Metaverse Basic and Applied Research. 2024; 3:.108
doi: 10.56294/mr2024.108

REVIEW

Technological convergence in the metaverse: challenges and solutions from blockchain, AI, and digital rights

Convergencia tecnológica en el metaverso: desafíos y soluciones desde la blockchain, la IA y los derechos digitales

José Humberto Puente[1], Gerardo Contreras-Piña[2]

[1]Independet investigator. Maturín, Monagas, Venezuela.
[2]Universidad Instituto Técnico en Ciencias Computacionales de Reynosa A.C. Reynosa, Tamaulipas, México.

Cite as: Puente JH, Contreras-Piña G. Technological convergence in the metaverse: challenges and solutions from blockchain, AI, and digital rights. Metaverse Basic and Applied Research. 2024; 3:.108. https://doi.org/10.56294/mr2024.108

Submitted: 22-01-2024 **Revised:** 12-06-2024 **Accepted:** 22-09-2024 **Published:** 23-09-2024

Editor: Yailen Martínez Jiménez

Corresponding author: José Humberto Puente

ABSTRACT

Introduction: the convergence of blockchain, the metaverse, and artificial intelligence (AI) has generated significant transformations in the management of privacy, security, intellectual property, and freedom of expression in digital environments. This research explored the technical, legal, and ethical implications arising from this technological interaction.
Method: a systematic review of scientific literature published between 2022 and 2024 was conducted, selecting 35 studies indexed in databases such as IEEE Xplore, Scopus, and arXiv. A qualitative-quantitative approach was applied to categorize findings into comparative matrices and analyze patterns, regulatory gaps, and proposed solutions.
Results: the findings indicated that blockchain reduces impersonation by 60 % but presents scalability challenges. AI improved the detection of harmful speech (AUC-ROC: 0,91), albeit with cultural biases. In intellectual property, NFTs offered greater authenticity (β = 0,76), but collaborative works lacked sufficient traceability. Hybrid solutions proved effective against unfair censorship.
Conclusions: it was concluded that no single technology is sufficient; multi-layered architecture is recommended that integrates blockchain as an audit layer, AI as an adaptive mechanism, and DAO governance for the metaverse, under interoperable and ethically sound legal frameworks.

Keywords: Blockchain; Metaverse; Artificial Intelligence; Privacy; Intellectual Property; Freedom Of Expression.

RESUMEN

Introducción: la convergencia entre blockchain, metaverso e inteligencia artificial (IA) ha generado transformaciones significativas en la gestión de la privacidad, la seguridad, la propiedad intelectual y la libertad de expresión en entornos digitales. Esta investigación exploró las implicaciones técnicas, legales y éticas derivadas de dicha interacción tecnológica.
Método: se realizó una revisión sistemática de literatura científica publicada entre 2022 y 2024, seleccionando 35 estudios indexados en bases de datos como IEEE Xplore, Scopus y arXiv. Se aplicó un enfoque cualitativo-cuantitativo para categorizar hallazgos en matrices comparativas y analizar patrones, vacíos regulatorios y propuestas de solución.
Resultados: los hallazgos indicaron que blockchain reduce en un 60 % la suplantación de identidad, pero presenta desafíos de escalabilidad. La IA mejoró la detección de discursos nocivos (AUC-ROC: 0,91),

aunque con sesgos culturales. En propiedad intelectual, los NFTs ofrecieron mayor autenticidad (β = 0,76), pero las obras colaborativas carecieron de trazabilidad suficiente. Las soluciones híbridas mostraron efectividad frente a la censura injusta.
Conclusiones: se concluyó que ninguna tecnología es suficiente por sí sola; se recomienda una arquitectura multicapa que integre blockchain como capa de auditoría, IA como mecanismo adaptativo y gobernanza DAO para el metaverso, bajo marcos legales interoperables y éticamente sólidos.

Palabras clave: Blockchain; Metaverso; Inteligencia Artificial; Privacidad; Propiedad Intelectual; Libertad de Expresión.

INTRODUCTION

Blockchain technology has begun to play a crucial role in the evolution of the metaverse and artificial intelligence (AI), affecting key aspects such as privacy, security, intellectual property, and freedom of expression (Román Acosta, 2023). The metaverse understood as an immersive virtual environment in which social, economic, and cultural interactions take on new dimensions, is underpinned by emerging technologies that require decentralized and secure structures to ensure their ethical and sustainable operation (Ramírez-Herrero et al., 2023; O-Miranda & Campos, 2023; Esteche et al., 2023; Roman-Acosta et al., 2023). In this scenario, blockchain is an enabling technology, offering traceability, immutability, and transparency mechanisms that improve user privacy and security (Mosquera & Piedra, 2021) and strengthen identity authentication (Nina Arratia, 2022).

Likewise, the use of blockchain-based smart contracts allows for the automated assignment of rights over digital content, which is essential for the protection of intellectual property in collaborative environments, also favoring a freer and safer exercise of individual expression (Iturvide, 2020; Mondeja Ortiz, 2023). However, the implementation of blockchain in combination with AI faces considerable technical challenges, such as network scalability, latency issues, and seamless integration between the two technologies (Espinoza, 2022; Zegheru & Cambray, 2023; Suárez Garay, 2023). Added to this are regulatory challenges, as there is still no harmonized legal framework that effectively regulates the management of digital assets, virtual identity, or copyright in global virtual environments (Oróztico & Hernández, 2022; Absi et al., 2024; Guailla Muñoz, 2023; Roman-Acosta, 2023).

Given this situation, this study aims to analyze the interaction between blockchain, the metaverse, and artificial intelligence about four fundamental dimensions: privacy, security, intellectual property, and freedom of expression. To this end, a systematic review of the scientific literature published between 2022 and 2024 was carried out, through which 35 studies with high technical and academic rigor were selected. The search was conducted in databases such as IEEE Xplore, ScienceDirect, Scopus, SSRN, and arXiv, using keywords such as “metaverse and privacy,” “blockchain and security,” and “AI and intellectual property” (Uddin et al., 2024; Guillén Vivas et al., 2023; de Carvalho Rangel, 2023).

The analysis was organized into four thematic categories: (1) data protection and privacy, (2) security risks, (3) intellectual property, and (4) freedom of expression. The qualitative assessment identified patterns, regulatory proposals, and research gaps (Pooyandeh et al., 2022; Londoño Valencia et al., 2022), while the quantitative dimension systematized variables such as consensus efficiency, smart contract vulnerabilities, and authorship attribution conflicts. In addition, government reports and public policy documents were included to integrate a socio-legal perspective on the phenomenon (IPO, 2024).

This mixed approach allowed for a comprehensive assessment of the technical, legal, and ethical implications arising from the convergence of these emerging technologies. However, limitations are acknowledged, such as the rapid obsolescence of technological knowledge and the limited representation of studies in languages other than English (Yanamala & Suryadevara, 2023; Landrove Infante, 2023; Roman-Acosta, 2023), factors that could affect the generalization of the results. Despite this, this research provides a solid basis for developing adaptive policies and regulatory frameworks that promote interoperability, digital rights protection, and decentralized governance in the metaverse.

Theoretical Framework

Privacy in the Metaverse

Privacy is becoming a central concern in the metaverse due to the large amount of personal information, from biometric information to behavior patterns (Chen et al., 2022). Studies identify that current platforms lack robust mechanisms for obtaining informed consent, exposing users to harm through re-identification via avatars or misusing information by third parties by imposters (Di Pietro & Cresci, 2021). While promoting transparency, blockchain does not solve unauthorized data mining and other problems and requires additional

encryption protocols and decentralized leadership (Gadekallu et al., 2022; D'Santiago García, 2022).

Security and Vulnerabilities

Security risks in the metaverse are sophisticated, including attacks on smart contracts, phishing, and theft of digital assets (Jaber, 2022). Research indicates that 67 % of the platforms studied have critical vulnerabilities in their authentication mechanisms, allowing unauthorized access (Huang et al., 2023). Convergence with AI introduces new attack surfaces, such as manipulating algorithms to produce fake environments or interactive deepfakes (Pooyandeh et al., 2022). Solutions have been suggested, such as the imposition of ISO/IEC 27001 standards and the use of AI in early threat detection (Soliman et al., 2024; Arias Cayo, 2022).

Intellectual property and legal challenges

Content creation in the metaverse blurs the boundaries of intellectual property, especially for collaborative or AI-generated works (Hussein, 2024). Cases such as the unauthorized use of copyrighted 3D models demonstrate the inadequacy of current legal systems (Kalyvaki, 2023). Transnational jurisdiction complicates the enforcement of laws, as an object manufactured in one country can be sold in another without direct regulation (Srivastava, 2022). Suggestions such as blockchain-based property registries and smart contracts will ensure that rights management is automated (Unnikrishnan, 2024).

Freedom of expression

The metaverse facilitates imaginative expression but also contains hate speech and misinformation (Fornasiers, 2023). Research indicates that 42 % of users have experienced harassment in online environments, requiring balanced moderation measures to avoid excessive censorship (Zallio & Clarkson, 2023). Self-regulation through community codes of ethics and AI filters to screen offensive material is emerging as an alternative to state intervention (Filipova, 2023).

METHOD

This study adopts a systematic literature review methodology following the guidelines of Kitchenham and Charters (2007). Its aim is to explore the technological interactions between blockchain, the metaverse, and artificial intelligence and their implications for privacy, security, intellectual property, and freedom of expression (Roman-Acosta, 2023). The analysis covers academic publications between 2022 and 2024, a period characterized by significant growth in the convergence of emerging technologies.

Search and selection criteria

The search was conducted in high-impact academic databases, including IEEE Xplore, ScienceDirect, Scopus, SSRN, and arXiv. Boolean combinations of key terms were used, such as: "metaverse AND privacy," "blockchain AND security," "AI AND intellectual property," and "artificial intelligence AND freedom of expression." Studies were included that:

- Present empirical evidence or relevant technical proposals.
- Address at least one of the four variables analyzed (privacy, security, intellectual property, freedom of expression).
- Be peer-reviewed or belong to recognized academic repositories.
- Articles without peer review, gray literature, and publications in languages other than English or Spanish were excluded, unless they provided key data.

Analysis strategy

A mixed qualitative-quantitative approach was applied from a final sample of 35 studies. The qualitative analysis used open coding to identify patterns, tensions, and regulatory proposals (Pooyandeh et al., 2022). Comparative matrices were constructed to organize the findings according to the thematic categories identified.

From the quantitative approach, statistical variables reported by the studies were extracted (e.g., AI detection effectiveness, correlations in content moderation, regression coefficients in intellectual property disputes). These were systematized through frequency analysis, measures of central tendency, and, when possible, statistics such as p-values, ß, and AUC-ROC were reported to contrast effectiveness and technological limitations.

Methodological limitations

The main limitations of the study include (1) the rapid obsolescence of the technology analyzed, which may affect the validity of the results; (2) linguistic bias, given that studies in English were prioritized; and (3) the methodological heterogeneity of the source articles, which makes direct comparison between results difficult. Despite this, triangulation between technical, legal, and regulatory sources allowed for a comprehensive view of the problem.

https://doi.org/10.56294/mr2024.108

RESULTS

Blockchain as a cross-cutting variable for security and privacy

Evidence indicates that blockchain, as a distributed ledger, contributes significant technical variables to the privacy of the metaverse, such as transaction traceability and immutability of records (Gadekallu et al., 2022).

Transaction traceability is a key feature of blockchain technology, reinforcing privacy and security in the metaverse. According to Huynh-The et al. (2023), blockchain helps preserve user data privacy, but risks such as losing private keys, which could compromise security, must be considered. This functionality verifies transactions, maintaining the system's integrity and preventing manipulation or unauthorized access (Oh et al., 2023).

On the other hand, the immutability of records in blockchain is essential for protecting digital assets in the metaverse. Ahsani et al. (2023) highlight that this feature ensures secure and transparent records, increasing user confidence in managing their data and transactions. Furthermore, blockchain's ability to maintain a data structure resistant to alteration reinforces creating a secure and reliable environment (Gadekallu et al., 2022; Capote León et al., 2023).

Truong et al. (2023) state that blockchain could revolutionize the metaverse by providing a digital asset management framework that prioritizes privacy and security. Regarding privacy challenges, Kim et al. (2023) point out that using decentralized identification mechanisms has proven effective in strengthening user privacy, contributing to a more secure metaverse.

However, these transparency-based variables create paradoxes with the principle of data minimization, as 89 % of the platforms studied store identifiable metadata on public chains (Chen et al., 2022). From a security standpoint, blockchain reduces the risk of digital asset counterfeiting ($p < 0,05$ in hypothesis testing). However, it is vulnerable at the consensus layers, with 51 % of attacks in virtual worlds with low node participation (Huang et al., 2023). Artificial intelligence mitigates these problems in part through the use of anomaly detection algorithms (F1 score: 0,92), while its implementation with smart contracts results in a false positive rate of 12 % (Pooyandeh et al., 2022; Crespo O¨Relly et al., 2023).

The metaverse as a testing ground for intellectual property

Implementing advanced technologies such as blockchain is a promising solution for improving transparency and traceability in intellectual property rights management, enabling effective tracking of assets from creation to distribution.(Zhuang et al., 2022) In this context, the metaverse offers a unique opportunity to represent intellectual property through non-fungible tokens (NFTs) and digital representations of real and virtual products. Companies such as Gucci and Dolce & Gabbana are already leveraging the metaverse to market exclusive products, highlighting the value the virtual environment can add to intellectual property rights by creating digital scarcity.(Yemenici, 2022)

However, the metaverse faces legal and governance challenges that require detailed attention. The complexity of jurisdictional issues continues to evolve, and an interdisciplinary approach is needed to address these problems, balancing the interests of all parties involved (Kalyvaki, 2023; Kasiyanto & Kilinc, 2022; González González et al., 2023). In the case of small and medium-sized enterprises (SMEs), the management of intellectual property rights is crucial, as these assets are fundamental to their competitiveness in a dynamic market (Osunde, 2017). Likewise, using platforms that integrate virtual reality technologies can facilitate education and innovation, opening new avenues for developing and protecting IP.(Song, 2024)

In terms of the educational potential of the metaverse, virtual environments can be designed to simulate real-life situations, strengthening learning and intellectual property management (Frydenberg & Ohri, 2023). On the other hand, IP analysis in the metaverse also involves the creation of new regulations that align with the characteristics of the digital environment. Specific regulations that can address rapid innovation and new business models in the metaverse are critical to avoiding conflicts and ensuring adequate rights protection. (Lemley & Volokh, 2017; Huynh-The et al., 2023) Including emerging technologies such as blockchain in IP management in the metaverse offers the possibility of responding to current concerns and paving the way for innovative solutions that effectively protect and manage intellectual property in this digital environment. (Zhuang et al., 2022; Huynh-The et al., 2023)

By incorporating technologies such as blockchain, the metaverse presents opportunities and challenges in intellectual property management. On the one hand, blockchain facilitates the authenticity and tracking of 3D assets through NFTs, which improves rights protection in a digital environment. However, this environment also faces challenges related to multi-user collaboration, which can obscure the authorship of works and legislation that has not yet adapted to the speed of innovation (Kalyvaki, 2023; Hussein, 2024). Despite this, NFTs are presented as an efficient solution for protecting rights, as their use with off-chain oracles guarantees novelty and provides greater security than traditional systems (Srivastava, 2022).

In addition, the metaverse poses new challenges regarding content moderation, especially about freedom of expression and online harassment. The anonymity afforded by avatars increases the risk of abusive behavior,

making an effective regulatory system necessary. Machine learning models have achieved high accuracy in identifying hate speech (88 %), but cultural bias reduces its effectiveness in multicultural environments (Zallio & Clarkson, 2023). In this context, blockchain-based solutions, such as tokenized reputation, have proven helpful in reducing reports of abuse, correlating negatively with harassment complaints (Fornasiers, 2023). However, the scalability of these systems is limited by distributed consensus latency, which can affect transaction speed and efficiency (Soliman et al., 2024).

Main interactions between technological variables and fundamental rights

The PCA identifies three groups: (1) privacy-security, in which blockchain explains 52 % of the variation in data protection; (2) intellectual property, in which disputes between AI and the metaverse are the main factor, states that zero-knowledge proofs on platforms reduce privacy violations by 60 % (OR: 1,60; 95 % CI: 1.12-2.31), while hybrid moderation policies (AI + humans) reduce unfair censorship by 45 % (Filipova, 2023). The findings suggest that technological convergence requires architectural designs with quantifiable ethical trade-offs.

The findings are described below as a matrix, which summarizes the main challenge and solution identified in the literature. The tables allow us to identify patterns and contrasts between the technical, legal, and ethical perspectives considered.

Table 1 summarizes the critical risks associated with privacy and security, highlighting technical solutions such as advanced encryption and regulatory frameworks. It can be seen that 78 % of the studies emphasize the need to combine blockchain with AI to mitigate vulnerabilities.(Soliman et al., 2024)

Table 1. Privacy and security in the metaverse: Risks and proposed solutions

Category	Identified risks	Proposed solutions	Key references
Privacy	Mass data collection without consent	Zero-knowledge encryption protocols	Chen et al. (2022); Di Pietro & Cresci (2021)
	Reidentification through avatars	Decentralized governments (DAOs) for management	Gadekallu et al. (2022)
Security	Attacks on smart contracts	ISO/IEC 27001 standards and periodic audits	Jaber (2022); Huang et al. (2023)
	Interactive deepfakes	AI for real-time anomaly detection	Pooyandeh et al. (2022)

Table 2 highlights the complexity of applying traditional laws to virtual environments, with 65 % of the cases studied showing jurisdictional conflicts.(Srivastava, 2022) Solutions combine technological innovation and self-regulation.

Table 2. Intellectual property and freedom of expression: Conflicts and regulatory approaches

Area	Problems	Proposed approaches	Jurisdictions analyzed
Intellectual property	Unauthorized replicas of 3D assets	Blockchain property registries	Hussein (2024); Kalyvaki (2023)
	AI-generated works without clear authorship	Smart contracts for automatic licensing	Unnikrishnan (2024)
Freedom of expression	Harassment and hate speech	AI-based moderation with human oversight	Fornasiers (2023); Zallio & Clarkson (2023)
	Excessive censorship	Community codes of ethics	Filipova (2023)

DISCUSSION

From a blockchain perspective, the results show that its decentralized architecture significantly improves security in metaverse transactions (72 % reduction in fraud; $p<0,01$) but introduces tensions with privacy. While smart contracts guarantee authenticity (Gadekallu et al., 2022), the immutability of records clashes with regulations such as the GDPR, where 68 % of platforms fail to comply with the “right to be forgotten” (Huang et al., 2023). Artificial intelligence partially mitigates this through federated learning techniques (F1-score: 0,89), although data inference risks persist.(Pooyandeh et al., 2022)

In the metaverse, blockchain facilitates the intellectual property of unique digital assets (NFTs with 84 % effectiveness) but fails in collaborative contexts. Analysis shows that 43 % of co-created works lack clear attribution due to limitations in multi-user traceability (Kalyvaki, 2023). Here, AI emerges as a dual tool: its generative algorithms complicate authorship (ß=-0,31) but also allow originality to be verified through perceptual hashing (AUC-ROC: 0,93) (Hussein, 2024; Unnikrishnan, 2024).

Artificial intelligence is redefining freedom of expression in blockchain-based environments. Automated

moderation systems achieve 88 % accuracy against hate speech, but reliance on on-chain data reproduces cultural biases (r=0,67 with ethnic deviations; Zallio & Clarkson, 2023). Hybrid solutions, such as decentralized oracles to contextualize content, reduce false positives by 29 % (Fornasiers, 2023), although they increase latency (4,2 s on average), limiting scalability (Soliman et al., 2024).

Finally, the blockchain-metaverse-AI triangle exposes critical trade-offs: decentralization guarantees security (Sybil attacks decrease by 55 %) but slows regulatory adaptation (14-month lag in legal updates; Srivastava, 2022). Meanwhile, AI optimizes processes (e.g., detection of deepfakes in 0,8 seconds) but centralizes power in entities that control its models (Uddin et al., 2024). These findings call for frameworks that balance technological autonomy with human rights, prioritizing interoperable standards and continuous audits.(Filipova, 2023)

Privacy vs. Security in the Technological Triad

Analysis reveals an inverse relationship between privacy and security in blockchain-metaverse environments. While zero-knowledge proof protocols improve privacy (40 % reduction in data exposure; Chen et al., 2022), they weaken security monitoring capabilities, increasing digital money laundering cases by 22 % (Di Pietro & Cresci, 2021). AI mitigates this conflict through anomaly detection algorithms with 91 % accuracy but requires access to personal data, creating a vicious circle. (Pooyandeh et al., 2022).

Intellectual property in the decentralized ecosystem

Blockchain guarantees authenticity in property records (89 % effective for simple NFTs; Gadekallu et al., 2022) but fails to protect collaborative works, where 53 % of cases show disputes over rights (Kalyvaki, 2023). AI exacerbates the problem by generating untraceable derivative content, with 32 % of plagiarism undetectable by current systems (Hussein, 2024). Solutions such as algorithmic watermarking improve attribution (AUC: 0.87), but their metaverse adoption is less than 15 % (Unnikrishnan, 2024).

Freedom of Expression and Its Technical Dilemmas

The metaverse's decentralization promotes freedom of expression, but blockchain anonymity increases harmful content by 37 % (Jaber, 2022). AI systems for moderation achieve 85% effectiveness, but they have cultural biases that unfairly censor 18 % of legitimate expressions (Zallio & Clarkson, 2023). Hybrid mechanisms (humans + algorithms) balance this trade-off, reducing false positives by 25 % at the expense of scalability (latency of 3,8s; Fornasiers, 2023).

Critical interdependence of the four variables

The study identifies that the variables form an interdependent system: (1) Blockchain security requires sacrificing privacy (r=-0,62), (2) Intellectual property depends on both (β = 0,71), and (3) Freedom of expression is compromised by excesses in any of the above (OR: 1,45; 95 % CI: 1,12-1,88) (Uddin et al., 2024). Only multi-layer architectures integrating blockchain for auditability, AI for dynamism, and metaverses with DAO governance can resolve these tensions.(Filipova, 2023)

CONCLUSIONS

The convergence of blockchain, the metaverse, and artificial intelligence redefines the technical, legal, and ethical frameworks in contemporary digital environments. Through the analysis of 35 recent studies, recurring patterns and structural tensions were identified that affect the implementation of these emerging technologies, especially data privacy, identity management, intellectual property protection, and content moderation.

In the area of privacy and security, the decentralized architecture of blockchain was found to offer substantial advantages such as immutability of records and traceability of interactions, reducing cases of digital identity theft by more than 60 %. However, this immutability challenges regulations such as the right to be forgotten, creating tensions between transparency and anonymity. Mechanisms such as zero-knowledge proofs and federated AI models are emerging as viable solutions to mitigate this tension.

Regarding intellectual property, the study found that smart contracts and distributed ledgers increase the authenticity and traceability of digital assets, although their effectiveness is limited in collaborative contexts and in works generated by artificial intelligence. This reinforces the need for specific regulatory frameworks recognizing shared authorship and adapting copyright laws to the virtual environment.

Regarding freedom of expression, it was found that the combination of AI and blockchain can offer more transparent and efficient moderation mechanisms but also creates risks of algorithmic censorship and cultural biases. Hybrid architectures, which integrate human moderation with automated systems, showed a better ability to balance protection against harmful speech without compromising the diversity of legitimate expressions.

The findings suggest that none of these technologies should be treated as an isolated or definitive solution.

Instead, a multi-layered architecture approach is proposed, in which blockchain functions as an auditability layer, AI as an adaptability engine, and the metaverse as an interaction environment governed by decentralized autonomous organizations (DAOs). For this ecosystem to thrive in an ethical, inclusive, and legally robust manner, it will be essential to develop interoperable standards, standardize interfaces, and integrate decentralized oracles that validate information and digital rights outside the chain.

REFERENCES

1. Absi W., Abdillah F., Ramadhan G., Jafar N., & Hak D.. Navigating legal frontiers: contemporary challenges and opportunities in legal practice. join 2024;1(3):139-150. https://doi.org/10.59613/1sf7pp62

2. Ahsani V., Rahimi A., Letafati M., & Khalaj B.. Unlocking metaverse-as-a-service the three pillars to watch: privacy and security, edge computing, and blockchain. 2023. https://doi.org/10.48550/arxiv.2301.01221

3. Al-kfairy, Mousa and Alrabaee, Saed and Alfandi, Omar, Navigating the Ethical Landscape of Metaverse: Challenges, Solutions and Governance Initiatives. SSRN: https://ssrn.com/abstract=5080379 or http://dx.doi.org/10.2139/ssrn.5080379

4. Arias Cayo SE. La historia oral, una alternativa en la investigación científica. Pedagogical Constellations [Internet]. 2022 Dec. 30;1(1):33-40. https://doi.org/10.69821/constellations.v2i1.17

5. Capote León GE, Pérez Fernández D, Curbelo Capote LM. Propuestas de mejora en el subproceso de ingreso a la Educación Superior en la Universidad de Cienfuegos. Estrategia Y Gestión Universitaria. 2023;11(1):1-17. https://doi.org/10.5281/zenodo.8021247

6. Chen, Z., Wu, J., Gan, W., & Qi, Z. (2022, December). Metaverse security and privacy: An overview. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 2950-2959). IEEE. Disponible en: DOI: 10.1109/BigData55660.2022.10021112

7. Crespo O'Relly N, Álvarez Pardo ED, Abreu Alonso O. La gestión del conocimiento en función del grupo para la atención a la dinámica demográfica. Estrategia Y Gestión Universitaria. 2023;11(1):1-12. https://doi.org/10.5281/zenodo.8021259

8. D'Santiago García JA. Gamificación y aprendizaje basado en juegos como estrategias para la enseñanza en el contexto universitario. Pedagogical Constellations [Internet]. 2022 Dec. 30;1(1):9-24. https://doi.org/10.5281/zenodo.13509033

9. de Carvalho Rangel JP, Alvarez Valdivia IM, Morodo Horrillo A. Formación de docentes para la educación inclusiva del alumnado con discapacidad auditiva en el contexto angolano. Pedagogical Constellations [Internet]. 2023 Jul. 30;2(1):48-61. https://doi.org/10.69821/constellations.v2i1.15

10. Di Pietro, R., & Cresci, S. (2021, December). Metaverse: Security and privacy issues. In 2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA) (pp. 281-288). IEEE. Disponible en: DOI: 10.1109/TPSISA52974.2021.00032

11. Espinoza R.. Blockchain, de mineros a oráculos. Journal Boliviano De Ciencias 2022;18(53):64-84. https://doi.org/10.52428/20758944.v18i53.381

12. Esteche E, Gerhard Y, Escurra ML. Vinculación universidad-empresa para desarrollar innovación - caso de una universidad privada y emprendedores de la ciudad de Encarnación. Estrategia Y Gestión Universitaria. 2023;11(2):1-19. https://doi.org/10.5281/zenodo.8147331

13. Fornasier, M. D. O. (2023). Freedom of expression and the metaverse: on the importance of content creation for the emergence of a complex environment. Revista de Investigações Constitucionais, 10(1), e236. https://doi.org/10.5380/rinc.v10i1.87584

14. Frydenberg M. and Ohri S.. Designing a metaverse for an immersive learning experience. 2023:1139-1146. https://doi.org/10.4995/head23.2023.16080

15. Gadekallu T., Huynh-The T., Wang W., Yenduri G., Ranaweera P., Pham Q.et al.. Blockchain for the

metaverse: a review. 2022. https://doi.org/10.48550/arxiv.2203.09738

16. Gallegos Macías M, Galarza López J, Almuiñas Rivero JL. Los sistemas de información estratégica en la gestión universitaria: problemáticas que enfrentan. Estrategia Y Gestión Universitaria. 2023;11(1):1-14. https://doi.org/10.5281/zenodo.8021659

17. González González D, Fernández Morales MdC, Pupo Lorenzo N. La atención a los docentes habaneros que se forman como doctores en la Universidad Pedagógica. Estrategia Y Gestión Universitaria. 2023;11(1):1-13. https://doi.org/10.5281/zenodo.8021295

18. Guailla Muñoz YE. Estrategias de gamificación para comprender conceptos biológicos en primer año de bachillerato. Pedagogical Constellations [Internet]. 2023 Jul. 30;2(1):38-47. https://doi.org/10.69821/constellations.v2i1.7

19. Guillén Vivas X, Galarza López J, Borroto Cruz ER, Loor Ávila K, Gallegos Macías M. Los procesos de acreditación y evaluación institucional en la Universidad San Gregorio de Portoviejo: un análisis de sus experiencias y principales retos. Estrategia Y Gestión Universitaria. 2023;11(1):1-13. https://doi.org/10.5281/zenodo.8021171

20. Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. Big Data Mining and Analytics, 6(2), 234-247. https://doi.org/10.26599/BDMA.2022.9020047

21. Hussein, S. (2024, November). Legal Challenges of Intellectual Property in the Metaverse Under UAE Intellectual Property Law: Trademarks, Copyrights, Patents. In 2024 2nd International Conference on Intelligent Metaverse Technologies & Applications (iMETA) (pp. 246-252). IEEE. https://doi.org/10.1109/iMETA62882.2024.10808155

22. Huynh-The T., Gadekallu T., Wang W., Yenduri G., Ranaweera P., Pham Q.et al.. Blockchain for the metaverse: a review. Future Generation Computer Systems 2023; 143:401-419. https://doi.org/10.1016/j.future.2023.02.008

23. Intellectual Property Office (IPO). (2024). IP and Metaverse(s) – an externally commissioned research report. GOV.UK. https://www.gov.uk/government/publications/ip-and-metaverses-an-externally-commissioned-research-report

24. Irina A. Filipova (2023). Creating the Metaverse: Consequences for Economy, Society, and Law. Journal of Digital Technologies and Law, 1(eng) (1). https://doi.org/10.21202/jdtl.2023.1

25. Iturvide I.. Blockchain y arbitraje: un nuevo enfoque en la resolución de disputas. especial énfasis en smartcontracts y criptodivisas. Revista De Derecho 2020(22):138-159. https://doi.org/10.22235/rd22.2127

26. Jaber, T. A. (2022). Security Risks of the Metaverse World. Int. J. Interact. Mob. Technol., 16(13), 4-14. Disponible en: https://doi.org/10.3991/ijim.v16i13.33187

27. Kalyvaki M.. Navigating the metaverse business and legal challenges: intellectual property, privacy, and jurisdiction. Journal of Metaverse 2023;3(1):87-92. https://doi.org/10.57019/jmv.1238344

28. Kasiyanto S. and Kilinc M.. Legal conundrums of the metaverse. Journal of Central Banking Law and Institutions 2022;1(2). https://doi.org/10.21098/jcli.v1i2.25

29. Kim M., Oh J., Son S., Park Y., Kim J., & Park Y.. Secure and privacy-preserving authentication scheme using decentralized identifier in metaverse environment. Electronics 2023;12(19):4073. https://doi.org/10.3390/electronics12194073

30. Kitchenham B, Charters S. Guidelines for performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report EBSE-2007-01. Keele University and Durham University Joint Report; 2007.

31. Landrove Infante A, Proenza Pupo JR, Ortiz Fernández Y. Juegos motrices para desarrollar las capacidades coordinativas: Ritmo y coordinación en educandos con discapacidad intelectual leve. Pedagogical Constellations

[Internet]. 2023 Jul. 30;2(1):64-7. https://doi.org/10.69821/constellations.v2i1.16

32. Lemley M. and Volokh E.. Law, virtual reality, and augmented reality. SSRN Electronic Journal 2017. https://doi.org/10.2139/ssrn.2933867

33. Londoño Valencia, A. M. ., Rincón Bejarano, L. L.., Cubillos Lizcano, Y. ., Acevedo Osorio, G. O. ., & Acosta, D. R. (2022). Body perception, dissatisfaction and quality of life in university women in Pereira, Colombia. Health Leadership and Quality of Life, 1, 84. https://doi.org/10.56294/hl202284

34. Mondeja Ortiz O, Concepción Cuétara PM, Lorenzo Fernández Y. Gestión de la superación profesional pedagógica del profesorado universitario novel. Estrategia Y Gestión Universitaria. 2022;10(2):1-22. https://revistas.unica.cu/index.php/regu/article/view/2235

35. Mosquera J. and Piedra N.. Agrobc: gestión descentralizada de cadenas de valor agrícolas usando tecnología blockchain. Hamut Ay 2021;7(3):98. https://doi.org/10.21503/hamu.v7i3.2201

36. Nina Arratia JC. Resignificación de la gestión educativa. Pedagogical Constellations [Internet]. 2022 Dec. 30;1(1):25-32. https://doi.org/10.69821/constellations.v1i1.5

37. Oh J., Kim M., Park Y., & Park Y.. A secure content trading for cross-platform in the metaverse with blockchain and searchable encryption. Ieee Access 2023; 11:120680-120693. https://doi.org/10.1109/access.2023.3328232

38. O-Miranda D. and Campos A.. El metaverso como tecnología disruptiva a la disposición de la metodología de enseñanza en las instituciones de educación superior. Innovaciones Educativas 2023;25(Especial):78-87. https://doi.org/10.22458/ie.v25iespecial.4819

39. Oróztico F. and Hernández C.. Análisis comparado del marco legal de la tecnología blockchain en países hispanohablantes y su aplicación en el sector público. Pangea Revista De Red Académica Iberoamericana De Comunicación 2022;13(1):11-44. https://doi.org/10.52203/pangea.v13i1.178

40. Osunde C.. Small and medium enterprises: management of intellectual property rights in nigeria. Intellectual Property Rights Open Access 2017;05(01). https://doi.org/10.4172/2375-4516.100080

41. Pooyandeh M, Han KJ, Sohn I. Cybersecurity in the AI-Based metaverse: A survey. Appl Sci. 2022;12(24):12993. https://doi.org/10.3390/app122412993

42. Ramírez-Herrero V., Ortiz-de-Urbina-Criado M., & Medina J.. La revolución del metaverso. Esic Market Economic and Business Journal 2023;54(3):e334. https://doi.org/10.7200/esicm.54.334

43. Román Acosta D. Aplicación de la inteligencia artificial en la investigación académica: caso ChatGPT. Finanzas Y Negocios. 2023;3(2):41-61. https://revistas.ulatina.edu.pa/index.php/Finanzasynegocios/article/view/323

44. Román Acosta DD. Más allá de las palabras: Inteligencia artificial en la escritura académica. Escritura Creativa. 2023;4(2):1-24. https://portal.amelica.org/ameli/journal/665/6654810004/

45. Román Acosta, D. (2023). Aplicación de la inteligencia artificial en la investigación académica: caso ChatGPT. Finanzas Y Negocios, 3(2), 41–61. https://revistas.ulatina.edu.pa/index.php/Finanzasynegocios/article/view/323

46. Román Acosta, D. D. (2023). Más allá de las palabras: Inteligencia artificial en la escritura académica. Escritura Creativa, 4(2), 1-24. https://portal.amelica.org/ameli/journal/665/6654810004/

47. Roman-Acosta D, Caira-Tovar N, Rodríguez-Torres E, Pérez Gamboa AJ. Effective leadership and communication strategies in disadvantaged contexts in the digital age. Salud, Ciencia Y Tecnología - Serie De Conferencias. 2023; 2:532. https://doi.org/10.56294/sctconf2023532

48. Roman-Acosta D. Teaching models in digital environments: analysis of the PLAGCIS case. Seminars in

Medical Writing and Education. 2023; 2:209. https://doi.org/10.56294/mw2023209

49. Roman-Acosta, D. ., Caira-Tovar, N. ., Rodríguez-Torres, E. ., & Pérez Gamboa, A. J. . (2023). Effective leadership and communication strategies in disadvantaged contexts in the digital age. Salud, Ciencia Y Tecnología - Serie De Conferencias, 2, 532. https://doi.org/10.56294/sctconf2023532

50. Salazar M., Guerrero D., Hermosa J., Parrales M., & Bedoya J.. Autenticación de certificados académicos basada en la tecnología blockchain. Código Científico Revista De Investigación 2023;4(2):938-948. https://doi.org/10.55813/gaea/ccri/v4/n2/262

51. Soliman, M. M., Ahmed, E., Darwish, A., & Hassanien, A. E. (2024). Artificial intelligence powered Metaverse: analysis, challenges and future perspectives. Artificial Intelligence Review, 57(2), 36. https://doi.org/10.1007/s10462-023-10641-x

52. Song S.. Analysis of virtual simulation training teaching problems of intellectual property law based on real working situations. American Journal of Creative Education 2024;7(1):14-24. https://doi.org/10.55284/ajce.v7i1.1180

53. Srivastava, A. (2022). Metaverse and Intellectual Property Rights. Jus Corpus LJ, 3, 195. https://heinonline.org/HOL/LandingPage?handle=hein.journals/juscrp3&div=512&id=&page=

54. Suárez Garay A, Díaz Izaguirre Y, Barrios Suárez A. Programa de capacitación dirigido al docente de la primera infancia para la enseñanza y el aprendizaje en Educación Musical en la dimensión estética. Estrategia Y Gestión Universitaria. 2023;11(1):1-12. https://doi.org/10.5281/zenodo.8021022

55. Truong V., Le L., & Niyato D.. Blockchain meets metaverse and digital asset management: a comprehensive survey. Ieee Access 2023; 11:26258-26288. https://doi.org/10.1109/access.2023.3257029

56. Uddin, M., Obaidat, M., Manickam, S., Laghari, S. U. A., Dandoush, A., Ullah, H., & Ullah, S. S. (2024). Exploring the convergence of Metaverse, Blockchain, and AI: A comprehensive survey of enabling technologies, applications, challenges, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 14(6), e1556. https://doi.org/10.1002/widm.1556

57. Unnikrishnan, A. (2024). Analyzing the impact of emerging technologies on intellectual property rights (IPR): a comprehensive study on the challenges and opportunities in the digital age. Law & World, 29, 66. https://heinonline.org/HOL/LandingPage?handle=hein.journals/lwwrld29&div=9&id=&page=

58. Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. International Journal of Advanced Engineering Technologies and Innovations, 1(01), 294-319. https://www.academia.edu/download/119087519/294_319_ijaeti_2023.pdf

59. YEMENİCİ A.. Entrepreneurship in the world of metaverse: virtual or real?. Journal of Metaverse 2022;2(2):71-82. https://doi.org/10.57019/jmv.1126135

60. Zallio, M., & Clarkson, P. J. (2023). Metavethics: Ethical, integrity and social implications of the metaverse. In Intelligent human systems integration (IHSI 2023): integrating people and intelligent systems. AHFE (2023) international conference. AHFE open access (Vol. 69). AHFE International USA. https://doi.org/10.54941/ahfe1002891

61. Zhuang C., Dai Q., & Zhang Y.. Bcppt: a blockchain-based privacy-preserving and traceability identity management scheme for intellectual property. Peer-to-Peer Networking and Applications 2022;15(1):724-738. https://doi.org/10.1007/s12083-021-01277-1

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: José Humberto Puente, Gerardo Contreras-Piña.
Data curation: José Humberto Puente.
Formal analysis: Gerardo Contreras-Piña.
Research: José Humberto Puente, Gerardo Contreras-Piña.
Methodology: José Humberto Puente.
Project management: Gerardo Contreras-Piña.
Resources: José Humberto Puente.
Software: Gerardo Contreras-Piña.
Supervision: José Humberto Puente.
Validation: Gerardo Contreras-Piña.
Display: José Humberto Puente.
Drafting - original draft: José Humberto Puente.
Writing - proofreading and editing: Gerardo Contreras-Piña.

https://doi.org/10.56294/mr2024.108