and copyright regulations across different regions, including Europe, Asia, and Colombia.

Furthermore, the study delves into the role of digital assets, Blockchain, and NFTs in safeguarding intellectual property within academic environments. These emerging technologies provide innovative solutions to long-standing concerns regarding ownership verification and tamper-proof record-keeping. By integrating these decentralized technologies, universities can strengthen the security of student projects while fostering a more transparent and reliable academic ecosystem.

The implementation of blockchain, NFTs, and digital certificates for securing intellectual property, particularly academic source code, presents several advantages and disadvantages:

Advantages:

- Immutability and Security: Blockchain ensures that once a transaction is recorded, it cannot be altered, providing strong protection against plagiarism or unauthorized modifications.
- Decentralization: Eliminates the reliance on a single authority, reducing the risk of data manipulation or institutional biases in ownership claims.
- Transparent Ownership Records: NFTs allow for the creation of unique digital signatures, providing indisputable proof of authorship and ownership.
- Automated Smart Contracts: These enable streamlined licensing agreements and automatic enforcement of intellectual property rights without intermediaries.

Disadvantages:

- High Energy Consumption: Many blockchain networks require substantial computational power, raising concerns about sustainability and efficiency.
- Regulatory Uncertainty: The legal framework for blockchain-based intellectual property protection is still evolving, with varying acceptance across jurisdictions.
- Complexity and Cost: Implementing blockchain and NFTs require technical expertise and may involve high transaction fees, making it less accessible for smaller institutions or individual students.
- Irreversible Transactions: While immutability is a strength, errors in ownership attribution or smart contracts can be difficult to correct.

By analyzing these advantages and disadvantages, it becomes evident that while blockchain and NFTs offer unprecedented security and authenticity, their adoption in academia requires careful consideration of legal and technical factors.

a. Code submission processes:

This is more so in the systems and computer engineering career whereby the final exercises like software and system development are perceived as last milestones in the training process [1]. In such projects, a student will post his/her source code, and the posted material will be analyzed based on both how well it works as well as other program guidelines. In most universities, code is shared in other internal digital platforms such as one drive and Google drive. They include replication such as in the Git repositories or learning management systems (LMS) such as Moodle, that offer security and guarantee of the integrity of the content. Still, the issue of source code protection remains the most critical one and concerns possible manipulation or theft of work before final evaluation [2]. It should be considered that this aspect is critical, since its change poses a risk of compromising academic integrity of the project and a student, as well as the reputation of the academic institution [3].

b. Thesaurus in Systems Engineering:

Massachusetts Institute of Technology (MIT) has created fine grained and specific thesauri that are aimed at improving the reusability of technical terms in systems engineering. For example, one of the major resources of MIT is the Thesaurus of Engineering Terminology (TET) containing a defined and extensively approved set of Global Standard in systems engineering. Dialogues created by this thesaurus are used in the software development tools, thus ensures conformity and compliance in the language used in projects [4].

Moreover, Stanford and Harvard, and other universities as well, have adopted and have further developed their own technical thesauri. These thesauri contain not only the words and phrases potentially used when searching for information, but also the precise definitions of the concepts being searched, and their interrelations, which makes search results understandable for researchers and students who employ commonly accepted terms and definitions. Such actions help in improving the quality of communication within such a project as well as safeguarding the intellectual property of students [5].

All in all, regarding the thesauri and policies used in the institution, these are meant for a fair and transparent evaluation process, as well as correct attribution of authorship and retention of academic knowledge [6].

c. Definition of Source Code:

Source code is defined as a sequential collection of coded statements written in a programming language which is intelligible to the programmer and is in a form that can be compiled/ interpreted and run on the machine [7]. To MIT, source code is important in any software project as it embodies the thinking and the answers that a programmer uses in achieving solutions. Thus, it becomes critical to protect this fundamental foundation for the creation of all the applications and systems and to preserve the author's intellectual integrity [8].

d. Definition and Copyright of Source Code

Source code is a structured collection of coded statements written in a programming language that can be compiled or interpreted to execute on a machine [9]. At MIT, source code is considered a fundamental component of software projects, encapsulating the problem-solving approaches and intellectual contributions of the developer. Therefore, protecting source code is essential to preserving academic integrity and the intellectual rights of its authors [10].

Legal protections for source code vary significantly across jurisdictions. In Europe, the Directive 2009/24/EC classifies source code as a literary work, granting authors ex-clusive rights to use and distribute their code. Similarly, Japan and South Korea have adopted legal frameworks to safeguard software copyrights, albeit with regional differences in implementation [11]. In Colombia, the National Copyright Office recognizes source code as a form of software work, granting its author economic and moral rights [12]. To combat piracy and unauthorized use, various measures have been implemented, including open licenses that specify usage conditions and digital protection technologies that restrict unauthorized access [13].

e. Digital Assets and Blockchain for Academic Protection

Digital assets encompass a broad range of resources in digital form, including documents, multimedia files, cryptocurrencies, and NFTs [14]. Protecting these assets is critical in an environment where data can be easily stolen or manipulated. Security measures such as encryption, private keys, and multi-factor authentication are commonly used to safeguard digital resources [15].

Blockchain technology has emerged as a robust solution for ensuring the integrity of digital assets by providing a decentralized and tamper-proof ledger [16]. Unlike traditional databases, blockchain operates through distributed ledger technology (DLT), which disperses records across multiple nodes, eliminating a single point of control and reducing the risk of unauthorized alterations [17]. The cryptographic nature of blockchain ensures that each record remains immutable and secure, making it a viable option for intellectual property management in academia [18].

f. NFTs as a Mechanism for Intellectual Property Protection

Non-fungible tokens (NFTs) are unique digital assets stored on a blockchain, capable of representing a variety of intellectual properties, including academic source code [19]. By tokenizing student projects as NFTs, institutions can generate a unique and verifiable digital signature that certifies the authenticity and ownership of each work [20]. This approach not only enhances security but also provides an immutable record of authorship. Additionally, the implementation of multi-chain blockchain technology could improve interoperability between different blockchain networks, offering more flexible and scalable solutions for managing NFTs in academic settings [21].

1.1. Discussion of Challenges and Limitations in the Study

While leveraging the tamper-proof provenance offered by Blockchain and NFTs for student source code verification holds immense promise, this study acknowledges several hurdles that must be addressed for widespread adoption [23]. These challenges include technical integration, scalability, performance, user adoption, security concerns, and regulatory compliance, all of which impact the feasibility of large-scale implementation in academic settings.

- **Technical Integration:** The integration of Blockchain-based solutions with existing university IT infrastructures presents a significant challenge. Academic institutions rely on legacy systems that may not be fully compatible with newer blockchain-based applications, requiring a migration strategy that minimizes workflow disruptions. Furthermore, interoperability between different blockchain protocols and existing digital credentialing platforms must be ensured to facilitate seamless adoption. Recent studies suggest that hybrid architectures combining on-chain and off-chain storage can help address compatibility issues and improve performance in academic environments [24].

- **Scalability and Performance:** Blockchain networks face significant scalability limitations due to increasing transaction loads, particularly in environments with high volumes of student submissions and academic records. As the number of users and projects grows, transaction throughput and processing times may become bottlenecks, leading to inefficiencies [25]. Several approaches, such as sharing, off-chain computation (e.g., Layer 2 solutions), and directed acyclic graphs (DAGs), have been proposed to enhance blockchain scalability in educational applications. Emerging technologies like rollups and sidechains also offer potential improvements by offloading computational tasks while maintaining security guarantees.
- As the number of users and projects increases, the scalability of the blockchain network is affected. Latency and processing issues can compromise system efficiency. Solutions such as sharding and off-chain computation have been proposed to mitigate these issues. Recent studies have shown that optimizing resource allocation in IoT networks through deep reinforcement learning techniques, such as the Distributed DDPG-based resource allocation approach, can significantly reduce latency and improve overall system performance [26]. This approach has been validated in mobile wireless-powered IoT environments, achieving minimization of information update times and optimizing resource efficiency in decentralized networks.
- **Security and Privacy Concerns:** Ensuring the security and privacy of academic records is critical. While blockchain offers immutability and transparency, it also raises concerns regarding unauthorized data exposure and potential attacks on smart contracts. Zero-knowledge Proofs (ZKPs) and Trusted Execution Environments (TEEs) have been explored as viable methods to enhance security and privacy in blockchain-based academic credentialing. Additionally, quantum resistance remains a long-term concern, as advancements in quantum computing could compromise existing cryptographic schemes used in blockchain networks [27].
- **User Adoption and Training:** The technical nature of blockchain systems presents a steep learning curve for faculty and students unfamiliar with decentralized technologies. A lack of blockchain literacy could hinder adoption and effective utilization [28]. Therefore, user-friendly interfaces, comprehensive training programs, and educational resources are essential to facilitate widespread acceptance. Research has shown that gamified learning approaches and interactive tutorials can enhance blockchain adoption in academic settings [29].

At the same time, when outlining the research advantages and prospects for application, the members of the research team see great hopes for development of this solution in the sphere of academic integrity and intellectual property rights. They have addressed these challenges in advance in their effort in designing and implementing the system to ensure a better and more efficient system in the future.

1.2. Study Objectives and Motivation Behind Them

The research objective is to ensure a systematic search of the literature on the security of digital assets and intellectual property in academic settings with the help of Blockchain and Non-Fungible Tokens (NFTs). The purpose of this study is to define and reveal the measures and approaches taken to protect the software, digital data and other relevant items in universities. To this end, the PRISMA methodology for searching, screening and sorting of the papers is used on the selected key databases. In addition, these four databases including IEEE Xplore, ScienceDirect, ACM Digital Library and SpringerLink have been selected because they contain numerous related research papers and articles.

Therefore, based on the overarching objective, this investigation seeks to address specific research questions (RQ):

- RQ1: What is the distribution of papers across different years, focusing on Final Project, Degree, Copyright, Software, Digital Content, and University Internal Protection?
- RQ2: How are the chosen papers related to the proposed keywords concerning these topics?
- RQ3: Which of the papers explore Blockchain-based tokens and Cross-Chain (Smart Contract) as a review related to the academic setting?
- RQ4: Which papers explore non-fungible tokens, Copyright, integrity, and software within academic and university contexts?
- RQ5: In the current landscape of Unique Assets of Digital Content, what constitutes the primary challenges that universities face regarding their internal protection processes?
- RQ6: What global standards are employed to safeguard the integrity and assets of digital content and media, especially in the context of educational institutions?
- RQ7: What types of NFTs are used to generate digital assets for content software and applications, and what methods and techniques are currently being utilized?

1.3. Contributions

This work aims to explore the application of blockchain and NFTS in the university context to secure the contents of the academic theses. Most attention will be paid to choosing resources related only to this application. The key objective is then to offer an effective solution for protecting the conceptual information that should be included in the students' theses.

The primary contributions can be summarized as follows:

- Synthesis of Existing Knowledge: To achieve this, we will perform a systematic review of the literature to provide a synthesis of the research studies in the field. Making this synthesis will give a clear connection on how both blockchain and NFTs can be applied to protect academic content. Further, we will describe the technical aspects and some of the ethical issues of their application in an academic context [30–32].
- Recommendations for Future Applications: From the identification of the project, recommendations on the future trend for the use of blockchain and NFTs in issues of intellectual property will be developed. This investigation will go outside the ivory tower's research confines as a means of providing valuable information for other aspects of intellectual property management strategies [33,34].
- Identification of Emerging Trends: The study will reveal contemporary and fresh ideas of utilizing blockchain and NFTs to address the issue of copyright and intellectual property rights. This will help in the ongoing debate of emerging technologies in the field of intellectual property [35,36].
- Practical Validation and Case Studies: We will look at examples of the adoption of blockchain and NFT in academic institutions, including current use cases and pilots. This analysis would reveal the experiences of practical difficulties or achievements in the implementation of these technologies in the context of this study [37,38].

2. Materials and Methods

Ableton of Blockchain with groundbreaking digital assets has been previously examined inversive literature, concerning information security and protection of intellectual property and the central notion of Blockchain: offering authenticity to digital contents in an educational environment. It also involves the evaluation of the Blockchain solution, NFT (Non-Fungible Token) which holds a great prospect towards guaranteeing the authenticity of the student-written software. Another example is the study that reveals the benefits of integrating NFT technology in creating special and non-tampered archives, such as ownership and history related to digital assets [39].

Further, that the use of decentralized storage solutions along with the application of Blockchain technology has been a central article in recent discussion. These approaches are meant to improve the security and access for digital content by using the nature of blockchain technology which is permanent and transparent [40]. For example, studies have shown how the benefits of hybrid Blockchain solutions will enable the safe storage and retrieval of academics' assets, thereby reducing dangers of hacking and loss [41].

Moreover, the review also considers other aspects such as technological and scalability and performance challenges of deploying Blockchain solutions in the education context. This is particularly so about the aspects concerning the scalability of the Blockchain networks given that protection of the digital assets and authentication of their ownership has been on the rise in the recent past. Recommendations have been given on how they might be solved, such as layer-two scaling and off-chain computation, in a manner that is not allowed to compromise on security [42].

Furthermore, the incorporation of such technologies in academic settings raises some concerns like the friendliness perspective where individuals can introduce in the Blockchain systems preferable level of ease. Therefore, it is important to ensure that the faculty members and the students can incorporate these technologies into their work so that they will continue to be popular in the distant future. Concerning the barriers to adoption, it has been ascertained that user-centered design and huge training programs should be used to minimize them [43].

Last, I would like to draw attention to the current satellite trends in the application of Blockchain and NFTs for intellectual property management; it is still working on the establishment of international standards to address and develop the utilization of the technology in the academic sphere. Ensuring these standards are compliant with the institutional policies is important to provide safe and legally acceptable environment to handle digital assets [44]. Altogether, this line of research evidence disruptive impact of Blockchain technology and NFTs in safeguarding academic content IP, while suggesting the application of this solution not only for academic facilities but for the management of any type of content in information society.

2.1. PRISMA

This section introduces the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology as a useful framework for searching and selecting relevant articles on blockchain technology in educational environments. This methodology is based on a series of systematic and reproducible steps that allow for a comprehensive and exhaustive review of the literature. The aim is to leverage the benefits of this methodology, which include:

- Conducting a comprehensive and exhaustive review of the literature.
- Reducing bias in study selection.
- Increasing the transparency and reproducibility of the review.
- Facilitating the synthesis of available evidence.

The PRISMA methodology steps that will be implemented are as follows:

a. Define the research question: What are the best practices for software project management in the post-production phase?

b. Identify relevant studies: Articles will be searched for in the following databases: IEEE Xplore, ACM Digital Library, ScienceDirect, and Scopus. The search terms will be: "Authenticity", "Blockchain", "Copyright", "Data protection", "Degree Works", "Digital certificates", "Digital Rights Management", "Intellectual Property", "Non-Fungible Tokens (NFTs)", "Source code", "Technological innovation".

c. Study selection: Studies that meet the following criteria will be selected:

    - Published in a Q1 or Q2 journal
    - Published in the last 10 years (2014-2024) to include recent advancements in blockchain and digital security.
    - Written in English or Spanish to ensure accessibility and broad applicability.
    - Directly relevant to the research question, specifically discussing blockchain, NFTs, and digital certificates in educational and intellectual property contexts.

d. Data extraction: The following data will be extracted from the selected studies:

    - Authors

- Year of publication
- Study title
- Abstract
- Methodology
- Results
- Conclusions

e. Data analysis: The data extracted from the different articles will be analyzed to identify the best practices for blockchain technology in educational environments.

f. Presentation of results: The results of the review will be presented in an informative table and its respective analysis.

Why PRISMA

The PRISMA methodology, designed for systematic reviews and meta-analyses, offers core principles that resonate strongly within this project's context:

- **Structured Literature Review:** While this project involves system development, a PRISMA-inspired approach to the literature review would ensure a comprehensive and unbiased exploration of existing research. This includes using well-defined search terms in relevant databases, clear inclusion and exclusion criteria for studies, and a thorough analysis focused on security, intellectual property protection mechanisms, and educational applications of blockchain.
- **Transparent Process:** Documenting the literature search strategy, system design choices, and evaluation methods aligns with PRISMA's emphasis on transparency. This allows others to understand the research process, assess its rigor, and potentially replicate the work.
- **Focus on Evidence:** PRISMA helps researchers move beyond subjective opinions and design a project that aims to generate concrete evidence. This can include data from security tests, insights from usability studies, and thematic analysis of feedback related to the system's impact on academic integrity.
- **Addressing Bias:** Even in a single-institution project, biases can creep in when designing or choosing technological components. A PRISMA mindset encourages the researcher to actively consider potential biases in the literature they're reviewing, the architecture they propose, and their evaluation criteria.

By incorporating these elements, the project gains the following benefits:

- **Credibility and Trustworthiness:** A well-documented, evidence-based, and bias-aware approach strengthens the research findings. This is crucial when recommending potentially disruptive technology to a university's stakeholders.
- **Synthesis and Insights:** PRISMA encourages researchers to move beyond just summarizing existing studies. It guides them toward identifying patterns, gaps, and areas ripe for innovation, making this project more likely to yield novel and useful solutions.
- **Foundation for Future Research:** A solid research foundation lays the groundwork for further exploration. The structured literature review can inform future meta-analyses, while findings of this project might inspire replication studies at other universities.

By clearly articulating PRISMA’s role in this study, the methodology’s relevance becomes more apparent, bridging the gap between literature review and the implementation of blockchain, NFTs, and digital certificates in academic settings.

2.3. Incorporation and Exclusion Parameters

To ensure a comprehensive and focused exploration of relevant research, the following parameters guide the literature selection process:

Incorporation Parameters

- **Direct Relevance to Education:** Studies explicitly investigating blockchain and NFT applications for intellectual property protection within academic settings are prioritized. This focus on the educational context ensures the review captures research directly applicable to the project's specific challenge.

- **Technical Depth:** Papers detailing technical implementations, architectural choices, NFT designs, and security mechanisms relevant to similar use cases are actively sought. These provide insight into the feasibility and potential design considerations for the proposed source code protection system.
- **Usability and Adoption Analysis:** Studies addressing the usability of blockchain-based systems for students and faculty, as well as potential integration challenges within university workflows, are considered vital. Practical insights into adoption barriers and facilitators contribute to the design of a solution tailored to the specific needs of the academic environment.
- **Empirical Data and Case Studies:** Papers presenting quantitative or qualitative evidence from pilot projects or implementations of similar systems are highly valued. Such data enables an assessment of the technology's potential impact on deterring plagiarism and safeguarding intellectual property.

Exclusion Parameters

- **Outdated Technologies:** Studies primarily focused on superseded blockchain platforms or earlier NFT standards are excluded to maintain focus on cutting-edge and actively maintained technologies.
- **Cryptocurrency Emphasis:** Papers with a central emphasis on cryptocurrency applications are excluded, even while acknowledging their reliance on blockchain. This refinement concentrates research on the application of blockchain specifically for intellectual property protection.
- **Focus on Relevant Educational Applications:** While some studies may offer valuable insights, those focusing on the application of blockchain in areas unrelated to intellectual property and higher education such as healthcare or supply chain management are excluded unless they directly contribute transferable knowledge to the educational domain.
- **Non-Academic Focus:** Priority is placed on studies conducted within academic institutions or contexts. Papers primarily exploring commercial applications are excluded to ensure the review reflects the specific challenges and regulations of the university setting.
- **Lack of Empirical Basis:** Purely conceptual or speculative discussions without data-driven analysis are excluded. The review favors studies grounded in concrete system designs, experimental results, or reasoned arguments.

3. Results

In this section, we present the findings of our detailed review focused on the application of blockchain and NFT technologies in relation to intellectual property security in academic papers. The analysis aimed to identify patterns, trends and insights related to the current secure integration of blockchain and NFT in the protection and authentication of source code in academic papers, covering the detailed evaluation of more than 100 selected studies.

The obtained results are presented in a concise manner with meticulously produced concise tables and graphs to present the obtained results. These visual representations make it easier to sort and analyze the wide range of papers reviewed, offering insights into key issues, methodologies, and emerging areas of interest at the crossroads between blockchain, NFT technology, and higher education.

3.1. Results Based on the Proposed Research Questions

- **RQ1: What is the distribution of papers across different years?**

As shown in Table 1, there are no papers from 2018 and earlier that align with the theme of blockchain integration and intellectual authenticity. This is because most papers from those years primarily focused on the introduction and potential of blockchain in other contexts, without specifically addressing its application for the protection of intellectual property or the authenticity of source code, which are key areas in our proposal.

The lack of papers during this period can be explained by the fact that the technology was still in its infancy during this period and has not been widely discussed in academic circles for such uses. Furthermore, the few papers that can be found before 2020 can maybe bring data that can already be obsolete or solutions that in the current environment would no longer be feasible or helpful because of fast evolution, important for the technological context, and the need in the improvement of the system of intellectual property.

Starting in 2020, there is a significant increase in publications, peaking in 2021 and 2022, with 31 articles published each year. This increase reflects growing interest and greater attention towards the integration of blockchain and NFT technologies in the protection of intellectual property and code authenticity. This coincides with the consolidation of these technologies and their recognition as effective tools to address challenges related to intellectual property in the academic environment.

The upward trend in publications during these recent years underscores the increasing importance and recognition of blockchain and NFTs as viable and necessary solutions for protecting intellectual property and authenticity in academia. This recent focus also indicates a shift towards broader adoption of these technologies, driven by their ability to offer immutable and transparent records that secure authorship and the integrity of digital assets.

Table 1. Distribution of papers by years.

Year	Number of papers
2018	7
2019	6
2020	16
2021	33
2022	34
2023	34
2024	2

- **RQ2: How are the chosen papers related to the proposed keywords?**

During the review of the articles, we observed that many of them not only focused on establishing a relationship between blockchain and various domains, but also on exploring how to ensure this connection to maintain the integrity and security of the chain. Table 2 categorizes these articles according to keywords such as integrity, copyright, software, digital content/asset, and non-fungible tokens (NFTs). It was evident that a significant number of studies emphasized the intersection of blockchain with copyright and software applications. For example, considerable attention to the integrity and protection of digital content was noted, suggesting a robust focus on information security.

In addition, many studies addressed both integrity and copyright, highlighting the importance of protecting digital assets in the blockchain environment. A particular interest in NFTs was also observed, with several papers exploring their specific applications and challenges. The distribution of different fields reveals a notable concentration on copyright and digital assets, indicating a thorough exploration of blockchain's potential in various sectors.

This detailed analysis highlights the diverse but interconnected nature of blockchain research, emphasizing both its technological advances and practical implementations. The review highlights that most studies focus on issues related to security and integrity, rather than on the blockchain integration framework, which is crucial for the future development of this technology.

Table 2. Classification of research papers on blockchain based on given keywords.

Work	Integrity	Copyright	Software	Digital content / Asset	Non-Fungible Token
[1–3,23–25,27,29,33,76,102,104,110,117–122]	X		X		
[10–12,26,28,30–32,39,42,44,71,72,83,89,91,97,99–101,105,106,108,109]	X		X	X	
[13,34,36,38,40,41,43,45,47,88,93,107]			X	X	
[16,35,49,52,56,59,65–70,123,126–132]			X	X	X
[19–21,37,46,50,51,75,82,90]		X	X	X	
[53,54,57,58,61,62,125,133–139]	X		X		X
[48,54,64]	X	X	X		X
[60,63,92,124,140–143]		X	X	X	X
[73,74,86,103,111–116]	X	X	X		
[77–82,84,87,94–96,98]	X	X	X	X	

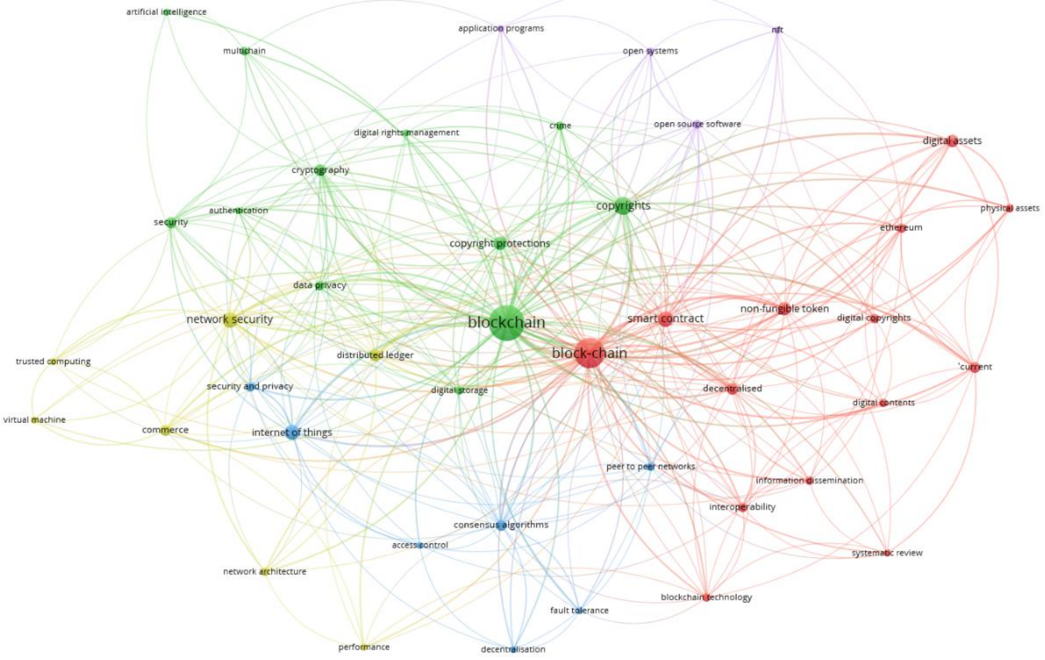

Figure 1. Co-occurrence analysis of keywords.

The VOSviewer-generated graph illustrates a co-occurrence analysis of keywords related to blockchain and its associated concepts. In this visualization, larger nodes represent terms that appear more frequently in the dataset, indicating their prominence in the analyzed literature. The most significant keywords include "blockchain", "block-chain", "network security", and "internet of things".

The colors in the network graph represent different thematic clusters, grouping related terms based on their conceptual associations:

- Green Cluster: This cluster primarily includes terms such as network security, privacy, encryption, and authentication, which are fundamental to the secure implementation of blockchain in business and cybersecurity applications.
- Red Cluster: This group encompasses terms like digital assets, smart contracts, Ethereum, and non-fungible tokens (NFTs), reflecting blockchain's role in the digital economy, asset tokenization, and decentralized systems.
- Blue Cluster: This category focuses on the Internet of Things (IoT), consensus algorithms, and access control, highlighting the interplay between blockchain and automated digital ecosystems.
- Purple Cluster: This cluster includes open-source software and open systems, emphasizing collaboration and transparency in blockchain development

Additionally, the graph reveals a strong emphasis on integrity and copyright protection, underlining the importance of securing digital assets within blockchain environments. Notably, there is significant interest in NFTs, with multiple studies exploring their applications and challenges. The distribution of thematic clusters indicates a strong research focus on copyright protection and digital assets, demonstrating blockchain's expanding role across various sectors.

- **RQ3: Which papers explore non-fungible tokens, Copyright, integrity, software and multichain?**

In conducting the search for different articles that could be related to the subject matter, 5 articles were found that are reviews and share a similar approach in their research on the integration of Non-Fungible Tokens, copyright, integrity, software and multichain, providing a detailed overview of how these technologies are being applied to ensure the protection and authenticity of software works.

Table 3. Papers that explore non-fungible tokens, copyright, integrity, software and multichain.

Reference	Main Keywords	Contribution
[24]	Blockchain, Consensus algorithm, Risk, Blockchain security.	This article provides an in-depth review of blockchain technology, including its history, consensus algorithms, cryptographic details (public key cryptography, zero-knowledge proofs, and hash functions), and a comprehensive list of blockchain applications. In addition, it focuses on blockchain security, assessing security risks, analyzing real attacks and failures, and summarizing recent security measures. Finally, it presents the challenges and research trends to achieve more scalable and secure blockchain systems for massive deployments.
[29]	Blockchain technology, Multichain, Simulation method, Tracing Drug	This study implements simulations with blockchain technology to track medicines, involving the pharmaceutical industry, wholesalers, health services and consumers. The main contribution is to improve traceability in the supply chain through a Decentralized Autonomous Organization (DAO) that organizes data and transactions in blockchain. The simulation demonstrates key features of blockchain such as transparency, immutability and peer-to-peer transactions, strengthening control over drug distribution.

[31]	Blockchain, digital transformation, food tracking and tracing, Multichain, private blockchain	In this article, the authors discussed the application of private blockchain using the Multichain open-source software that can be applied in agri-food products like food tracking and tracing, product life cycle and anti-counterfeit. He points out that digital evolution enabled by disruptive technologies including IoT, augmented reality, artificial intelligence & blockchain affects all spheres of human activity. Ever since blockchain was designed for cryptocurrencies, it has become a disruptor or an enabler of innovation in different sectors.
[46]	NFT, Non-Fungible Token, Minting, Ethereum, Copyright, Infringement, Blockchain	This article addresses transactions of intrinsically valuable assets in the digital world using Blockchain-based NFTs (Non-Fungible Tokens) used in games, literature, art and music. As various NFT exchanges emerge, copyright infringement issues also arise. The article classifies the types of copyright infringement that can occur in NFT exchanges and proposes countermeasures. Ten types of NFT exchanges are examined, and it is hoped that the proposed countermeasures will help revitalize the NFT market by providing solutions to these problems.
[47]	NFT, voting blockchain, escrow account	This paper proposes a secure blockchain architecture for NFTs that confirms transaction ownership and implements a secure payment method. NFTs, stored in a blockchain-based digital ledger, represent items such as photos, videos, audio and other intellectual properties, certifying their uniqueness. The proposed architecture uses a transaction confirmation node called J Node to prevent errors in token transfer via an escrow account.
[55]	Non-fungible tokens, Digital identity, Verifiable credentials, Blockchain technology, Smart contract;	This white paper addresses two key problems of NFTs: data storage security and breaches and fraud. It proposes a theoretical solution for storing digital assets underlying NFTs in a decentralized manner and presents "Connect2NFT", an application that connects Twitter accounts with NFTs to verify owner authenticity. A performance analysis and comparison with similar applications is performed, contributing to improving security and authenticity in the NFT space.
[60]	Blockchain, elliptical cryptography, unique token, Fractionalization, property right	In this paper, authors outlined UML diagrams for property rights distribution module through the fractal decomposition of NFTs, that are based on blockchain and conform to the ERC-1155 standard. The blockchain which is used in most illustrious in the executing of operations in Bitcoin helps in maintaining data and security and without having a third party who is believed to be trustworthy. Implements of this module creates the possibility of obtaining specific ownership fractions in decentralized application by means of Ethereum cryptographic protocols. The objective is when creating a new NFT, a functionality should enable the fractalization and the sale of fractions to other people when guaranteeing security and meeting functionality requirements.

[64]	Blockchain, non-fungible-token, analytic hierarchy process, credit rating, internet of things	The paper proposes a method to measure the credit rating of users in a blockchain traceability system, addressing the lack of efficient technologies to ensure the authenticity of data before it is stored in the blockchain. It analyzes trading processes and models in NFT markets and uses the analytic hierarchy process (AHP) to establish a credit rating system based on an evaluation matrix and efficiency coefficient. Experimental results show that this credit evaluation system can help judge the reputation of users and decide whether to restrict transactions of users with abnormal behaviors.
[74]	Decentralized copyright, international copyright, cross-border copyright, copyright protection, consortium blockchain, proof of authority	The paper discusses an understanding of a novel copyright framework in the global protection and international IP management using a consortium blockchain. By doing so, it enables copyright to be registered and traded internationally without the need of a universal cloud, with the use of proof-of-authority consensus mechanism. Member countries also authenticate and settle transactions on the block chain while a tokenized payment is employed for the copyright fees. Based on some of the ideas above, a prototype was created and tested; there were some ideas that were provided to help manage international copyrights.
[79]	Copyright protection, Blockchain, Deep learning, Data models, Music, Generative adversarial networks, Mathematical model	Deep learning models as applied to music composition and music copyright protection using blockchain technology is the innovation described by the paper. A deep convolutional generative adversarial network (DCGAN) has been utilized to synthesize monophonic melodies in addition to a multi-instrumental arrangement model called MICA. Besides, a new scheme known as Improved Byzantine Fault Tolerance (IPBFT) has been put forward to safeguard copyrights of digital music. The performance analysis reveals that the DCGANs and MICA models are more accurate and perform better as compared to other models and IPBFT based system is more efficient and has high throughput of 3469 transactions per second, it has 0% of error rate.
[82]	Block-chain, Digital copyright, Algorithm, Technology	The article investigates how blockchain technology, based on P2P networks and cryptography, can solve problems in the digital copyright industry: the confirmation, authorization and maintenance of rights. Using blockchain's self-monitoring, traceability and decentralization features, as well as the Map function, the study improves the data transmission rate in a multi-channel model and significantly reduces the probability of digital copyright infringement.
[83]	Blockchain, distributed hash tables, embedded systems, automotive networks	The paper proposes a software and data provenance mechanism for the automotive industry that ensures the integrity and reliability of vehicular software. Since automotive software is complex and security-critical, and updates can introduce risks, the proposed approach uses distributed hash tables (DHTs) and a public blockchain to ensure high security, scalability, and efficiency, thus

		protecting users, service providers, and original equipment manufacturers (OEMs) against software compromises and errors.
[85]	Software protection, privacy distributed objects, services software, cryptographic controls, authentication, data encryption	In the article the author provides a solution to an issue of software piracy and how to protect the copyrights through implementation of what could be termed as decentralized software license validation system using blockchain technology and cryptocurrencies. The proposed method forms an environment where the privileges and rights of participants are observed; this has enhanced software protection since the 1970s when the issue of license validation as the major solution to combat piracy came up.
[88]	Blockchain; Distributed ledger; Blockchain-based Library management; Ethereum, bitcoin, Peer-to-peer network	The paper presents a blockchain-based library management system to overcome problems in auditing and inventory of books, journals and periodicals, despite automation with RFID. Blockchain technology provides transparent and immutable records, which improves auditing and inventory control in advanced libraries. The implementation of a library management system using smart contracts written in Solidity in Remix IDE is demonstrated. The article includes the smart contract source code and screenshots of the blockchain-based book management system.
[92]	Smart contract system, non-fungible token, copyright	The problems that are invited by the article are how through NFT, the creators of arts can easily be enabled to register and sell the arts through an implemented smart contract which will mean that the ownership of the artwork can change hands with evidence of a verified digital certificate. Looking at how one posts on NFTs and other marketplace galleries offline galleries. As for the advantages and disadvantages of applying NFT for copyright protection, the former are listed as follows the legal genuineness of applying NFT to the protection of copyrights Given the fact that NFT is still relatively young, unheard-of technology.
[99]	Blockchain, Multichain, Decentralization, Privacy, Data Sharing	The article presents a decentralized data sharing architecture using the MultiChain blockchain, applied to the travel industry and adaptable to other domains such as education, health and sports. The solution enables companies in the travel industry, such as travel agencies, hotels and shopping malls, to share user profile data in a secure and controlled manner. A hotel booking service is used as an example, where users decide what data to share, ensuring privacy and control. The data is converted into an open format and shared across the blockchain for easy integration with other nodes. The paper evaluates the performance of the model by measuring latency and memory consumption in three test scenarios, showing fast responses in all cases.
[100]	Fin-Tech, Blockchain, Distributed	The article develops a complex of reforms in financial transactions based on the decentralized application of the blockchain model, demonstrating the possibility of

	Ledger Technologies (DLT), Cryptography, Equity Market, Integrity	increasing the reliability of financial transactions in such spheres as Fin-Tech, Medicare, hospitality, manufacturing, and others. Applied to financial services, blockchain or the distributed ledger technologies (DLT) ensure the integrity of record through cryptography to eliminate vices like money laundering. Major characteristics of those blockchains, including PoW and PoS, and their effects on the stock exchange, wealth management, payments and remittances, commerce and insurance are highlighted in the article.
[104]	Wheat products, traceability, authority-control, hierarchical supervision, blockchain, multi-chain	To cover the shortcomings of centralized monitoring and privacy leakage in agricultural traceability system, this paper proposes a hierarchical monitoring model of wheat supply chain based on blockchain and Hyperledger Fabric. The model guarantees the availability and clarity of the data and strict control of private data, with their protection through encryption and possibility of access control in terms of shares. The results indicate high security levels while the average latency times are 6. 67 ms for public data and up to 37. 78 ms for private data monitoring, where protection of privacy and data monitoring in real time is possible.
[108]	Blockchain, Asset traceability, Data security, Immutability	The article describes the possibilities of deploying blockchain in an organization’s supply chain and of sharing assets without formal permissions. The developed software application takes advantage of blockchain technology allowing it to provide more secure storage and immutable records for the asset transfers that can either be public or private depending on the setting of the application. Data cannot be altered after entry and the push for accuracy means it will not require any manual check.
[110]	Blockchain, smart contracts, MultiChain, submission systems	The article covers a real-life case of redesigning a homework submission system based on the blockchain approach. Nonetheless, it was not a perfect match for blockchain, it helped us to have some fun and discover some compelling features of this technology that can be used in a hard and familiar problem. It expanded the knowledge base about what blockchain could potentially solve for, and what issues it could avoid.

- **RQ4: Which of the papers explores Blockchain-based tokens and Cross-Chain (Smart Contract) as a review related?**

The review of the articles reveals that several papers explore the use of Blockchain-based tokens and Cross-Chain solutions in the context of smart contracts. These studies focus on how these technologies can improve security, efficiency and data management in various sectors, highlighting especially in education and real estate. For example, one of the articles proposes a decentralized education system based on smart contracts that uses the Ethereum Virtual Machine (zkEVM) to manage academic certificates, eliminating bureaucracy and reducing costs. This system ensures compliance with regulations such as GDPR, providing a more secure and efficient solution for managing educational documents.

Another paper presents a conceptual framework for the adoption of Blockchain-based smart contracts in the smart city real estate sector. This study identifies key aspects and details the use of the Ethereum Virtual Machine (EVM) to develop these contracts, improving the user experience and benefiting property owners and real estate agents by aligning with Industry 4.0. In addition, solutions for Domain Name System (DNS) centralization using Blockchain are addressed, optimizing domain management and speeding up transactions.

These papers highlight how the integration of Blockchain and Cross-Chain solutions can transform traditional sectors by implementing advanced technologies that improve transparency, security and operational efficiency, while complying with regulatory standards and offering new, more robust and reliable business models.

Table 4. Analysis of Blockchain-based tokens and Cross-Chain.

Reference	Contribution
[34]	To redesign the higher education system, the article has a solution of solving the issue and the cost of certifying, by implementing blockchain. It analyses the prerequisites for decentered education highlighting the necessity of applying a blockchain scale solution which is ZKP integrated with Ethereum virtual machine. The improved system for managing educational documents, which has been described in this paper, fulfills the proposed requirements and regulations including GDPR and uses smart contracts and the modular blockchain structure to provide a more secure solution compared to the existing ones.
[36]	The article presents a conceptual framework for the adoption of blockchain-based smart contracts in the smart city real estate sector. Through a literature review, it identifies ten key aspects and details the use of the Ethereum Virtual Machine (EVM) to develop these contracts. The study provides a design for owners and users, and a procedure to manage smart contracts, improving the user experience and benefiting owners and real estate agents, aligning the sector with Industry 4.0.
[41]	In this paper, centralization within the existing current domain name system DNS is discussed, and blockchain is suggested to be a solution. Adjacent environments also showcase that the core of Ethereum, the Ethereum Virtual Machine (EVM), is tailored to support a smart contract-based Domain Name System to enhance domain name governance and finality, as well as accelerating the transactions. The EVM also contains new data structures together with new opcodes to make the transaction processing flow easier. The evaluation proves that there is a two-order-of-magnitude enhancement in the blockchain based domain name resolution system as presented in the research above.
[44]	This article will show how blockchain technology, which is characterized by its impenetrable security measures and decentralized nature, stands to disrupt numerous industries with emphasis on the financial and banking industry. It also refers to the new trend involving NFTs, digital tokens associated with unique works of art like paintings, music or indeed tweets. The paper explores the negative impacts of the blockchain and NFT across different sectors; IoT, banking, music, agriculture food and supplies, and healthcare.
[51]	The article presents the concepts, characteristics and development processes of blockchain-based NFTs (non-fungible tokens), highlighting their use in collectibles, crypto-artworks and games. Its core elements and typical fields of application are discussed, as well as issues and risks related to property

	rights, value, technology and oversight. Related literature is also reviewed and research topics on value assessment, transaction modes and pricing of NFTs are proposed. Finally, the trend of digitization driven by NFTs is examined.
[53]	The article discusses blockchain technology and the relatively new phenomenon of NFTs (non-fungible tokens). It analyzes the growth prospects and current shortcomings of the concept. It examines the NFT phenomenon from a technological point of view, as it is not yet well described in scientific publications. Based on the market analysis, the authors suggest further development of the blockchain, strengthening its security and conducting additional research in this area.
[62]	What the metaverse does is to combine aspects of the physical world with those of virtual reality to allow functions like trading and entertainment through avatars. We describe the increase in NFTs (non-fungible tokens), which are most used in video games and art and explore how these assets could be used to address real-life issues due to their specific features. Blockchain and tokenization are at the base of the metaverse and the NFTs, and they have several use cases such as Model Chain in the medical field or verifiable transactions in the commercial world. The research highlights experiences that explain how blockchain is used in NFTs and its drawbacks; it encourages further research on its implementation and link with the metaverse.
[63]	The article discusses the rise of tokenization of assets such as stocks, funds, debt and intellectual property due to the growth of decentralized finance (DeFi). Blockchain technology allows physical or digital assets to be converted into NFTs (non-fungible tokens) and traded in cryptocurrencies, using a distributed ledger technology (DLT) system for immutable, traceable and secure transactions. Although NFTs are mainly used in digital art, collectibles, and gaming, this article proposes their application in real estate management. It examines the requirements for an NFTs-enabled property management and exchange system and presents a detailed model for its implementation, providing key components and guidelines for its use in property management problems.
[76]	This article describes the trends in utilizing open-source software and challenges of compliance with the corresponding licenses, namely GPL, MIT, Apache, Mozilla, and BSD. As to the source code, the license conformity can be easily checked; it has roots in legal, ethical and security scopes. To optimize open-source software licenses hence reducing on violation, a blockchain is used to implement the licenses. The solution includes the use of four modules: Interplanetary File System (IPFS), smart contracts, MetaMask as a transaction manager and a permission blockchain to meet the licensing requirements.
[94]	The attempt made in the article is to proffer a novel IPR management framework in the smart contracts based blockchain system. Work done in a frame of the MediaVerse project funded by the European Commission outlines an extension of smart legal contracts that are aligned with the blockchain smart contracts and include their management of cloning, notarial aspects, rights transfer and revenues distribution. This is the reason why the concept is aimed at enhancing the management and monetization of Digital Rights with an intent of promoting the rights of content creators.

- **RQ5: In the current landscape about Unique Asset of Digital content, what constitutes the primary challenges that Universities internal protection process?**

While analyzing the articles, we noticed that not only demonstrate the existence of a link between the blockchain and various domains, but also the possibility of how this relationship would ensure the cohesion to protect the chain's sanctity. The studies considered a range of issues related to the management of the university's internal processes of information security for specific digital content. Among the challenges include data security and privacy particularly where large chunks of information is involved and flows across devices – this creates problems in the protection of privacy. However, blockchain technology is accompanied by performance and scalability problems which include transaction per second, block size and many others.

The other crucial factor is a multichain, where there is a combination of more than one blockchain and handling multiple blockchains come with other complications including the integration of blockchains. This also brings out the issue of social control and regulation since decentralization can create problems with governance and regulation. At long last, the future consequences of integrating blockchain to IoT are unknown since they have a complex future in security, privacy, and coordination.

However, there exists a stark lack of strong protocols for the decentralized storage and authentication of patents such as the NFTs, and simple solutions on how the authenticity and ownership of these patents will be verified. As blockchain rises as a more crucial focus in handling digital assets it is important to solve these challenges.

Table 5. Main challenges in the current landscape of Unique Asset or Digital content and Universities internal protection.

Reference	**Challenges**
[38]	In the merging of blockchain with IoT some challenges are pointed out. Some of the main issues include data protection and privacy because when dealing with personal information, its use across different devices presents a challenge in its protection from third party intervention. Besides, there is a set of limitations of the blockchain technology, some of which are the poor throughputs and size of the block that define the capacity of the system. The challenges of multichain, which arise when one must manage more than one blockchain involve issues to do with integration of the different blockchains involved. It also has issues of social control and regulation because decentralization is always an issue about the ability to govern and regulate. Last but not the least, the future of integration of blockchain with IoT for long turn and its space security aspects along with privacy and efficiency are still mysteries to understand.
[48]	Decentralized Storage and Authentication Requirements: Our paper highlights the urgency of elaborating efficient solutions for decentralized storage and NFT-authenticated patents. Decentralized Verification: However, the invention can require the improvement of effective communication to create the opportunities for decentralized verification of the patent authenticity and its owner. Blockchain Implementation Issues: NFTs with blockchain approaches, so there is possible to guarantee the relative stability of patents' management. Real World Application Challenges: That is why it is necessary to apply for NFT and consider it more in the context of its business application for patenting, financing, biotechnology, ticketing, etc. Future Direction and Open Issues: Outlining the current issues that remain open and the development that is yet to be accomplished on the prospects of deploying NFTs with patents and the legal, compatibility and expansibility concerns that exist.

[72]	In the article provided, the technological growth of blockchain in smart grids has been investigated through multiple factors where it shifted from centralized to decentralized one. It discusses block chain in gird, billing and metering while outlining projects and use case in energy sector. It also outlines existing security threats in smart grids, Ethereum Virtual Machine environment, and smart contracts. It predicts the pros and cons of various protocols and analyzes their suitability in specific use cases, which can serve as a reference for the further study on the construction of secure blockchain foundation in smart utility grids.
[80]	This paper also examines how blockchain technology can be effective in providing mechanisms such as digital copyright protection by decentralizing the technology, making it invulnerable, creating time stamps and records and ensuring that these records are traceable. Nevertheless, numerous advantages are provided using blockchain technology for the registration and confirmation of digital copyright, monitoring of transactions, and preservation of evidence Among them, there are several challenges and difficulties arising from the implementation of blockchain technology, here they are. In this study, the authors put forward blockchain-based system construction for digital copyright protection to try and record the copyright process, detect data infringement, and offer accurate electronic evidence along with cost reduction to enhance the efficiency of judicial resort.
[81]	The article highlights several problems in applying blockchain technology to protect multimedia content. First, it shows the lack of a comprehensive and systematic manner of categorizing on identifying applications of blockchain in copyright protection. In addition, it notes that there are very few successful systems to this end which suggests a clear deficiency in the literature. It means that there is no development and it's because there is no integration between technicality and applicational knowledge. There are also technical barriers in the implementation of such systems and more investigations need to be carried out with a view to surmounting these barriers in the development of an efficient multimedia copy right protection system based on blockchain.
[84]	The article addresses legal challenges related to the use of blockchain in copyright protection. Key issues include: deciding whether to store content on or off blockchain, and adjusting the legal status of online intermediaries; finding a balance between the immutable nature of blockchain and the need to adjust records due to the flexible nature of copyright; ensuring trust in blockchain records, given that they cannot validate facts originating off-chain; and legalizing cryptocurrency transactions, as well as the status and legal consequences of smart contracts. In addition, the economics of blockchain-based copyright management systems must be considered to ensure they have necessary network effects.
[102]	It is important to address four significant issues regarding data protection and privacy in edge computing and blockchain explained in the article below. The issues include: the limitations of blockchain in tackling security problems for edge computing; the idea of using a multi-chain (master-slave) system combined with an edge computing framework to enhance data security; how the proposed signature authentication scheme based on ECC can be amalgamated with blockchain encryption processing; in applying appropriate control with user privileges for a subset of the basic system; and the difficulty of low system overhead on improving algorithm performance and increasing transaction rates simultaneously.

[105]	The paper details give several difficulties in deploying private blockchain infrastructure to store academic certificates. The main concerns are as follows: certificate forgery and validation through hashing; selection of the private blockchain solution (Multichain) that has less cost in comparison with public blockchains with storage charges; and the need to create secure and transparent data storage though low cost and easy to support infrastructure.
[126]	The purpose of this paper is to outline the implementation of a mobile digital library system which enables a user to upload books, borrow books, read them, and return them using the mobile interface without having to go to the university of Sam Ratulangi library. Digital content protection methodologies including watermarking and locking to prevent selection and copying are employed in the system to fight against piracy and plagiarism. It becomes crucial to understand and follow the application of these techniques because it makes sure of the safeguard and preservation of digital assets to evade corruption of the content when stored electronically that is very vital for management of digital resources in a digital library.
[128]	Some of the issues which can be considered as critical for the internal protection of unique digital assets in Universities are: Firstly, it is still necessary to rethink the existing legal frameworks to provide the application of open models such as CC licenses. Moreover, there are major challenges in relation to maintaining viable business models through which the producers of open content, as is the case with filmmakers, can monetize their work. Fourthly and lastly, it is evident that failure to develop coherent and comprehensive policies and regulation with respect to production, financing, and marketing will cause a chain of fragmentation of the Open Content Filmmaking (OCF) movement, which is a hindrance to the progress of this movement.
[130]	In the context of protecting unique digital assets in universities, the article identifies several key challenges related to the preparation of future teachers in institutions of higher pedagogical education. These include the need to develop professional digital competencies that are isomorphic to teaching functions, forming a holistic system of competencies. Three fundamental functions stand out: heuristic-digital, management-digital and self-development-digital, in addition to general competencies such as digital security. The complexity lies in integrating these competencies into a coherent system that addresses the digitization of education, protects personal data, respects copyright and ensures digital security, which is crucial in the digitized educational environment.
[132]	Regarding the issue of the copyright protection of special learning resources in universities, this article discusses a few aspects of copyright issues on production and distribution of digital resources including folk music. Since there is an increase in digital copyright infringement, there is a necessity for a blockchain based digital protection enforcement model. Some of the limitations are identifying the right architecture for safeguarding of copyrights, realizing its applicability in real-life scenarios and identification of any weaknesses in the model. Moreover, reform and innovation in music education at the university level also raises the question of integration of this technology as the solutions for battling against piracy as essential for a digital learning process are as well.
[134]	Finally, based on the identified goals in the formation of the curriculum of the Bachelor's degree in social communication at the Universidad Centroamericana José Simón Cañas in El Salvador, this case analysis

	underlines some of the difficulties in the process of forming digital competencies. Regarding the main difficulties stated, they refer to the failure in deep understanding of digital skills, the scarcity of the environments allowing the development of critical skills towards the use of technologies, and the complete absence of the content on copyright, collective intelligence, and Internet security. These elements are essential to provide guidance and prevention on identity and personal data on the web and social networks and to learn about abuse and technology addictions. Revealed necessities to revise and reinforce the curriculum offering the protection of assets at the educational level.
[136]	From the study several issues emerge concerning the protection of content in libraries using the digital rights management (DRM) systems. This paper examined that librarians understand that although DRM systems acting positive roles in combating against the infringement of copyright laws, they possess several disadvantages. One problem is that such systems do not allow the limited use of information, such as sharing articles and other electronic resources with colleagues and forcing users to work with the material in a fragmental manner. At the same time, it was noted that some e-books and e-journals could be downloaded freely by the unauthorized users while they have DRM technology installed. Based on these arguments, there is a strong necessity for adequate government policies, regulating issues of copyright and fair use of information, taking into consideration the features of DRM technologies that contribute to the life of digital libraries, their advantages and drawbacks.
[138]	The article reveals the problematics of regulating and protecting rights in the sphere of ICO (Initial Coin Offering) by considering the state and legal factors. Some of the main risks include employing the existing legislation to protect intellectual property rights; prevent legalization and illicit origin money laundering; and protecting personal data without adaptations for ICOs. This may reduce the efficiency of the acts of regulation in an innovative and technological space like the ICOs. The findings indicate the necessity of the development of more concrete rules to handle these problems, which may be useful for universities, professors, and students as far as the digital economy and regulation of advanced technologies are concerned.
[140]	We can define the following difficulties with the digital economy context and the digitization of universities: Today the processes of education, research, international cooperation, marketing, finance and economics in higher education institutions need their digitization. Among them IT threats include protection of personal data and security issues, which are critical in the growing process of digitization of education systems. The article provides emphasis on the dependence on the effective before the demands of the digital economy for the direction of a strategy to provide higher education and positive synergistic effects from using information and communication technologies in universities and measures for the implementation of this strategy.

- **RQ6: What global standards are used to safeguard the integrity and assets of digital content and media?**

Thus, in the conditions of relatively short existence of digital culture, the issues of text and media integrity and protection appeared to be one of the key concerns. With the increased use of digital assets, there comes increased risks such as hacking into the database, piracy, data loss and theft of intellectual property. In response to these challenges, several international standards have been put in place to protect digital content and media. These standards which have been developed by different international organizations, define frameworks and policies that assist organization to protect its digital resources and content as well as their intellectual property.

While reviewing the content of related works, it was found that, in addition to the identification of the link between blockchain technology and various domains, attempts have also been made to identify ways to sustain this connection with the help of effective algorithms for the integrity and security of the blockchain. Some of the issues that these studies raise include data security and privacy, especially when using the data on different devices. More to the point, there is a problem of performance and relative scalability, such as raw computing capacity and block size. When there are two or more blockchains, which are referred to as 'multichain', these issues include coordination and communication between the blockchains, social controls and regulation because of decentralization. In addition, the future usage of blockchain with the Internet of Things (IoT) needs further assessment of its long-term effect on security, privacy, and efficiency.

Furthermore, the enhancement of proper solutions for the decentralized management and verification of virtual properties, for example, patents in the form of NFT is increasing. A perfect match of geographically decentralized procedures of patent authenticity and propriety checking is also needed. Hence, given the role of digital asset protection in the modern blockchain landscape, these challenges need to be addressed properly. The following article aims at discussing some of the most common set of standards globally found within this field with regards to their duties, application and with special concern to the digital content and media industry.

Table 6. Global standards used to safeguard the integrity and assets of digital content and media.

Reference	Description
[66]	Non fungible tokens (NFTs) therefore have numerous factors that hinder their growth these include usability challenges that affects their usage by the user and interoperability issues that affects its ability to interoperate with other platforms as well as standards which restricts its functionality. Although they are relatively new and have increased in popularity recently, NFT technology is not yet fully developed in its development. Some examples of such standards have been ERC-721 and ERC-1155 which have been the basic framework, but new standards that build upon NFTs have been developed. Also, the markets which are associated with NFTs have begun to experience some sort of speculative bubble regarding the prices of certain tokens, and the technology itself is still immature compared to other technologies because it is relatively new.
[69]	The article examines the legal requirements of the California Consumer Protection Act (CCPA) and the General Data Protection Regulation (GDPR), as well as the intersections between privacy laws, genomic data and smart contracts such as fungible and non-fungible tokens (NFTs). These laws impose restrictions on the storage, access, processing and transfer of personal data, which presents challenges for lawyers, data processors and companies offering blockchain-based solutions, especially in relation to high-risk genomic data. The technical features of NFTs, distributed storage and wallets enable tracking and management of genomic datasets, offering data donors a way to establish digital ownership and control under privacy laws through smart contracts with "programmable privacy." The design of blockchain-based value propositions must include privacy by design capabilities in the smart contract coding language. The article explores how data engineers can integrate legal requirements into smart contracts,

	exemplifying the approach with the Genobank.io platform, which preserves the privacy of genomic data.
[111]	This paper presents a blockchain-based secure data sharing platform using Interplanetary File System (IPFS) to overcome trust, transparency, security and immutability issues in traditional trusted third-party dependent (TTP) platforms. In the proposed system, data is stored in IPFS and divided into secret parts, with access roles managed through smart contracts written in Solidity. Users are authenticated with RSA signatures and must pay for digital content, after which they can leave reviews that are validated to eliminate forgeries. The use of Ethereum blockchain, decentralized storage, encryption and an incentive mechanism ensures transparency, security, access control, owner authenticity and data quality. The proposed scheme was tested on an Ethereum test network, showing that the use of the Shamir Secret Sharing Scheme (SSS) results in lower computational times compared to 128-bit and 256-bit Advanced Encryption Standard (AES).
[112]	This article explores the challenges and misunderstandings in the art market related to non-fungible token (NFT) technology and blockchain, through the perspective of an art technology entrepreneur. Despite initial enthusiasm and significant projects in Asia, NFT transactions have reached an all-time low, and there is little empirical research on blockchain use in the art market. The article discusses current NFT and blockchain use cases in comparison to the traditional art market, with a particular focus on the ongoing work of the Art ID Standard consortium, which encompasses decentralized identity and blockchain use cases. Perspectives are offered on the implications of these challenges for artists, collectors, and the art ecosystem at large.
[114]	This paper discusses the development of a DRM system based on blockchain to overcome the drawbacks of centralization and opacity inherent in a traditional DRM system. It also makes transactions and license information to be described on the blockchain to enhance data transparency & security. Similarly, smart contracts make issuance of licenses automatic, and reliable transactions without the need for centralized servers. The proposed system also has the advantage of easing the flexibility of charging various prices to reflect the varied rules regarding the use of the content. The main contribution reported in the paper is the specification of a blockchain-based licensing scheme that can integrate with existing DRM standards and thus can be easily adopted by the industry.
[115]	This research helps to fill the gap between digital competencies in accounting and finance training because of the growing use of automation and technologies like blockchain. As proven by massive funding in the FinTech space and high job automation of accounting roles, graduates must develop digital competencies. The study employs a three-step method that involves overlay of digital topics to the course, assessment of existing practices and tools on digital learning, and interviews with subject matter specialists for confirmation of the necessity of digital inclusions to the course. The findings reveal that merely five per cent of all the required applications are explicitly taught while specialists agree with the increase in the use of digital content and the importance of digital integration in learning. Hence the study finds out that though digital inclusion is relevant many instructors are unaware of the latest technological development hence the need for change in the field of accounting and Finance education.
[118]	This article provides a systematic review of EHRs interoperability and uses blockchain solutions, where 18 blockchain based solutions to EHR

	interoperability challenges are highlighted. There are, however, challenges that come with these solutions in the aspect of reliability, privacy, integrity, sharing and standards. It showed that such a review is conducted under six phases, which are acquaintanceship with research questions, article selection or data mining and progress tracking using Google Scholar, Web of Science, and IEEE. Out of those 18 articles, the requirements of interoperable blockchain-based EHRs, related standards, and the solutions to enhance interoperability are discussed. The areas include the best practice for interoperability of blockchain standards, implementations, applications and issues related to the adoption of blockchain in EHR management are touched on in the study.
[120]	The paper also discusses the blockchain mobile platform called HealthPocket to exchange health information of proven genuineness through a dynamic consent mechanism aligned to HL7 FHIR. These, often used in healthcare standards all over the world, enable clinical data exchange with reliability and accuracy. Blockchain coupled with the dynamic consent system means that any health information exchanged cannot be changed hence it addresses security and protection of personal information. The platform helps different medical institutions to work together and share data between different institutions and around the world because all the data filled in the template is compatible.
[122]	The article explores the capabilities of blockchain technology as a public good in the education sector, especially in the context of self-sovereign digital identity. While blockchain has been identified as an opportunity to drive needed changes in educational processes, use cases have been limited due to disconnects on fundamental issues such as governance, self-sovereignty, interoperability, choice of blockchain platforms, and trust in standards and infrastructure integrity. In particular, the article focuses on the challenges and viable solutions in the digital credential sector in Europe, highlighting the importance of interoperability and integrity of digital identity and content, considering them essential for the effective implementation of blockchain in education.
[123]	This paper suggests the integration of HSM with block chain technology particularly with public key cryptography algorithm/ standards. HSMs also offer physical protection, which can be called 'root of trust'; it adds a new layer of security to the system design, which can provide more reliable authenticity, authorization and integrity solutions. This paper focuses on the effectiveness and applicability of carrying out a proof of concept with this proposal Al time performance analysis shows that integrating the HSM with the Blockchain can go a long way to enhance the security of the industrial IoT systems. The major contribution concerning global standards is the PKCS standards for security when integrating HSM into Blockchain, which is an overall security requirement when using decentralized environments for content and assets protection.

- **RQ7: What types of NFTs are used to generate digital assets for content software and applications, and what methods and techniques are currently being utilized?**

NFTs have become a significant change on the digital spectrum as it has presented an innovative method of attesting to the ownership and uniqueness of digital entities. Automatically, and artificially, as exclusive, cryptographic tokens, NFTs have been employed to provide provenance of digital assets and content, software, and applications; in doing so, original owners and creators are now able to monetize their work in breakthrough ways. NFTs' rapidly increasing popularity concerns various fields in the sphere of digital assets, such as art, music, virtual land, and in-game items. This evolution has been caused by the need for secure and verifiable ownership in a digital environment which is captured by NFTs using blockchain technology.

While analyzing articles identified in the previous stage, it was found that different kinds of NFTs are used to create digital assets regarding content software and applications. Some of them include. The utility NFTs, offerings that grants the holder, certain privileges in a digital ecosystem, the collectible NFTs, which apply widely in gaming and virtual worlds, and the functional NFTs which are essential and embedded into the operational features of the software application. The studies also discussed the ways and means adopted in generating and developing these NFTs along with focusing on the smart contracts which play an essential part to facilitate transactions and ownership regimes. Moreover, Ethereum and Binance Smart Chain are the most popular platforms for developing, trading, and storing NFTs with their help, when it comes to their safety and non-tweakable nature.

The constant creation and implementation of new NFTs for digital assets in content software and applications thus requires that proper methods and appropriate techniques be developed to harness this technology. This article will strive to offer the current use of NFT types, and the techniques applied in creating and handling them in the current market with insights on future advancements of this progressive and innovative segment.

Table 7. Methods and techniques used in the generation of digital assets for content software and applications using NFTs.

Reference	Title	Content
[125]	NFT as a proof of Digital Ownership-reward system integrated to a Secure Distributed Computing Blockchain Framework	The paper suggests the organizational infrastructure in the blockchain context with the “Hyperledger Fabric” technology on which companies can securely transmit and share the information. One of the ways is embracing digital asset technology where it encodes data in Non-Fungible Tokens (NFTs) to reduce the possibility of forging information. It uses smart contracts and adopts the IPFS decentralized storage system in which all the components interface via a WEB application. The solution is feasible, manageable and applicable to the development of new systems and processes in digital asset management.
[127]	Royalty-Friendly Digital Asset Exchanges on Blockchains	The study addresses the automatic distribution of royalty payments associated with digital assets, especially Non-Fungible Tokens (NFTs). It proposes a marketplace-independent trading framework for royalty management, called RM-TLSC (Royalty Management Token-Level Smart Contract), which creates synergies between the token and smart contract paradigms, ensuring royalty management throughout the asset lifecycle. An open-source software implementation for the Ethereum blockchain is provided, and the generality of the approach is verified with proof-of-concept for the Tezos blockchain. Effectiveness is demonstrated with a case study related to the ISO 21000-23 media smart contract standard.
[129]	On the Scrutinization of the NFT Valuation Factors	The paper investigates the concept of software relative to Non-Fungible Tokens (NFTs) with more emphasis on inception and selling of NFTs based on the underpinning digital or tangible assets. What it specifically does is that it outlines a method for evaluating the value of an NFT and

		how best to anticipate its success. Though, it points out that community and scarcity are dominating the valuation of an NFT and again dwell more on the relationship between factors and NFTs' prices. It also provides the possible future research prospects within this field.
[131]	Blockchain and NFT: a novel approach to support BIM and Architectural Design	The research focuses on the benefits of blockchain technology in the use of Building Information Modeling (BIM) system adopted in structural designing and construction project management. It explains how, and why, Non-Fungible Tokens (NFTs) could be used to manage the provenance and ownership of relatively bespoke and precise digital goods – such as BIM models – represented by digital files. These NFTs help to solve questions related to copyright, as well as manage author's and owner's rights for numerous large projects; they also help with file certification. The findings of the study also show that incorporation of BIM with blockchain can enhance security and raise efficiency in the administration of digital assets in architectural, engineering and construction projects through effective protection of copyright and sharing of information.
[133]	Forecasting NFT Prices on Web3 Blockchain Using Machine Learning to Provide SAAS NFT Collectors	The study investigates Non-Fungible Tokens (NFTs), describing them as unique digital assets that may include art, video game goods and entertainment collectibles. These NFTs are distinguished by their exclusivity and authenticity, backed by digital certificates. The paper introduces a Software as a Service (SAAS) based system that uses Web3 blockchain technology to facilitate the management, security and trading of these digital assets. This system enables unrestricted access and detailed analysis of NFTs. In addition, the study applies adaptive enhanced convolutional neural networks (AICNN) and a tree seed chaotic atom search optimization (TSC-ASO) algorithm to predict the prices of NFTs, demonstrating that this methodology is effective in generating accurate predictions about the future value of these assets.
[135]	Is non-fungible token pricing driven by cryptocurrencies ?	The study analyzes Non-Fungible Tokens (NFTs) as the first application of blockchain technology to reach public prominence. NFTs are exchangeable rights to digital assets (images, music, videos, virtual creations) whose ownership is recorded in smart contracts on the blockchain. It is investigated whether the price of NFTs is related to that of cryptocurrencies. Through a spillover index, a limited volatility transmission between cryptocurrencies and NFTs is observed, while a wavelet coherence analysis shows a co-movement between the two markets. This suggests that the pricing behaviors of cryptocurrencies could help us to understand the pricing patterns of NFTs. However, the low volatility transmission indicates that NFTs could be considered an asset class with low correlation with respect to cryptocurrencies.
[137]	NFT luxury brand marketing	The paper explores the way Industry 4. It also means that 0 technology can increase the value of digital assets in the

	in the metaverse: Leveraging blockchain-certified NFTs to drive consumer behavior	metaverse of luxury brands in the virtual marketplace to retain their brand image and target new customers. In this way, luxury brands can guarantee the process of marketing and shelter consumers' digital properties with the help of blockchain-based NFTs' ability to check assets' originality. The study examines the consumer attitudes towards luxury NFTs in the metaverse and found out that the psychological evaluation aspects are the reason influencing the purchase of such products. Thus, the study expands the horizons of game theory and prospect theory while presenting arguments based on the psychological perception of the risks that result in failures/successes in purchasing (or not purchasing) luxury fashion NFT in global virtual markets.
[139]	Non-Fungible Tokens (NFTs): A Review of Pricing Determinants, Applications and Opportunities	The work intends to examine the current and upcoming opportunities of the Non-Fungible Tokens (NFTs) market with special emphasis on price factors and application. It looks at the status of the NFT markets and the investors' attitude and expectations towards these products. It offers an overview of, and a comparative analysis of, the financial and econometric models used in literature, about their predictive capabilities, when it comes to valuing NFTs. This paper presents a conceptual model for the analysis of the formation of NFT prices and aims to reveal the value creation drivers behind these assets to explain investors' behavior in the blockchain environment.
[141]	Patents and intellectual property assets as non-fungible tokens; key technologies and challenges	The paper investigates the role of NFTs in intellectual property, which is still a relatively uncharted terrain when it comes to NFTs as opposed to digital art, video games and collectibles. However, with the rapid development of tokenization and DeFi, through the token-like and non-tangible characteristics, NFTs have a chance to enhance the transparency and marketability of the intangible asset like patent. As part of the research, they proposed a conceptual framework of patents as NFTs and elaborated on the filing specifications for intellectual property assets as NFTs. Furthermore, it identifies the new issues as well as future considerations towards NFT-based patents that contain the foundation and the direction to companies for employing this technology in problems such as patenting, financing, and biotechnology.
[142]	A Review of Non-fungible Tokens Applications in the Real-world and Metaverse	The research delves into the rise in popularity of Non-Fungible Tokens (NFT) which were first introduced in 2017 utilizing blockchain technology and are now being increasingly utilized in both commercial and scholarly investigations. The paper examines the existing uses of NFT and delves into their possibilities within the Metaverse. A blockchain technology that facilitates interactions with digital personas in a virtual realm. It elaborates on how NFT can enhance identity management and rights to ownership of assets within the Metaverse while also suggesting potential future applications, in research and industry.

[143]	Non-Fungible Tokens (NFT): New Emerging Digital Asset	The article delves into the expanding realm of Non-Fungible Tokens (NFT) which has seen growth in recent years. The concept originated from Ethereum. Allows for the creation of tokens with distinctive digital attributes tied to factors like age rarity and liquidity. As of May 2021, NFT sales have surpassed $34 million in value, capturing global interest for their lucrative investment potential. However, the NFT landscape is still nascent with technological advancements and a need for comprehensive assessments. This document offers a look at NFT ecosystems covering new approaches and potential risks and rewards as well as technical elements like protocols and standards that are important features to consider in this space of digital assets. It also includes an evaluation of safety measures and explores design concepts along with the opportunities and hurdles involved in the NFT ecosystem. Marking it as a pioneering analysis, in this field.

4. Discussion

In analyzing the presented articles, several key contributions and areas of interest for future research in the field of digital content protection and data integrity using emerging technologies like blockchain were identified. The following discussion covers the results and challenges posed by the selected articles:

4.1. Integration of Hardware Security Modules (HSM) and Blockchain

This development in industrial-IoT domain from a security point of view is remarkable when HSM, along with blockchain technology, are integrated. This hardware-based root-of-trust is vital to protect against physical tampering and unauthorized access to critical systems, rendering an HSM essential for any organization currently [70]. When it comes to blockchain, HSMs are key management elements that enable the best encryption processes possible, improving the overall security architecture. This combination is particularly attractive in situations where the safekeeping of sensitive data is paramount, such as academic records management and certification processes in educational institutions [123]. However, interoperability and standard decryption require extensive overhead for multiple HSMs, as do hundreds of different blockchains. Future research should explore how standardized HSM-enabled blockchain solutions could enhance the integrity of academic credentials and digital rights in education.

4.2. Blockchain-Based Digital Rights Management (DRM)

The main advantages of using blockchain technology in DRM can be understood if one examines the shortcomings of traditional DRM systems which can indeed be centralized and nontransparent [95]. The presented solution of utilizing blockchain ensures the possibility of effectively providing information on copyrights and transactions in an unchangeable while being transparent to all parties interested in the process. The use of smart contracts makes the process of enforcing the rights concerning the copyright terms as well as the issue of licenses efficient in the elimination of the need for a central server and control and the associated issues with hacking and unauthorized access [114]. Despite such benefits, there are certain problems that arise during the shift to blockchain-based DRM systems: compliance with existing models of DRM; the problem of the blockchain’s ability to perform at varying scales; and the problem of developing an intuitive interaction with the system. However, there is a crucial lack that requires the definition of new legal concepts and subsequent regulation, adequate for blockchain application to DRM. Further research should be focused on evaluating the feasibility of employing such methods, identifying the scalability solutions for implementing blockchain DRM systems on a large scale and determining the legal requirements, which would enable large scale implementation of such systems in the global market [136].

4.3. Information-Sharing Platforms in the Scientific Community

Introducing the blockchain into the scientific community is in line with the solution to secure data sharing [37]. Conventional processes of exchanging data typically involve the help of a third party, and this can negatively affect the levels of trust, openness, and data quality. Blockchain, alongside such technologies as InterPlanetary File System (IPFS), forms a decentralized structure that increases data protection and makes records' updates irreversible [45]. This is especially the case in the published literature, especially in the scientific literature where the data generated must be accurate and reproducible. The proposed blockchain-based platforms enhance the security of data sharing where smart contracts are used for the management of the access control and the data sharing agreement [58]. They are as follows; The scalability of the data, the expensive cost of storage in blockchain, and the questions on how to incorporate these technologies in research. It is recommended that future studies investigate the main methods of addressing such challenges such as efficient data management, low transaction costs and improved application of blockchain technology and systems to researchers.

4.4. Use of Non-Fungible Tokens (NFTs) in the Art Market.

The application of NFT in the art market is a new way of establishing the identity and ownership of the digital art [92]. Through incorporation of blockchain, NFT confirms that a certain piece of content is original and unique. It could significantly disrupt the conventional art market since it will create new income sources for artists and the collectors will have more revenue to ensure that the works they are purchasing are original. Various challenges persist with the market for NFTs, including floppiness of the current market, effects on blockchains' energy use, and little research on the economic effects of NFTs in the art market [104]. Thirdly, it is for better and more efficient regulations of NFT there must be certain practices and legislation that could guarantee more safety to the artists, collectors and investors as well. More studies should be conducted as to the future viability of NFTs, standard guidelines for their application, the social and ecological impact of the blockchain in the art economy, and regarding environmental and regulatory concerns of blockchain and NFT [139].

4.5. Education and Digital Competencies.

This can be attributed to the fact that there seems to have been an increased rate of digitization across industries including those in the higher learning institutions' areas of interest such as accounting and finance [34]. Since digital technologies as blockchain are gradually integrating into these fields, the graduates need to be ready to operate in this environment. This comprises skills in the management of content in digital environments, distributed records in the blockchain, and autonomous decentralized systems of P2P nodes. Nonetheless, the current curricula offer a mismatch of the skills students are prepared for and the real-world expectations today [105]. Furthermore, many educators who are directly involved with teaching their students may not possess the know-how to teach the new technologies. To fill these gaps, the future research should aim at designing more extensive teacher training programmers, designing segmented and flexible curriculum models, and incorporating the processes in which learners integrate deals with technologies in their curricular learning activities. This will not only equip students with knowledge on how to handle situations in an economy with prominent applications of the internet and technology but also enable educational institutions to remain relevant in a fast-changing world [132].

4.6. Addressing Implementation Challenges in Blockchain and NFTs for Academic Integrity.

Despite the transformative potential of Blockchain and NFTs in securing academic intellectual property, several **challenges hinder large-scale adoption** in university environments. To overcome these barriers, **targeted mitigation strategies** must be developed to ensure seamless integration, usability, and regulatory compliance.

1. **Institutional Integration and Scalability Solutions:** One of the primary concerns is the technical complexity involved in integrating Blockchain with existing Learning Management Systems (LMS) and institutional repositories. To facilitate this process, hybrid architectures combining off-chain storage (e.g., IPFS) with on-chain verification can optimize performance while maintaining decentralization. Additionally, permissioned blockchains offer a scalable alternative, allowing universities to control access while benefiting from Blockchain's security features.
2. **Enhancing Adoption through User-Centered Design:** For Blockchain and NFTs to gain traction in academia, ease of use is critical. Implementing intuitive user interfaces within university portals will lower the barrier for faculty and students. Moreover, comprehensive training programs should be introduced to familiarize users with Blockchain-based certification systems. Gamification strategies, such as rewarding students with NFT-based certifications for academic achievements, can also boost engagement and drive widespread adoption.

5. Conclusions

This review aimed to analyze the status and implementation of Blockchain and NFT technologies in protecting the authenticity and intellectual property of source code within academic environments. Through a systematic examination of over 100 recent articles, this study has identified key advancements, persistent challenges, and future directions in the integration of these technologies. Over the past five years, academic interest in Blockchain and NFTs has increased steadily, particularly in areas related to security, digital certification methods, and code integrity.

The growing relevance of Blockchain and NFTs in ensuring the authenticity and ownership of software developments in academia is evident in the reviewed literature. The number of related publications has risen consistently since 2018, with notable peaks in 2021 and 2023. Most studies emphasize the need for enhanced security measures, highlighting Blockchain's potential to ensure software traceability and integrity, while NFTs offer a unique capability to create immutable digital certificates for intellectual property protection.

However, several unresolved challenges remain, including scalability, efficiency, cost, integration complexity, quantum resistance, and the balance between centralization and decentralization. Addressing these issues is essential for fully unlocking the potential of Blockchain and NFTs in academic applications. Nevertheless, the reviewed studies propose various techniques and architectural improvements to mitigate these limitations, including advances in cryptographic methods, the integration of both on-chain and off-chain solutions, the use of Trusted Execution Environments (TEEs), and decentralized file storage solutions. Further research is required to optimize the trade-offs between scalability, efficiency, security, and privacy in Blockchain-based academic systems.

This review serves as a foundation for academics and practitioners seeking to advance the secure adoption of Blockchain and NFTs in educational environments. By summarizing both the progress made and the existing gaps, this study provides a basis for future research efforts in this evolving field. While these technologies present promising opportunities, additional studies are needed to develop practical solutions for secure, decentralized, and efficient systems that protect the intellectual property of software developments in academia. In this regard, this review establishes a reference point for further exploration, guiding future efforts toward meaningful integration and advancement in intellectual property protection and digital content integrity within academic institutions.

In conclusion, these technologies have promising possibilities in integration but there is still potential for further studies, which will make possible the formation of the practical solutions for providing the secure decentralized and efficient systems for managing and protecting the intellectual property of the software developments in academia. In this way, this review establishes the base and a starting point to proceed in this new field. In this paper, the current situation on the integration of Blockchain and NFTs has been described based on the literature available in the current world. Thus, in these conclusions, to identify the most significant emerging limitations, gaps as well as the more significant progress, we have also relied on the findings in the relevant articles as highlighted above. These conclusions are not meant to suggest specific solutions to the problems which have been identified; rather, these conclusions are meant to serve as a roadmap to help progress toward change and meaningful integration into the practices of intellectual property protection and authenticity of software developments in academic organizations.

Author Contributions: This review study has the following individual contributions: Methodology, L.J.R.L.; Software, L.J.R.L. and G.G.M.L.; Validation, L.J.R.L.; Resources, L.J.R.L.; Formal analysis, G.G.M.L.; Data curation, G.G.M.L.; Writing—review and editing, L.J.R.L. and G.G.M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: The authors acknowledge Universidad El Bosque for support to research project code AUX-2024-01-04, and access to scientific databases.

Conflicts of Interest: The authors declare that there is no conflict of interest.

References

1. K. Chiba and H. Ito, “Sublinear Computation Paradigm: Constant-Time Algorithms and Sublinear Progressive Algorithms,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 105, no. 3, 2022, doi: 10.1587/transfun.2021EAI0003.
2. M. Saimon, Z. Lavicza, and T. (Noah) Dana-Picard, “Enhancing the 4Cs among college students of a communication skills course in Tanzania through a project-based learning model,” Education and Information Technologies, vol. 28, no. 6, 2023, doi: 10.1007/s10639-022-11406-9.
3. S. Han, S. Nikou, and W. Yilma Ayele, “Digital proctoring in higher education: a systematic literature review,” International Journal of Educational Management, vol. 38, no. 1. 2024. doi: 10.1108/IJEM-12-2022-0522.
4. MIT, "MIT Libraries: Copyright and Licensing," MIT, 2023. [Online]. Available: https://libraries.mit.edu/copyright/. [Accessed: 14-Aug-2024].
5. Stanford University, "Software Intellectual Property," Stanford, 2022. [Online]. Available: https://stanford.edu/software-ip/. [Accessed: 14-Aug-2024].
6. Harvard University, "Research Data Security," Harvard, 2023. [Online]. Available: https://harvard.edu/research-security/. [Accessed: 14-Aug-2024].
7. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms, 3rd ed. Cambridge, MA: MIT Press, 2009.
8. MIT, "Source Code Definition," MIT, 2023. [Online]. Available: https://mit.edu/source-code-definition/. [Accessed: 14-Aug-2024].
9. European Union, "Directive 2009/24/EC on the legal protection of computer programs," Official Journal of the European Union, 2009.

10. K. Lee and H. Park, "Copyright and Intellectual Property Law in East Asia," Journal of East Asian Studies, vol. 15, no. 2, pp. 123-135, 2021.
11. Dirección Nacional de Derechos de Autor, "Guía sobre derechos de autor en Colombia," DNDA, 2023. [Online]. Available: https://derechosdeautor.gov.co/guia-derechos-autor/. [Accessed: 14-Aug-2024].
12. R. Stallman, "Open Source Licensing: Ensuring Freedom in Digital Work," Journal of Software Freedom, vol. 7, no. 3, pp. 85-97, 2021.
13. N. I. Kshetri, "Digital Assets: Definition and Protection Strategies," Journal of Digital Economy, vol. 14, no. 1, pp. 25-35, 2023.
14. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 14-Aug-2024].
15. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6-19, 2016.
16. A. Tapscott and D. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World, New York, NY: Penguin Random House, 2018.
17. K. Mougayar, The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology, Hoboken, NJ: John Wiley & Sons, 2016.
18. J. A. Garay and A. Kiayias, "The Blockchain Model of Cryptography and Security," Advances in Cryptology – CRYPTO 2015, vol. 9216, pp. 116-140, 2015.
19. R. A. Hackett, "The Future of Digital Assets: Blockchain and Beyond," Harvard Business Review, vol. 94, no. 5, pp. 45-53, 2022.
20. D. O'Reilly, "NFTs and Intellectual Property," Journal of Blockchain Research, vol. 9, no. 3, pp. 97-108, 2022.
21. A. Alizadeh, "Tokenizing Intellectual Property: The Case for NFTs in Academia," Journal of Digital Asset Management, vol. 18, no. 2, pp. 67-79, 2023.
22. B. Buterin, "Multichain and Interoperability: Future Directions," Ethereum Foundation, 2023. [Online]. Available: https://ethereum.org/multichain-interoperability/. [Accessed: 14-Aug-2024].
23. H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, "Accounting and auditing with blockchain technology and artificial Intelligence: A literature review," International Journal of Accounting Information Systems, vol. 48, p. 100598, Mar. 2023, doi: 10.1016/j.accinf.2022.100598.
24. H. Guo and X. Yu, "A survey on blockchain technology and its security," Blockchain: Research and Applications, vol. 3, no. 2, p. 100067, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.
25. R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," ACM Computing Surveys, vol. 52, no. 3, pp. 1–34, May 2020, doi: 10.1145/3316481.
26. P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, vol. 6, no. 2, pp. 147–156, May 2020, doi: 10.1016/j.dcan.2019.01.005.
27. E. Fernando, M. Meyliana, H. L. H. S. Warnars, and E. Abdurachman, "Blockchain Technology for Tracing Drug with a Multichain Platform: Simulation Method," Advances in Science, Technology and Engineering Systems Journal, vol. 6, no. 1, pp. 765–769, Feb. 2021, doi: 10.25046/aj060184.
28. J. Chang, J. Ni, J. Xiao, X. Dai, and H. Jin, "SynergyChain: A Multichain-Based Data-Sharing Framework With Hierarchical Access Control," IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14767–14778, Aug. 2022, doi: 10.1109/JIOT.2021.3061687.
29. A. Mishra, "Linux Security using Blockchain," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 3, pp. 3776–3782, Jun. 2020, doi: 10.30534/ijatcse/2020/194932020.
30. S. Ismail, H. Reza, H. K. Zadeh, and F. Vasefi, "A Blockchain-based IoT Security Solution Using Multichain," in 2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023, 2023. doi: 10.1109/CCWC57344.2023.10099128.
31. A. Ismailisufi, T. Popovic, N. Gligoric, S. Radonjic, and S. Sandi, "A Private Blockchain Implementation Using Multichain Open Source Platform," in 2020 24th International Conference on Information Technology, IT 2020, 2020. doi: 10.1109/IT48810.2020.9070689.

32. R. A. Koussema and H. Haga, "Highly Secure Residents Life Event Management System Based on Blockchain by Hyperledger Fabric," Journal of Computer and Communications, vol. 09, no. 09, 2021, doi: 10.4236/jcc.2021.99003.
33. Z. Chen, W. Ding, Y. Xu, M. Tian, and H. Zhong, "Fair auctioning and trading framework for cloud virtual machines based on blockchain," Computer Communications, vol. 171, pp. 89–98, Apr. 2021, doi: 10.1016/j.comcom.2021.02.010.
34. D. L. Fekete and A. Kiss, "Toward Building Smart Contract-Based Higher Education Systems Using Zero-Knowledge Ethereum Virtual Machine," Electronics (Switzerland), vol. 12, no. 3, 2023, doi: 10.3390/electronics12030664.
35. M. Zichichi, G. D'Angelo, S. Ferretti, and M. Marzolla, "Accountable Clouds Through Blockchain," IEEE Access, vol. 11, pp. 48358–48374, 2023, doi: 10.1109/ACCESS.2023.3276240.
36. F. Ullah and F. Al-Turjman, "A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities," Neural Computing and Applications, vol. 35, no. 7, pp. 5033–5054, Mar. 2023, doi: 10.1007/s00521-021-05800-6.
37. N. Kumar, V. Goel, R. Ranjan, M. Altuwairiqi, H. Alyami, and S. A. Asakipaam, "A Blockchain-Oriented Framework for Cloud-Assisted System to Countermeasure Phishing for Establishing Secure Smart City," Security and Communication Networks, vol. 2023, pp. 1–13, Apr. 2023, doi: 10.1155/2023/8168075.
38. S. Karagwal, S. Tanwar, S. Badotra, A. Rana, and V. Jain, "Blockchain for Internet of Things (IoT): Research Issues, Challenges, and Future Directions," in EAI/Springer Innovations in Communication and Computing, 2023, pp. 15–34. doi: 10.1007/978-3-031-04524-0_2.
39. J. Panduro-Ramirez, M. Lourens, A. Gehlot, D. P. Singh, Y. Singh, and D. J. Salunke, "Blockchain Approach for Implementing Access Control In IOT," in 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), IEEE, Jan. 2023, pp. 596–599. doi: 10.1109/AISC56616.2023.10085452.
40. H. Xu, W. Liu, and X. Liu, "Blockchain-Based Trust Auction for Dynamic Virtual Machine Provisioning and Allocation in Clouds," Wireless Communications and Mobile Computing, vol. 2021, pp. 1–10, Jun. 2021, doi: 10.1155/2021/6639107.
41. S. Wang et al., "Blockchain Smart Contract Virtual Machine Optimization Technology for Domain Name Systems," in 2021 IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI), IEEE, Dec. 2021, pp. 445–451. doi: 10.1109/IAAI54625.2021.9699960.
42. S. Basu, S. Karmakar, and D. Bera, "Blockchain based secured virtual machine image monitor," in ICISSP 2021 - Proceedings of the 7th International Conference on Information Systems Security and Privacy, 2021.
43. A. Mishra, S. Karmakar, A. Dutta, A. Bose, and M. Mohapatro, "Design and Deployment of IoT enabled Blockchain based resilient Supply-chain Management System using Ethereum," International Journal of Computing and Digital Systems, vol. 12, no. 4, pp. 1029–1050, Oct. 2022, doi: 10.12785/ijcds/120183.
44. V. Tanwar and K. R. Ramkumar, "An Analysis of Blockchain and NFT Technologies and their Drawbacks," in 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), IEEE, May 2023, pp. 1251–1259. doi: 10.1109/ICAAIC56838.2023.10140828.
45. L. Wu, W. Lu, Z. Peng, and C. Webster, "A blockchain non-fungible token-enabled 'passport' for construction waste material cross-jurisdictional trading," Automation in Construction, vol. 149, p. 104783, May 2023, doi: 10.1016/j.autcon.2023.104783.
46. C. G. Kim, "A Study on Technology to Counter Copyright Infringement According to NFT Transaction Types," Journal of the Semiconductor & Display Technology, vol. 20, no. 4, 2021.
47. H. Takahashi and U. Lakhani, "Voting blockchain for High Security NFT," in 2021 IEEE 10th Global Conference on Consumer Electronics, GCCE 2021, 2021. doi: 10.1109/GCCE53005.2021.9621968.
48. M. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "A Decentralized Framework for Patents and Intellectual Property as NFT in Blockchain Networks," Computational Mathematics and Theoretical Computer Science, 2021, doi: 10.21203/rs.3.rs-951089.
49. L. Ante, "Non-fungible token (NFT) markets on the Ethereum blockchain: Temporal development, cointegration and interrelations," SSRN Electronic Journal, 2021, doi: 10.2139/ssrn.3904683.}
50. Q. Rui, L. Juanjuan, W. Xiao, Z. Jing, Y. Yong, and W. Fei-Yue, "NFT: blockchain-based non-fungible token and applications," Chinese Journal of Intelligent Science and Technology, vol. 3, no. 2, 2021.

51. R. Qin, J. Li, X. Wang, J. Zhu, Y. Yuan, and F. Y. Wang, "NFT: blockchain-based non-fungible token and applications," Chinese Journal of Intelligent Science and Technology, vol. 3, no. 2, 2021, doi: 10.11959/j.issn.2096-6652.202125.
52. L. Ante, "The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum," SSRN Electronic Journal, 2021, doi: 10.2139/ssrn.3861106.
53. D. R. Zagidullin and N. S. Pulyavina, "The prospects for the development of blockchain technology in the NFT format," Lizing (Leasing), no. 1, pp. 40–44, May 2021, doi: 10.33920/VNE-03-2107-06.
54. K. Mentzer, J. Price, E. Powers, and N. Lavrenchuk, "EXAMINING THE HYPE BEHIND THE BLOCKCHAIN NFT MARKET," Issues In Information Systems, vol. 23, no. 4, 2022, doi: 10.48009/4_iis_2022_102.
55. J. Bellagarda and A. M. Abu-Mahfouz, "Connect2NFT: A Web-Based, Blockchain Enabled NFT Application with the Aim of Reducing Fraud and Ensuring Authenticated Social, Non-Human Verified Digital Identity," Mathematics, vol. 10, no. 21, p. 3934, Oct. 2022, doi: 10.3390/math10213934.
56. M. Rasolroveicy and M. Fokaefs, "Performance and Cost Evaluation of Public Blockchain: An NFT Marketplace Case Study," in 2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), IEEE, Sep. 2022, pp. 79–86. doi: 10.1109/BRAINS55737.2022.9908999.
57. L. Sun, X. F. Li, H. Zhao, B. Yu, T. Zhou, and X. R. Li, "NFT-based method for assetization of physical assets on blockchain," Zhejiang Daxue Xuebao (Gongxue Ban)/Journal of Zhejiang University (Engineering Science), vol. 56, no. 10, 2022, doi: 10.3785/j.issn.1008-973X.2022.10.002.
58. I. Journal, "Non-Fungible Tokens (NFT). The Analysis of Risk and Return," INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, vol. 06, no. 06, Jun. 2022, doi: 10.55041/IJSREM14188.
59. K. B. Wilson, A. Karg, and H. Ghaderi, "Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity," Business Horizons, vol. 65, no. 5, pp. 657–670, Sep. 2022, doi: 10.1016/j.bushor.2021.10.007.
60. Y. Rudytsia and N. Bogdanova, "UML MODEL OF THE PROPERTY RIGHT DISTRIBUTION MODULE USING NFT FRACTIONALIZATION BASED ON BLOCKCHAIN TECHNOLOGY," International Science Journal of Engineering & Agriculture, vol. 1, no. 3, pp. 98–109, Aug. 2022, doi: 10.46299/j.isjea.20220103.8.
61. K. H. Gia et al., "Delivery Management System based on Blockchain, Smart Contracts and NFT: A Case Study in Vietnam," International Journal of Advanced Computer Science and Applications, vol. 14, no. 1, 2023, doi: 10.14569/IJACSA.2023.01401100.
62. P. Li, "The Application of Blockchain and Cryptocurrency in Meta-universe and NFT," BCP Business & Management, vol. 44, pp. 55–61, Apr. 2023, doi: 10.54691/bcpbm.v44i.4793.
63. M. K. Hari, A. Agrawal, R. Bhatia, A. Bhatia, and K. Tiwari, "T-PASS: A Blockchain-based NFT Enabled Property Management and Exchange System," in 2023 International Conference on Information Networking (ICOIN), IEEE, Jan. 2023, pp. 140–145. doi: 10.1109/ICOIN56518.2023.10048973.
64. C. Chen, H. Huang, B. Zhao, D. Shu, and Y. Wang, "The Research of AHP-Based Credit Rating System on a Blockchain Application," Electronics (Switzerland), vol. 12, no. 4, 2023, doi: 10.3390/electronics12040887.
65. H. Taherdoost, "Non-Fungible Tokens (NFT): A Systematic Review," Information (Switzerland), vol. 14, no. 1. 2023. doi: 10.3390/info14010026.
66. K. Ko, T. Jeong, J. Woo, and J. W. Hong, "Survey on blockchain-based non-fungible tokens: History, technologies, standards, and open challenges," International Journal of Network Management, vol. 34, no. 1, Jan. 2024, doi: 10.1002/nem.2245.
67. A. Manzoor, M. Samarin, D. Mason, and M. Ylianttila, "Scavenger hunt: Utilization of blockchain and iot for a location-based game," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3037182.
68. S. Hong, Y. Noh, J. Hwang, and C. Park, "Fabasset: Unique digital asset management system for hyperledger fabric," in Proceedings - International Conference on Distributed Computing Systems, 2020. doi: 10.1109/ICDCS47774.2020.00163.
69. D. Uribe, G. Waters, and G. Io, "Privacy Laws, Genomic Data and Non-Fungible Tokens," The Journal of The British Blockchain Association, vol. 3, no. 2, 2020.

70. J. Arcenegui, R. Arjona, and I. Baturone, "Secure Management of IoT Devices Based on Blockchain Non-fungible Tokens and Physical Unclonable Functions," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 12418 LNCS, 2020, pp. 24–40. doi: 10.1007/978-3-030-61638-0_2.
71. O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," IEEE Internet of Things Journal, vol. 8, no. 12, 2021, doi: 10.1109/JIOT.2020.2996590.
72. C. Liu, X. Zhang, K. K. Chai, J. Loo, and Y. Chen, "A survey on blockchain-enabled smart grids: Advances, applications and challenges," IET Smart Cities, vol. 3, no. 2, pp. 56–78, Jun. 2021, doi: 10.1049/smc2.12010.
73. N. Jing, Q. Liu, and V. Sugumaran, "A blockchain-based code copyright management system," Information Processing & Management, vol. 58, no. 3, p. 102518, May 2021, doi: 10.1016/j.ipm.2021.102518.
74. Md. M. Islam and H. P. In, "Decentralized Global Copyright System Based on Consortium Blockchain With Proof of Authority," IEEE Access, vol. 11, pp. 43101–43115, 2023, doi: 10.1109/ACCESS.2023.3270627.
75. X. Wen, "Application of blockchain technology in copyright protection of digital music information," International Journal of Grid and Utility Computing, vol. 14, no. 2/3, p. 136, 2023, doi: 10.1504/IJGUC.2023.131015.
76. A. Kumar, A. Gupta, L. M. Sanagavarapu, and Y. R. Reddy, "An approach to open-source software license management using blockchain-based smart-contracts," in ACM International Conference Proceeding Series, 2022. doi: 10.1145/3511430.3511448.
77. W. Liang, D. Zhang, X. Lei, M. Tang, K. C. Li, and A. Y. Zomaya, "Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection," IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, 2021, doi: 10.1109/TETC.2020.2993032.
78. X. Chen, A. Yang, J. Weng, Y. Tong, C. Huang, and T. Li, "A Blockchain-Based Copyright Protection Scheme With Proactive Defense," IEEE Transactions on Services Computing, vol. 16, no. 4, 2023, doi: 10.1109/TSC.2023.3246476.
79. Z. Cai, "Usage of deep learning and blockchain in compilation and copyright protection of digital music," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3021523.
80. L. Luo, "Application of Blockchain Technology in Intellectual Property Protection," Mathematical Problems in Engineering, vol. 2022, 2022, doi: 10.1155/2022/4641559.
81. A. Qureshi and D. M. Jiménez, "Blockchain-based multimedia content protection: Review and open challenges," Applied Sciences (Switzerland), vol. 11, no. 1. 2021. doi: 10.3390/app11010001.
82. J. Guo, H. Zhou, L. Yang, and X. Chen, "Research on digital copyright blockchain technology," in Proceedings - 2020 3rd International Conference on Smart BlockChain, SmartBlock 2020, 2020. doi: 10.1109/SmartBlock52591.2020.00028.
83. G. Falco and J. E. Siegel, "Assuring automotive data and software integrity employing distributed hash tables and blockchain: A Preprint," arXiv. 2020.
84. A. Savelyev, "Copyright in the blockchain era: Promises and challenges," Computer Law and Security Review, vol. 34, no. 3, 2018, doi: 10.1016/j.clsr.2017.11.008.
85. A. Litchfield and J. Herbert, "Resolv: Applying cryptocurrency blockchain methods to enable global cross-platform software license validation," Cryptography, vol. 2, no. 2, 2018, doi: 10.3390/cryptography2020010.
86. J. Herbert and A. Litchfield, "A novel method for Decentralised Peer-to-Peer software license validation using cryptocurrency blockchain technology," in Conferences in Research and Practice in Information Technology Series, 2015.
87. W. Yang, P. He, Z. Yang, X. Yi, and C. Chen, "Digital Copyright Depository System Enhanced by Blockchain," in Proceedings - 2020 International Conference on Culture-Oriented Science and Technology, ICCST 2020, 2020. doi: 10.1109/ICCST50977.2020.00044.
88. Manish Verma, "The Study on Blockchain Based Library Management and its Characterization," International Journal of Trend in Scientific Research and Development, vol. 5, no. 3, 2021.
89. A. Kaushik and M. Malik, "Securing the transfer and controlling the piracy of digital files using Blockchain," in Proceedings - 2022 5th International Conference on Computational Intelligence and Communication Technologies, CCICT 2022, 2022. doi: 10.1109/CCiCT56684.2022.00066.

90. G. Lee, “Legal Issues Related to Blockchain Technology—Examples from Korea,” in Perspectives in Law, Business and Innovation, 2020. doi: 10.1007/978-981-15-1350-3_9.
91. T. Igarashi, T. Kazuhiko, Y. Kobayashi, H. Kuno, and E. Diehl, “Photrace: A Blockchain-Based Traceability System for Photographs on the Internet,” in Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021, 2021. doi: 10.1109/Blockchain53845.2021.00089.
92. D. P. A. D. Rafli, “NFT Become a Copyright Solution,” Journal of Digital Law and Policy, vol. 1, no. 2, 2022, doi: 10.58982/jdlp.v1i2.166.
93. C. Chen, Y. Li, Z. Wu, M. Xu, R. Wang, and Z. Zheng, “Towards Reliable Utilization of AIGC: Blockchain-Empowered Ownership Verification Mechanism,” IEEE Open Journal of the Computer Society, vol. 4, 2023, doi: 10.1109/OJCS.2023.3315835.
94. E. Ferro et al., “Digital assets rights management through smart legal contracts and smart contracts,” Blockchain: Research and Applications, vol. 4, no. 3, 2023, doi: 10.1016/j.bcra.2023.100142.
95. Z. Ma, W. Huang, and H. Gao, “Secure DRM scheme based on blockchain with high credibility,” Chinese Journal of Electronics, vol. 27, no. 5, 2018, doi: 10.1049/cje.2018.07.003.
96. Z. Song, Z. Yu, W. Shang, and Y. X. Li, “A Digital Copyright Protection Method Based on Blockchain,” in Communications in Computer and Information Science, 2021. doi: 10.1007/978-981-16-7993-3_38.
97. S. Y. A. Zaidi et al., “An attribute-based access control for IoT using blockchain and smart contracts,” Sustainability (Switzerland), vol. 13, no. 19, 2021, doi: 10.3390/su131910556.
98. P. Patil, M. Sangeetha, and V. Bhaskar, “Blockchain for IoT Access Control, Security and Privacy: A Review,” Wireless Personal Communications, vol. 117, no. 3. 2021. doi: 10.1007/s11277-020-07947-2.
99. A. K. Shrestha, R. Deters, and J. Vassileva, “User-controlled privacy-preserving user profile data sharing based on blockchain,” arXiv. 2019.
100. A. Raj, A. Kumar, V. Sharma, S. Rani, and A. K. Shanu, “Enhancing Security Feature in Financial Transactions using Multichain Based Blockchain Technology,” in 4th International Conference on Intelligent Engineering and Management, ICIEM 2023, 2023. doi: 10.1109/ICIEM59379.2023.10166589.
101. R. Amirta, M. S. Deepika, and R. G. Franklin, “Decentralized access control with anonymous authentication of data stored using blockchain,” Research Journal of Engineering and Technology, vol. 11, no. 1, 2020, doi: 10.5958/2321-581x.2020.00002.1.
102. S. Hu, “Improved Private Data Protection Scheme for Blockchain Smart Contracts,” International Journal of Distributed Sensor Networks, vol. 2023, 2023, doi: 10.1155/2023/5963039.
103. Y. Yi, “Application of Blockchain Technology Based on Privacy Data Protection in RMB Internationalization Path,” Mobile Information Systems, vol. 2022, 2022, doi: 10.1155/2022/1904593.
104. X. Li, Q. Luo, X. Yang, N. Luo, D. Xu, and C. Sun, “Design and Implementation of Blockchain Hierarchical Supervision Model for Wheat Supply Chain,” Nongye Jixie Xuebao/Transactions of the Chinese Society for Agricultural Machinery, vol. 54, no. 3, 2023, doi: 10.6041/j.issn.1000-1298.2023.03.037.
105. D. N. Prata, H. X. de Araújo, and C. Santos, “Blockchain Technology applied to Education,” International Journal of Advanced Engineering Research and Science, vol. 6, no. 7, 2019, doi: 10.22161/ijaers.6736.
106. A. Sawant, N. Prabhu, and S. Nagpure, “Securing IoT Using MultiChain,” SSRN Electronic Journal, 2019, doi: 10.2139/ssrn.3370759.
107. Meyliana et al., “Blockchain technology for vehicle maintenance registration,” in Proceedings of 2021 International Conference on Information Management and Technology, ICIMTech 2021, 2021. doi: 10.1109/ICIMTech53080.2021.9534974.
108. N. B. L. V. Prasad, M. N. A. Pramodh, R. V. S. Lalitha, K. Kavitha, and K. Saritha, “Tracking Industrial Assets Using Blockchain Technology,” in Lecture Notes in Electrical Engineering, 2022. doi: 10.1007/978-981-16-9885-9_16.
109. I. Riabi, H. K. ben Ayed, B. Zaghdoudi, and L. George, “Blockchain based OAuth for IoT,” in 2021 10th IFIP International Conference on Performance Evaluation and Modeling in Wireless and Wired Networks, PEMWN 2021, 2021. doi: 10.23919/PEMWN53042.2021.9664701.
110. S. Barbosa, R. Butler, and C. Pettey, “A MultiChain-Based Homework Submission System,” in Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017, 2018. doi: 10.1109/CSCI.2017.185.

111. M. Naz et al., "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," Sustainability (Switzerland), vol. 11, no. 24, 2019, doi: 10.3390/su11247054.
112. D. Chun, "When the NFT Hype Settles, What Is Left beyond Profile Pictures? A Critical Review on the Impact of Blockchain Technologies in the Art Market," Arts, vol. 12, no. 5, 2023, doi: 10.3390/arts12050181.
113. C. Núñez-Gómez and V. Garcia-Font, "HyperNet: A conditional k-anonymous and censorship resistant decentralized hypermedia architecture," Expert Systems with Applications, vol. 208, 2022, doi: 10.1016/j.eswa.2022.118079.
114. Z. Zhang and L. Zhao, "A design of digital rights management mechanism based on blockchain technology," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018. doi: 10.1007/978-3-319-94478-4_3.
115. S. Muthaiyah, K. Phang, and S. Sembakutti, "Bridging skill gaps and creating future ready accounting and finance graduates: An exploratory study," F1000Research, vol. 10, 2021, doi: 10.12688/f1000research.72880.1.
116. S. Riaz, A. Mushtaq, and H. Ibrar, "Content Generation in Web 3.0 and Blockchain-Based Decentralized Social Networks: A Theoretical Adoption Framework," in IEEE Region 10 Annual International Conference, Proceedings/TENCON, 2022. doi: 10.1109/TENCON55691.2022.9977762.
117. K. Kimura, M. Imamura, and K. Omote, "Cross-Referencing Scheme to Ensure NFT and Platform Linkage Unaffected by Forking," in 2023 IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2023, 2023. doi: 10.1109/ICBC56567.2023.10174994.
118. F. A. Reegu et al., "Systematic Assessment of the Interoperability Requirements and Challenges of Secure Blockchain-Based Electronic Health Records," Security and Communication Networks, vol. 2022, 2022, doi: 10.1155/2022/1953723.
119. S. K. Lo, M. Staples, and X. Xu, "Modelling schemes for multi-party blockchain-based systems to support integrity analysis," Blockchain: Research and Applications, vol. 2, no. 2, 2021, doi: 10.1016/j.bcra.2021.100024.
120. Y. S. Bae et al., "Development of Blockchain-Based Health Information Exchange Platform Using HL7 FHIR Standards: Usability Test," IEEE Access, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3194159.
121. F. A. Reegu et al., "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," Sustainability (Switzerland), vol. 15, no. 8, 2023, doi: 10.3390/su15086337.
122. A. Grech, I. Sood, and L. Ariño, "Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education," Frontiers in Blockchain, vol. 4, 2021, doi: 10.3389/fbloc.2021.616779.
123. A. J. Cabrera-Gutierrez, E. Castillo, A. Escobar-Molero, J. A. Alvarez-Bermejo, D. P. Morales, and L. Parrilla, "Integration of Hardware Security Modules and Permissioned Blockchain in Industrial IoT Networks," IEEE Access, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3217815.
124. Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," Human-centric Computing and Information Sciences, vol. 10, no. 1, 2020, doi: 10.1186/s13673-020-0214-5.
125. A. Cantu, J. Geng, and C. Rong, "NFT as a proof of Digital Ownership-reward system integrated to a Secure Distributed Computing Blockchain Framework," in Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, 2022. doi: 10.1109/CloudCom55334.2022.00024.
126. R. Lendo, A. Jacobus, and H. A. Mapaly, "Rancang Bangun Aplikasi Perpustakaan Digital Berbasis Mobile Menggunakan Framework Flutter," Jurnal Teknik Informatika, vol. 18, no. 1, 2023, doi: 10.35793/jti.v18i1.50490.
127. A. C. Moreaux and M. P. Mitrea, "Royalty-Friendly Digital Asset Exchanges on Blockchains," IEEE Access, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3283153.
128. E. Giannatou, G. M. Campagnolo, M. Franklin, J. K. Stewart, and R. Williams, "Revolution postponed? Tracing the development and limitations of open content filmmaking," Information Communication and Society, vol. 22, no. 12, 2019, doi: 10.1080/1369118X.2018.1464590.
129. A. Cheung and J. Keung, "On the Scrutinization of the NFT Valuation Factors," in Proceedings - Asia-Pacific Software Engineering Conference, APSEC, 2022. doi: 10.1109/APSEC57359.2022.00082.

130. O. Kucheryaviy, "System of professional-digital competencies of a teacher ofahigher pedagogical educational institution," ScienceRise: Pedagogical Education, no. 2(47), 2022, doi: 10.15587/2519-4984.2022.255072.
131. M. Casillo, F. Colace, B. B. Gupta, A. Lorusso, F. Marongiu, and D. Santaniello, "Blockchain and NFT: a novel approach to support BIM and Architectural Design," in 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT 2022, 2022. doi: 10.1109/3ICT56508.2022.9990815.
132. B. Luan, "On the inheritance of national music culture in colleges and universities and the reform and innovation of music education in colleges and universities under block-chain technology," in ACM International Conference Proceeding Series, 2021. doi: 10.1145/3482632.3482984.
133. R. Almajed, A. Z. Abualkishik, A. Ibrahim, and N. Mourad, "Forecasting NFT Prices on Web3 Blockchain Using Machine Learning to Provide SAAS NFT Collectors," Fusion: Practice and Applications, vol. 10, no. 2, 2023, doi: 10.54216/FPA.100205.
134. L. Elena Agudelo-Gonzalez, C. Marta-Lazo, and I. Aguaded, "Digital Competencies in the Journalism Curriculum: Case Analysis of a Central American University," Vivat Academia, no. 155, 2022.
135. M. Dowling, "Is non-fungible token pricing driven by cryptocurrencies?," Finance Research Letters, vol. 44, 2022, doi: 10.1016/j.frl.2021.102097.
136. A. Mwanzu, "Perceptions of Librarians on the Usefulness of DRM Technology in Protecting against Copyright Violation," Library Philosophy and Practice, vol. 2021, 2021.
137. E. Sung, O. Kwon, and K. Sohn, "NFT luxury brand marketing in the metaverse: Leveraging blockchain-certified NFTs to drive consumer behavior," Psychology and Marketing, vol. 40, no. 11, 2023, doi: 10.1002/mar.21854.
138. G. F. Ruchkina and D. N. Ermakov, "Analysis of foreign experience in the regulatory framework of distributed ledgers and ico (Initial coin offering) within innovative economy," Humanities and Social Sciences Reviews, vol. 7, no. 4, 2019, doi: 10.18510/hssr.2019.74121.
139. R. Kräussl and A. Tugnetti, "Non-Fungible Tokens (NFTs): A Review of Pricing Determinants, Applications and Opportunities," Journal of Economic Surveys, vol. 38, no. 2, 2024, doi: 10.1111/joes.12597.
140. N. Kholiavko, O. Popelo, I. Bazhenkov, I. Shaposhnykova, and O. Sheremet, "Information and Communication Technologies As a Tool of Strategy for Ensuring the Higher Education Adaptability To the Digital Economy Challenges," International Journal of Computer Science and Network Security, vol. 21, no. 8, 2021.
141. S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "Patents and intellectual property assets as non-fungible tokens; key technologies and challenges," Scientific Reports, vol. 12, no. 1, 2022, doi: 10.1038/s41598-022-05920-6.
142. S. B. Far, S. M. H. Bamakan, Q. Qu, and Q. Jiang, "A Review of Non-fungible Tokens Applications in the Real-world and Metaverse," in Procedia Computer Science, 2022. doi: 10.1016/j.procs.2022.11.238.
143. A. Dev, K. Shaji Gomez, and S. V. Mathew, "Non-Fungible Tokens (NFT): New Emerging Digital Asset," International Journal of Research in Engineering and Science (IJRES) ISSN, vol. 10, no. 4, 2022.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.